IT Security Association Germany
Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

Richtlijn "Stand der techniek"

Technische en organisatorische maatregelen

2025

Nederlands versie

In co-operatie met:

PRIVACY EN BEVEILIGING ADVIES
BREEMAN

Erkenning

TeleTrusT bedankt de volgende personen voor hun deelname aan de TeleTrusT Task Force Stand der Technik en voor hun actieve bijdrage aan deze richtlijn.

Projectmanagement

Tomasz Lawicki - Capgemini
RA Karsten U. Bartels LL.M. - HK2 Rechtsanwälte

Auteurs en deelnemende experts

Abou Nasser, Morad - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Bartels, Karsten U. - HK2 Rechtsanwälte
Barth, Michael - genua
Bausewein, Christoph - CrowdStrike
Benzmüller, Ralf - G DATA
Bernhardt, Ulf - valantic
Dehning, Oliver - eco
Dominkovic, Dennis - SEC Consult
Dubbel, Sascha
Falkenthal, Oliver - CCVOSSEL
Fischer, Marco - procilon
Föllmer, Nancy - heinzl
Glemser, Tobias - secuvera
Gremeyer, Erik - ATM Consulting
Heyde, Steffen - secunet
Jäger, Hubert - Digital Trust Innovations
Kahrs, Malte - MTRIX
Kissling, Kristian - DCSO
Kohn, Ulrich - Adva Network Security
Kolmhofer, Robert - FH Oberösterreich
Kowol, Dominik - eperi
Krosta-Hartl, Pamela - LANCOM
Kynast, Michael - DCSO
Lang, Thomas - valantic
Lawicki, Tomasz - Capgemini
Leitner, Alexander - UNINET
Liedke-Deutscher, Bernd - TÜV Informationstechnik
Maier, Janosch - Crashtest Security
Martin, Karl-Ulrich - Detack
Menge, Stefan - Achtwerk
Mielke, Tobias - TÜV Informationstechnik
Mühlbauer, Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Müller, Siegfried
Pfister, Benjamin - VAF
Rechberg, Johanna - UNINET
Rost, Peter - secunet
Schlensog, Alexander - secunet
Weigmann, Matthias - ANMATHO
Wilke, Klaus - CCVOSSEL
Zingsheim, André - TÜV TRUST IT

Dit document dient als leidraad en geeft een overzicht. Zij beweert niet uitputtend te zijn, noch beweert zij een exacte uitlegging van de bestaande wettelijke bepalingen te zijn. Het mag niet in de plaats komen van de studie van de relevante richtlijnen, wet- en regelgeving. Bovendien moet rekening worden gehouden met de bijzondere kenmerken van de respectieve producten en hun verschillende toepassingen. In dit opzicht is een groot aantal andere constellaties denkbaar voor de beoordelingen en procedures die in het document aan de orde komen.

Colofon

Uitgever:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4310
E-Mail: info@teletrust.de
https://www.teletrust.de

V 1_2025-09 NL

Dutch version: Jan Breeman

Inhoudsopgave

Afbeeldingoverzicht

Tabeloverzicht

Principes van de hand-out

Toen in juli 2015 de IT-Sicherheitsgesetz (ITSiG) in werking trad, heeft de Bundesverband IT-Sicherheit e.V. (TeleTrusT) de werkgroep "Stand der Technik" (AK-SdT) geïnitieerd om de betrokken partijen aanbevelingen te doen voor oriëntatie en actie op de vereiste stand van de techniek van technische en organisatorische maatregelen. Om aan deze hoge standaard te voldoen, heeft de werkgroep voor de ontwikkeling, evaluatie en actualisering van de hand-out de volgende principes gedefinieerd:

1. **Basiskennis van het document**
   Deze hand-out is bedoeld om zowel aanvragende als aanbiedende bedrijven (fabrikanten, dienstverleners) te helpen bij het bepalen van de stand van de techniek art in de zin van de toepasselijke wetgeving. Het document kan dienen als referentie voor contractuele afspraken, aanbestedingsprocedures en voor de classificatie van geïmplementeerde beveiligingsmaatregelen.

   Deze hand-out is bedoeld als startpunt voor het bepalen van wettelijk verplichte IT-beveiligingsmaatregelen, het vervangt niet het technische, organisatorische of juridische advies of de beoordeling voor individuele gevallen. Desalniettemin kan het worden gebruikt om IT-beveiligingsmaatregelen te identificeren om de immuniteit van het systeem tegen aanhoudende bedreigingen te versterken.

2. **Verantwoordelijkheid voor ontwikkeling, evaluatie en actualisering**
   De TeleTrusT-werkgroepen "Stand der Technik" en "Recht" houden zich bezig met het beantwoorden van de vraag hoe de betreffende stand van de techniek in de zin van de wet kan worden bepaald met betrekking tot de technische en organisatorische maatregelen en hoe de wettelijke vereisten moeten worden geïmplementeerd.

3. **Inzicht in de procedure**
   De werkgroep ontwikkelt haar resultaten in een transparant proces en legt de aanbevelingen voor actie en oriëntaties in een regelmatig actualiseringproces voor openbare discussie.

4. **Evaluatieprocedure**
   De werkgroep baseert haar beoordeling op een gestandaardiseerd schema, dat voor de afzonderlijke maatregelen in kwestie wordt ingevuld en gepubliceerd. De methode voor het classificeren van de stand van de techniek van de hier beschreven beveiligingsmaatregelen wordt uitgelegd in deel 2 van dit document.

5. **Bijwerken**
   Om recht te doen aan de technologische vooruitgang is het de bedoeling om deze hand-out regelmatig te actualiseren en te publiceren. Kleine aanpassingen en aanvullingen op de hand-out (zoals nieuwe bijdragen aan de technische maatregelen) kunnen in de loop van het jaar verschijnen als herzieningen van de hand-out.

6. **Disclaimer en juridische kennisgeving**
   Deze hand-out vormt geen juridisch bindende interpretatie of technische norm. Het kan echter worden gebruikt als een erkende consensus in de sector, in professionele kringen, in het kader van audits en bij de interpretatie van ongedefinieerde juridische termen. Het vervangt geen individueel juridisch, technisch of organisatorisch advies. De inhoud is gebaseerd op de huidige stand van de techniek, wetenschap en praktijk op het moment van publicatie. Wijzigingen in rechtsgrondslagen en technische ontwikkelingen kunnen een update vereisen. De toepassing van de aanbevelingen in deze hand-out is op eigen risico.

1 Inleiding

1.1 Wettelijke en regelgevende basis

De vraag wat concreet onder state-of-the-art op het gebied van IT-beveiliging moet worden verstaan is een van de meest veeleisende uitdagingen bij het juridisch conforme ontwerp en de implementatie van technische en organisatorische maatregelen voor de bescherming van netwerk- en informatiesystemen en verwerkte gegevens, en diensten die via deze netwerk- en informatiesystemen worden aangeboden of toegankelijk zijn.

Lange tijd werd in de wetgeving geen rekening gehouden met IT-beveiliging. In het afgelopen decennium werden de nationale en Europese wetgevers echter op regelgevend niveau geconfronteerd met de toenemende digitalisering van alle gebieden van het leven en de economie. Sindsdien wordt de wetgeving op het gebied van IT-beveiligingsrecht gekenmerkt door een bijzondere dynamiek waarop bijna geen enkel ander rechtsgebied kan bogen. Het samenspel van nationale (implementatie)wetgeving en Europese eisen, het soms naast elkaar bestaan van sectorspecifieke en crosssectorale regelgeving en de permanente regeldruk als gevolg van technische ontwikkelingen en voortdurend veranderende dreigingsituaties maken het IT-beveiligingsrecht tot een ingewikkelde uitdaging voor zowel bedrijven, overheden als rechtsbeoefenaars.

Om de dynamiek tegen te gaan, is in een groot deel van de rechtshandelingen voorzien in het gebruik van de state-of-the-art als referentieterm en technologieniveau. De stand van de techniek kan ook belangrijk zijn voor de specificatie van ongedefinieerde juridische termen, zoals de "noodzaak" of "geschiktheid" van maatregelen. Hierna worden de belangrijkste wet- en regelgeving van het IT-beveiligingsrecht die betrekking hebben op de stand van de techniek kort gepresenteerd.

1.1.1 De IT-Sicherheitsgesetze (ITSiG) en Europese harmonisatie

De Europese NIS-richtlijn en de nationale IT-Sicherheitsgesetz ten kunnen worden geïdentificeerd als het "hart" van de IT-beveiligingswetgeving, die met name ingrijpende veranderingen in de BSiG teweegbracht. Het doel van deze verordeningen is te zorgen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in alle sectoren, waarmee nationale en grensoverschrijdende risico's adequaat worden aangepakt. Het doel van de Europese transformatie is het creëren van een uniform kader met minimumvereisten voor de IT-beveiliging van netwerk- en informatiesystemen binnen de hele Europese Unie.

1.1.1.1 2015 ITSiG

De IT-Sicherheitsgesetz (ITSiG) is op 25.07.2015 in werking getreden en kan worden gezien als het "startsein" voor het verbeteren van de beveiliging van informatietechnologiesystemen in Duitsland.

De ITSiG is een zogenaamde Artikelwet, die verschillende sectorspecifieke wetten wijzigde. In het bijzonder heeft de ITSiG in de wet op het Bundesamt für die Sicherheit in der Informationstechnik (BSiG)voorschriften voor kritieke infrastructuren (KRITIS) opgesteld. Daarnaast zijn wetswijzigingen doorgevoerd in de volgende wetten: Atomgesetz (AtomG), Energiewirtschaftsgesetz (EnWG), Telemediengesetz (TMG) en Telekommunikationsgesetz (TKG).

De ITSiG voorzag in de meest uitgebreide wijzigingen voor de BSiG. Voor het eerst zijn de KRITIS-providers afzonderlijk aangesproken en zijn aan hen IT-beveiligingverplichtingen opgelegd. Dit had gevolgen voor bedrijven die te maken hebben met de levering van energie, informatietechnologie en telecommunicatie, vervoer en verkeer, gezondheid, water, voedsel en financiën. Daarbij streefde de BSiG naar een op risico's gebaseerde aanpak: alleen die bedrijven werden aangepakt die zo belangrijk waren dat hun faillissement een aanzienlijke bedreiging vormen voor de bevoorrading en de openbare veiligheid. Dit werd door een wettelijke verordening (KRITIS-Verordening bepaald op basis van drempelwaarden in de afzonderlijke sectoren.

Deze KRITIS- providers werden op grond van (oude versie BSiG § 8a lid 1) verplicht om passende technische en organisatorische voorzorgsmaatregelen te nemen om de beschikbaarheid, integriteit, authenticiteit en vertrouwelijkheid van hun IT-systemen te beschermen. In deze context was de state-of-the-art al van elementair belang als minimumnorm die in acht moest worden genomen. Andere bepalingen bevatten onder meer een verplichting om het bewijs van deze vereisten te leveren (oude

versie BSiG § 8a lid 3) en een verplichting om bepaalde IT-beveiligingsincidenten te melden (oude versie BSiG § 8b lid 4)
Het TeleTrusT-commentaar op de IT-Sicherheitsgesetz en de toelichting daarbij zijn te vinden via de volgende link: www.teletrust.de/it-sicherheitsgesetz.

1.1.1.2 NIS-richtlijn

De Europese Commissieheeft in 2016 de "Richtlijn betreffende maatregelen om een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen te waarborgen" (de NIS-richtlijn) aangenomen die in nationaal recht moest worden omgezet. Dit heeft echter, aangezien de nationale wetgever met de vaststelling van de ITSiG in 2015 al had geanticipeerd op een groot deel van de door de Europese wetgever beoogde vereisten, niet geleid tot fundamentele wijzigingen. De overeenkomstige NIS-richtlijn uitvoeringswet, die 27.04.2017 werd aangenomen leidde daarom alleen tot een wijziging van de BSiG.

Op basis van de richtlijn werd onder meer BSiG § 8c (oude versie) ingevoerd, waardoor aanvullende verplichtingen voor aanbieders van digitale diensten in het leven werden geroepen. Digitale diensten zijn gedefinieerd als online marktplaatsen, online zoekmachines en cloudcomputingdiensten van een gestandaardiseerde omvang. Deze diensten moeten ook technische en organisatorische maatregelen (TOM) implementeren om, rekening houdend met de stand van de techniek, de IT-beveiliging te beschermen. De maatregelen zijn bedoeld om een op het risico afgestemd beschermingsniveau te waarborgen, waarbij onder meer de beveiliging van systemen en faciliteiten, de afhandeling van beveiligingsincidenten en het beheer van de bedrijfscontinuïteit worden gewaarborgd, bovendien breidde de NIS-uitvoeringswet de bevoegdheden van het Federaal Bureau voor Informatiebeveiliging in de BSiG uit. Door de Uitvoeringswet NIS als artikelwet zijn ook de overeenkomstige bepalingen in de AtomG, EnWG, SGB V en TKG gewijzigd.

1.1.1.3 2021 ITSiG 2.0

In mei 2021 is de ITSiG versie 2.0 in werking getreden en dit heeft de bestaande regelgeving inzake informatiebeveiliging in Duitsland aanzienlijk uitgebreid.

Naast de tot nu toe gedefinieerde sectoren, zoals energie, water, voedsel, gezondheid, informatietechnologie en telecommunicatie, transport en verkeer en financiën en verzekeringen, heeft ITSiG 2.0 zich op twee andere gebieden gericht:

- Enerzijds is het **stedelijk afvalbeheer** toegevoegd als een nieuwe sector van kritieke infrastructuur. Deze sector omvat de inzameling, het vervoer, de nuttige toepassing en de verwijdering van stedelijk afval.
- Anderzijds zijn, naast KRITIS- providers en aanbieders van digitale diensten,ook **bedrijven van bijzonder openbaar belang (UBI)** toegevoegd als nieuwe doelgroep. Hiertoe behoren bedrijven die vanwege hun belang voor de gemeenschap bijzonder beschermingswaardig worden geacht. De UBI's hebben hun eigen programma van verplichtingen in overeenstemming met BSiG § 8f.

Deze uitbreiding heeft ertoe geleid dat nu aanzienlijk meer organisaties verplicht zijn om effectieve maatregelen te nemen om hun IT-beveiliging te verhogen.

De ITSiG 2.0 bracht uitgebreide verplichtingen met zich mee voor providers van kritieke infrastructuur en bedrijven van bijzonder openbaar belang (UBI), zoals:

- **Inbraakdetectiesystemen:** Providers zijn verplicht om technische hulpmiddelen en ondersteunende processen te gebruiken voor de continue detectie van bedreigingen tijdens het gebruik (BSiG § 8a lid 1a). Deze systemen moeten uiterlijk op 1 mei 2023 geïmplementeerd en in audits aangetoond zijn.

- **Directe registratie:** Providers moeten zich onmiddellijk na het bepalen van hun KRIITIS-status registreren bij de BSI en een contactpunt aanwijzen (BSiG sectie 8b lid 3). De BSI heeft ook de bevoegdheid om zelfstandig providers te identificeren als kritieke infrastructuur en om de relevante documenten te inspecteren.

Bovendien reguleerde ITSiG 2.0 voor het eerst "kritieke componenten". Het gebruik van speciale IT-componenten in kritieke infrastructuursystemen moet,, overeenstemming met BSiG sectie 9b lid 1, worden gemeld aan het federale ministerie van Binnenlandse Zaken, die dan het gebruik ervan kan verbieden. Daarnaast voorziet de ITSiG 2.0 in hogere boetes voor overtredingen en versterkt het de

bevoegdheden van het BSI. In geval van overtredingen kan de BSI diepgaand inzicht in de IT-systemen van de providers eisen en, indien nodig, maatregelen treffen.

De stand van de techniek heeft ook zijn weg gevonden naar de verplichtingen voor UBI's. De UBI-zelfverklaring die in overeenstemming met BSiG artikel 8f lid 1 moet worden ingediend, moet onder meer bevatten hoe ervoor kan worden gezorgd dat de IT-systemen van de organisatie adequaat worden beschermd en dat aan de stand van de techniek wordt voldaan. In tegenstelling tot KRITIS- providers is echter voor de UBI geen directe verplichting om te voldoen aan de stand van de techniek.

1.1.1.4 NIS2-richtlijn

De NIS2-richtlijn ("Richtlijn betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie") van 14 december 2022 is een EU-richtlijn die tot doel heeft een hoog gemeenschappelijk niveau van cyberbeveiliging binnen de Europese Unie te waarborgen en vervangt de NIS-richtlijn van 2016. De uiterste datum voor omzetting door de lidstaten was 17 oktober 2024. De Duitse wetgever heeft de deadline voor implementatie niet gehaald, ten tijde van het opstellen van deze handreiking was nog geen uitvoeringswet beschikbaar.

De NIS2-richtlijn breidt het toepassingsgebied uit, herziet het regelgevingsysteem van de oorspronkelijke NIS-richtlijn en introduceert strengere beveiligingseisen en rapportagevereisten voor een breed scala aan sectoren en bedrijven.

Als gevolg van de herstructurering van het toepassingsgebied, de verlaging van de drempels en het opnemen van nieuwe sectoren zijn aanzienlijk meer ondernemingen onderworpen aan de NIS2-richtlijn dan aan de NIS-richtlijn. Elke organisatie dat kritieke diensten levert of een aanzienlijk maatschappelijk belang heeft, valt onder de nieuwe, strengere eisen van de NIS2-richtlijn.

Om een uniforme definitie te waarborgen en interpretatieverschillen tussen de lidstaten te voorkomen, stelt de NIS2-richtlijn duidelijke criteria voor de classificatie van organisaties vast. Het verdeelt betrokken bedrijven in **essentiële instellingen** en **belangrijke faciliteiten**.

Volgens NIS2 Art. 3 lid 1 omvatten de essentiële entiteiten onder meer middelgrote tot grote ondernemingen die kunnen worden toegewezen aan een sector die is opgenomen in NIS2 bijlage 1 (nieuw toegevoegde sectoren zijn bijvoorbeeld afvalwater, beheer van ICT-diensten en ruimte). Ongeacht de grootte van de organisatie worden onder meer gekwalificeerde verleners van vertrouwensdiensten en DNS-dienstverleners geregistreerd. Overheidsinstellingen worden ook gereguleerd als essentiële instellingen. Bovendien omvat het toepassingsgebied van de NIS2-richtlijn ook providers van bijzonder kritieke diensten, op voorwaarde dat zij door de lidstaten als een essentiële entiteit worden aangemerkt (NIS2 Art. 2 lid 2 onder b-e).

Als belangrijke entiteit omvat de NIS2-richtlijn, volgens artikel 3 lid 2, andere ondernemingen die actief zijn in een van de in Bijlage 1 of Bijlage 2 bij de NIS2-richtlijn genoemde sectoren. Bijlage 2 omvat onder meer de sectoren productie, verwerking en distributie van levensmiddelen, productie/fabricage van goederen en onderzoek. Ook hier bestaat de mogelijkheid dat de lidstaat als belangrijke instelling wordt aangemerkt.

Net als bij de NIS-richtlijn is de verplichting om technische en organisatorische maatregelen te nemen ook terug te vinden in de NIS2-richtlijn. Deze moeten geschikt en proportioneel zijn en moeten, om een risicoadequaat veiligheidsniveau te waarborgen (NIS2 Art. 21 lid 1), naast de relevante Europese en internationale normen en de implementatiekosten ook rekening houden met de stand van de techniek.

Voor het eerst zijn (NIS2 Art. 21 lid 2) minimumeisen voor risicobeheersmaatregelen in detail gespecificeerd Ook is, om potentiële kwetsbaarheden bij externe leveranciers te minimaliseren, meer aandacht voor de beveiliging van de toeleveringsketen.

Bovendien moeten veiligheidsincidenten met aanzienlijke gevolgen onmiddellijk worden gemeld aan de bevoegde autoriteiten (NIS2 Art. 23).

Voor een specifieke catalogus van verplichtingen wordt verwezen naar de Implementatiewet.

1.1.1.5 Wet implementatie en versterking van de cyberbeveiliging van NIS2 (NIS2UmsuCG)

De wet die nodig is om de NIS2-richtlijn (voor Duitsland) ten uitvoer te leggen bestaat momenteel niet. In juli 2024 publiceerde het federale ministerie van Binnenlandse Zaken een conceptwetsvoorstel voor de "NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz" (NIS2UmsuCG).

In wezen voorzag de NIS2UmsuCG in een volledige vernieuwing van de BSiG, die een nieuwe regelgevende structuur en een aanzienlijke uitbreiding van het toepassingsgebied moest ondergaan.

Door het ontwerp van de nieuwe BSiG (BSiG-E) werden de voorwaarden van de NIS2-richtlijn niet overgenomen, in plaats daarvan werd een onderscheid werd gemaakt tussen **bijzonder belangrijke instellingen** en **belangrijke instellingen**; door de BSiG-E vallen daar ook onder **instellingen van de federale overheid**. In totaal wordt het aantal organisaties dat door het implementatieontwerp in Duitsland wordt getroffen, geschat op meer dan 30.000.

Naast een aanzienlijke uitbreiding van het toepassingsgebied voorzag de BSiG-E ook in een uitgebreid programma van verplichtingen voor de geadresseerde bedrijven: Bij de uitvoering van de NIS2-richtlijn zijn bedrijven verplicht de bovengenoemde risicobeheersmaatregelen te nemen en moeten ze voldoen aan de stand van de techniek. Volgens de BSiG-E moeten providers van kritische installaties, als subgroep van bijzonder belangrijke installaties, voldoen aan nog strengere eisen op het gebied van risicobeheersmaatregelen. Verder voorziet de BSiG-E in een gedetailleerd rapportagesysteem, registratieverplichtingen, informatieverplichtingen, bewijsverplichtingen en implementatie-, monitoring- en trainingsverplichtingen voor het management.

Het Duitse Federale Bureau voor Informatiebeveiliging (BSI) zal als toezichthoudende autoriteit een centrale rol op zich nemen en zal verantwoordelijk zijn voor een groot aantal nieuwe organisaties. De BSiG-E versterkt de bevoegdheden van de BSI, met name met betrekking tot registratie- en rapportageverplichtingen en de handhaving van beveiligingsnormen.

Naast de NIS2UmsuCG is de invoering van een overkoepelende wet KRITIS gepland, die bedoeld is om de veerkracht en het bedrijfscontinuïteitbeheer (BCM) voor providers van kritieke installaties te reguleren. Deze wet heeft tot doel de fysieke veiligheid en veerkracht van kritieke infrastructuur te vergroten.

Noch de NIS2UmsuCG, noch de overkoepelende wet KRITIS werden uiteindelijk door de verkeerslichtregering geïmplementeerd. Op het moment van publicatie van deze hand-out valt nog te bezien of en welke wijzigingen toekomstige uitvoeringswetten zullen aanbrengen in de eerdere ontwerpen.

1.1.2 Andere Europese rechtsbronnen

1.1.2.1 General Data Protection Regulation (GDPR)

In 2016 werd de Europese Algemene GDPR aangenomen en is uiteindelijk op 25.05.2018 in werking getreden. Het primaire doel van de GDPR is het beschermen van de persoonsgegevens van Europese burgers. De verordening is gebaseerd op een op risico's gebaseerde benadering met betrekking tot de beschermingsdoelstellingen.

Op verschillende plaatsen van de GDPR is de stand van de techniek van bijzonder belang.

Volgens GDPR Art. 25 moeten de beginselen van gegevensbescherming worden nageleefd door technisch ontwerp (privacy by design) en door standaard instellingen voor de gegevensbescherming (privacy by default). Deze beginselen moeten door middel van op risico's afgestemde en passende technische en organisatorische maatregelen worden toegepast.

Op het gebied van de technische gegevensbescherming moeten, om de rechten en vrijheden van natuurlijke personen te beschermen, in overeenstemming met GDPR Art. 32 lid 1 passende technische en organisatorische maatregelen worden genomen.

In het kader van zowel GDPR Art. 25 lid 1 en GDPR Art. 32 lid 1 moet bij de te nemen technische en organisatorische maatregelen rekening worden gehouden met verschillende aspecten:

- Waarschijnlijkheid van optreden en ernst van het risico op schending van rechten door de betrokkene
- Type, omvang, omstandigheden en doel van de verwerking
- Implementatiekosten
- Modernste stand van de techniek

Net als de IT-beveiligingswetgeving geeft de GDPR geen definitie van wat wordt bedoeld met state-of-the-art. Hetzelfde geldt voor de EU-wet tot wijziging en implementatie van gegevensbescherming (DSAnpUG-EU) en de daaruit voortvloeiende nieuwe versie van de federale wet op de gegevensbescherming (BDSG).

Bij de uitvoering van de specificaties moet echter niet alleen rekening worden gehouden met de stand van de techniek, maar ook uitgebreid worden gedocumenteerd. Daartoe zijn verregaande documentatieverplichtingen in het leven geroepen, met name door de verplichting om een gegevensbeschermingseffectbeoordeling en verantwoordingsplicht uit te voeren. In dit verband bepaalt de verordening documentatieverplichtingen als afzonderlijke wettelijke verplichtingen. Daarom moeten technische en organisatorische maatregelen individueel worden bepaald en in detail worden beschreven en gedocumenteerd.

1.1.2.2 Digital Operational Resilience Act (DORA)

De Digital Operational Resilience Act van 14 december 2022 is een verordening van de Europese Unie die tot doel heeft de digitale operationele weerbaarheid in de financiële sector te versterken. Naast de in DORA Art. 2 lid 1 opgesomde "financiële ondernemingen" (kredietinstellingen, betalingsinstellingen, handelsplatformen, verzekeringsondernemingen, enz.) is het ook van toepassing op derden aanbieders van ICT-diensten voor die financiële ondernemingen. De bedrijven die door de DORA werden getroffen moesten de vereisten uiterlijk op 17 januari 2025 volledig implementeren.

De DORA voorziet in een uitgebreide catalogus van verplichtingen. Naast gedetailleerde verplichtingen om een kader voor ICT-risicobeheer uit te voeren, met inbegrip van strategieën, procedures, protocollen en instrumenten om de bescherming van ICT-activa te waarborgen (DORA Art. 5 e.v.) zijn er ook speciale verplichtingen op het gebied van beheer, monitoring, rapportage en registratie voor de behandeling van ICT-gerelateerde incidenten (DORA Art. 17 e.v.), verplichtingen inzake weerbaarheidtests (DORA Art. 24 e.v.) en verplichtingen om ICT-risico's van derden aanbieders te beheren, met inbegrip van het bijhouden van een informatieregister (DORA Art. 28 e.v.).

De stand van de techniek wordt niet expliciet als juridische term genoemd in de DORA, het wordt echter geïntroduceerd door niet-gedefinieerde juridische termen: bijvoorbeeld door de vereisten van "juiste en adequate" bescherming van ICT-activa (DORA Art. 6 lid 2).

1.1.2.3 Harmonised rules on artificial intelligence and amending Regulations (AI-verordening)

Met de AI-verordening van 13 juni 2024 heeft de Europese Unie voor het eerst de ontwikkeling, de handel en het gebruik van artificiële intelligentie gereguleerd. Het heeft tot doel de gezondheid, de veiligheid en de grondrechten te beschermen tegen de schadelijke effecten van AI-systemen en tegelijkertijd de innovatie op het gebied van AI te versterken door middel van een geharmoniseerd Europees rechtskader. De AI-verordening hanteert ook een op risico's gebaseerde aanpak. Terwijl AI-systemen met een onaanvaardbaar risico over het algemeen verboden zijn (AI-verordening Art. 5) zijn AI-systemen met een hoog risico aan strenge eisen onderworpen (AI-verordening Art. 6 e.v.). AI-systemen met een beperkt risico zijn daarentegen onderworpen aan louter transparantieverplichtingen (AI-verordening Art. 50). Grotendeels risicovrije AI-systemen kunnen vrijwillig bepaalde vereisten en gedragscodes vaststellen (AI-verordening Art. 95). De AI-verordening is gericht op een groot aantal verschillende actoren, van wie sommige onderworpen zijn aan overlappende en soms verschillende verplichtingen (aanbieders, exploitanten, importeurs, distributeurs, gemachtigde vertegenwoordigers).

Naast AI-systemen worden ook General-Purpose AI Models (GPAI-modellen) gereguleerd door de AI-verordening, waarbij GPAI-modellen met systeemrisico aan strengere eisen moeten voldoen (AI-verordening Art. 51 e.v.).

De stand van de techniek is te vinden op verschillende plaatsen van de AI-verordening: Bij het voldoen aan de vereisten voor AI-systemen met een hoog risico moet rekening worden gehouden met de algemeen aanvaarde stand van de techniek met betrekking tot AI en AI-gerelateerde technologieën (AI-verordening Art. 8 lid 1). Overeenkomsten tussen aanbieders van AI-systemen met een hoog risico en derden in de waardeketen moeten ondersteuningsverplichtingen bevatten in overeenstemming met de algemeen aanvaarde stand van de techniek. Met betrekking tot de transparantieverplichtingen uit hoofde van AI-verordening Art. 50 moeten aanbieders van AI-systemen er ook voor zorgen dat hun technische oplossingen doeltreffend, interoperabel, veerkrachtig en betrouwbaar zijn, rekening houdend met de algemeen aanvaarde stand van de techniek zoals die tot uitdrukking kan komen in de relevante technische normen. Hier is dus, bij wijze van uitzondering, een lichte concretisering van de term. Ten slotte is de stand van de techniek te vinden in de verplichtingen van aanbieders van GPAI-modellen met systeemrisico: De modelbeoordeling van aanbieders overeenkomstig AI-verordening Art. 55 lid 1a moet

worden uitgevoerd met behulp van gestandaardiseerde protocollen en instrumenten die overeenstemmen met de stand van de techniek. De stand van de techniek wordt ook vaak in de overwegingen weerspiegeld.

De AI-verordening laat dus op indrukwekkende wijze zien hoe belangrijk de stand van de techniek is als juridische term om de dynamische ontwikkelingen van nieuwe technologieën op een juridisch effectieve manier vast te leggen.

1.1.2.4 European Union Cybersecurity Certification Scheme for Cloud Services (EUCS)

Daarnaast werkt de Europese Unie samen met het European Union Cybersecurity Certification Scheme for Cloud Services aan een uniform certificeringkader voor clouddiensten, gebaseerd op EU-verordening 2019/881 (Cybersecurity Act). Het doel is om de betrouwbaarheid en transparantie van het cloudaanbod in heel Europa te vergroten door middel van geharmoniseerde beveiligingscertificering, vooral in de publieke sector en in gereguleerde markten. De EUCS voorziet in drie veiligheidsniveaus (basis, substantieel en hoog), waarvan de eisen nauw aansluiten bij de stand van de techniek. Zodra het EUCS in werking treedt, zal het, ook met betrekking tot de stand van de techniek en de betrouwbaarheid van verwerkingspaden, een belangrijk nalevingonderdeel zijn voor aanbieders die bijvoorbeeld kritieke infrastructuur, overheidsinstanties of gezondheidszorg bedienen.

1.1.2.5 Europese ruimte voor gezondheidsgegevens (EHDS)

Met EU-verordening 2025/327 betreffende de Europese ruimte voor gezondheidsgegevens (EHDS) creëert de EU ook een regelgevend kader voor het grensoverschrijdend gebruik van elektronische gezondheidsgegevens. De EHDS stelt hoge eisen aan technische beveiliging, interoperabiliteit en toegangscontrole. Bij het ontwerp van platforms, toegangsinfrastructuren en opslagoplossingen moet rekening worden gehouden met de stand van de techniek en zal naar verwachting in uitvoeringshandelingen worden gespecificeerd. Voor aanbieders en exploitanten in de IT-omgeving van de gezondheidszorg is de EHDS, vooral in interactie met de GDPR en sectorale beveiligingswetten, van strategisch belang.

1.1.3 Andere nationale rechtsbronnen

- **Energiewirtschaftsgesetz (EnWG):** EnWG § 11 voorziet in verschillende IT-beveiligingsverplichtingen voor beheerders van energiesystemen en energievoorzieningnetwerken. De eisen hebben voorrang op de meer algemene BSiG § 8a, vgl. BSiG § 8d lid 2 Nr. 2. Naast registratie- en rapportageverplichtingen en de verplichting om een beveiligingscatalogus in te voeren, omvat de verplichtingencatalogus ook de verplichting om risicogeschikte systemen te gebruiken voor het opsporen van aanvallen, om bedreigingen voortdurend te identificeren en te vermijden en opgetreden fouten te verhelpen. Ook de stand van de techniek moet worden nageleefd. Het gebruik van dergelijke systemen moet ook regelmatig worden aangetoond.
- **Atom gestetz (AtomG):** AtomG Art. 44b bevat een speciale bepaling met betrekking tot IT-beveiliging. De norm voorziet in een bijzondere meldingsplicht in geval van aantasting van de IT-systemen van de exploitanten van nucleaire installaties als deze kunnen leiden of hebben geleid tot een dreiging of verstoring van de nucleaire veiligheid.
- **Sozialgesetzbuch (SGB V) Fünftes Buch):** Met SGB V § 393, die op 01.07.2024 werd ingevoerd, werden IT-beveiligingeisen voor de verwerking van gezondheids- of sociale gegevens in de cloud ingevoerd. Voorwaarde hierbij is dat er passende technische en organisatorische maatregelen zijn genomen om de informatiebeveiliging te waarborgen in overeenstemming met de stand van de techniek.
- **Telekommunikationsgesetz (TKG):** TKG Art. 165 voorziet onder meer in een verplichting voor providers van openbare communicatienetwerken en openbaar toegankelijke telecommunicatiediensten om technische en organisatorische voorzorgsmaatregelen te nemen om telecommunicatie- en gegevensverwerkingsystemen te beschermen tegen interferentie en risico's. Ook hier moet rekening worden gehouden met de stand van de techniek (TKG § 165 lid 2 zin 3).
- **Das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG):** Volgens TDDDG § 19 IV moeten aanbieders van digitale diensten, in het kader van wat technisch mogelijk en economisch redelijk is, door middel van technische en organisatorische voorzorgsmaatregelen ervoor zorgen dat de technische faciliteiten die zij gebruiken om hun digitale diensten aan te bieden, voldoende worden beschermd tegen ongeoorloofde toegang en verstoringen. Er moet rekening worden gehouden met de stand van de techniek.

- **Geschäftsgeheimnisschutz-Gesetz (GeschGehG):** De GeschGehG beschermt houders van bedrijfsgeheimen tegen ongeoorloofde verkrijging, gebruik en openbaarmaking ervan. Informatie kan echter alleen als bedrijfsgeheim worden aangemerkt als de rechtmatige eigenaar deze aan passende geheimhoudingsmaatregelen heeft onderworpen. Welke geheimhoudingsmaatregelen passend zijn, hangt af van de omstandigheden van het individuele geval. De eigenaar van het geheim heeft de mogelijkheid om organisatorische, technische en juridische maatregelen te nemen om het geheim te beschermen. In het kader van toepasselijkheid, als juridisch in te vullen term, kan opnieuw rekening worden gehouden met de stand van de techniek.

1.2 Branchespecifieke beveiligingsstandaarden (B3S)

Volgens BSiG § 8a lid 2S. 1 kunnen providers van kritieke infrastructuren en hun brancheorganisaties, om aan de eisen te voldoen, branchespecifieke veiligheidsnormen (B3S) aan de BSI voorstellen. De BMI maakt vervolgens een proeve van bekwaamheid[1].

De B3S zijn bedoeld om organisaties in de betreffende branche te helpen bij het aantonen van de juiste beveiligingsmaatregelen. Het gebruik van B3S verandert niets aan de reikwijdte en andere vereisten voor de selectie en het onderhoud van IT-beveiligingsmaatregelen.

Daarom moeten in de branchespecifieke veiligheidsnormen ook specifieke bepalingen worden opgenomen hoe de stand van de techniek permanent op een wettelijke manier als een doelverplichting wordt ingevuld. Daarom zijn in de branchespecifieke veiligheidsnormen ook concreet te treffen bepalingen opgenomen, hoe op de lange termijn en op een wettelijke manier aan de stand van de techniek moet worden voldaan. De B3S voorzien hier echter meestal niet in.

De meeste B3S zijn niet beschikbaar voor het grote publiek.

1.3 Evenredigheid van de maatregelen

De wetgeving vereist dat geselecteerde gebruikersgroepen voldoen aan of rekening houden met de stand van de techniek op het gebied van informatiebeveiliging[2]. Wat betreft de selectie van specifieke veiligheidsmaatregelen en de criteria op basis waarvan deze moeten worden geselecteerd, blijft de wetgeving echter begrijpelijkerwijs vaag. Het maakt het echter mogelijk om de selectie van beveiligingsmaatregelen adequaat te maken. Concreet betekent dit dat de gebruikende bedrijven de beveiligingsmaatregelen mogen selecteren op basis van economische aspecten.

De beveiligingsmaatregelen moeten worden geselecteerd in het kader van een risicobeoordeling. Vastgestelde grondslagen hiervoor zijn bijvoorbeeld de bepaling van de beschermingsbehoeften in overeenstemming met BSI IT-Grundschutz en de analyse van de beschermingsbehoeften in overeenstemming met ISO 27001ff. Deze hand-out kan dienen als bron van ideeën voor de selectie van veiligheidsmaatregelen.

Ook al is het wettelijk toegestaan om bij de selectie van de uit te voeren beveiligingsmaatregelen rekening te houden met de economische geschiktheid ervan, toch moet ook rekening worden gehouden met de efficiëntie en effectiviteit van reeds bestaande beveiligingsmaatregelen. Het is essentieel ook te kijken naar de eigen infrastructuur, applicatielandschap, bedrijfsprocessen, dreigingsituatie en al aanwezige beveiligingsmaatregelen die al in de organisatie van kracht zijn.

Vanwege deze complexiteit is het individuele onderzoek naar de geschiktheid van de beveiligingsmaatregelen in deze hand-out achterwege gelaten.

[1] Overzicht van branchespecifieke B3S bij BSI: www.bsi.bund.de

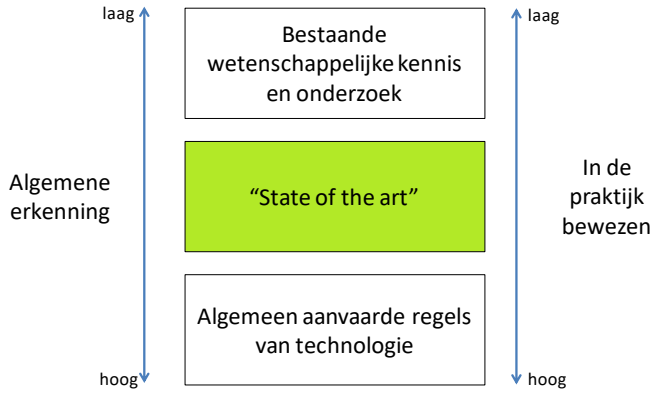
[2] In de wetgeving wordt vaak alleen schriftelijk naar IT-beveiliging verwezen. Rekening houdend met de gespecificeerde beschermingsmaatregelen in termen van inhoud, moet het toepassingsgebied echter breder worden gedefinieerd. Daarom wordt informatiebeveiliging in deze hand-out als een overkoepelend onderwerp beschouwd.

2 Bepaling van de stand van de techniek

2.1 Verduidelijking van de voorwaarden

De state-of-the-art stand van de techniek[3] moet worden onderscheiden van soortgelijke termen zoals de "algemeen aanvaarde regels van de techniek" (hierna "aaRT" genoemd) en de "stand van wetenschap en onderzoek" (hierna SdW[4]). Dit onderscheid is de essentiële basis voor het bepalen van het vereiste technologieniveau. Zoals uit vele praktijkvoorbeelden blijkt, worden deze drie termen zowel in de jurisprudentie als in de publieke opinie vermengd of zelfs verward[5].

Deze drie termen werden geïntroduceerd met de Kalkar-besluit[6] van het Federale Constitutionele Hof in 1978 en de bijbehorende "driestappentheorie". Op basis van deze beslissing kunnen de drie technologie-statussen grafisch ongeveer als volgt worden weergegeven:



Afbeelding 1: Driestappentheorie volgens het Kalkar-besluit

Het stand van de techniek niveau bevindt zich tussen de meer innovatieve " stand van wetenschap en onderzoek " en de beproefde "Algemeen erkende regels van de techniek" (SdT). Deze drie technologiestanden worden geflankeerd door de categorieën "algemene erkenning in de praktijk" en "proeftijd in de praktijk".

Vanwege het systeem van de wetten is een duidelijk onderscheid tussen subjectieve en objectieve elementen van het misdrijf vereist. Het kenmerk state-of-the-art moet puur objectief en technisch worden opgevat. De subjectieve aspecten houden rekening met de wetten in de specifieke feiten van het geval. Ze hebben echter geen betrekking op de definitie van de state-of-the-art zelf.

De "stand van de techniek" kan dus worden omschreven als de processen, faciliteiten en werkingswijzen die beschikbaar zijn bij het verkeer van goederen en diensten en waarvan de toepassing de verwezenlijking van de respectieve doelstellingen van rechtsbescherming daadwerkelijk kan waarborgen[7].

Kort gezegd betekent het dat de state-of-the-art verwijst naar de beste prestaties van een IT-beveiligingsmaatregel die op de markt beschikbaar is om het wettelijke IT-beveiligingsdoel te bereiken. Technisch gezien wordt onder topprestaties met name de efficiëntie en effectiviteit van veiligheidsmaatregelen verstaan.

---

[3] De term "technologieniveau" wordt gebruikt als vervanging voor "stand van de technologie".
[4] "Stand van Wetenschap en Technologie" kan als vervanging worden gebruikt. Om een conceptueel onderscheid met de State-of-the-art mogelijk te maken, wordt in deze hand-out consequent de term "Stand van Wetenschap en Onderzoek gebruikt.
[5] Dr. Mark Seibel, Richter am OLG, www.podium.dthgev.de/was-bedeutet-stand-der-technik
[6] BVerfGE, 49, 89 [135 f]
[7] Bartels / Backer, Die Berücksichtigung des Stands der Technik in der GDPR, DuD 4-2018, 214; Bartels / Backer / Schramm, Der "Stand der Technik" im IT-Sicherheitsrecht, Tagungsband zum 15. Deutschen IT-Sicherheitskongress 2017, Bundesamt für Sicherheit in der Informationstechnik, 503.

Het gebruik van de term "stand van de techniek" in de wetgeving versterkt de veronderstelling dat het om een zeer concrete maatregel gaat. In de praktijk is er echter niet één maatregel die overeenkomt met de state-of-the-art en andere niet. Afhankelijk van de behoefte aan bescherming en de dreiging kunnen er veel oplossingen en bundels van maatregelen zijn die als state-of-the-art kunnen worden beschouwd.

Technische maatregelen in de fase "stand van wetenschap en onderzoek" zijn zeer dynamisch in hun ontwikkeling en gaan over naar de State-of-the-art fase wanneer ze op de markt komen. Niettemin kunnen nieuwe en innovatieve producten vaak "kinderziektes" hebben die met strakke tussenpozen moeten worden opgelost en die van invloed zijn op de effectiviteit van de maatregel.

Bij toenemende standaardisatie neemt de dynamiek af. Technische maatregelen in het stadium van "algemeen aanvaarde technologische regels" zijn ook op de markt beschikbaar. Hun innovatiegraad neemt af, ze zijn wijdverbreid in de praktijk en worden vaak beschreven in de bijbehorende normen. Deze maatregelen zijn niet, alleen maar omdat ze zich al lange tijd op de markt hebben bewezen, per se slecht, ze kunnen echter zwakke punten hebben omdat de aanvallers een manier kunnen hebben gevonden om hun beschermingsmechanismen te omzeilen. Soms zijn gerichte aanpassingen echter voldoende om het gewenste beschermende effect te herstellen.

Hoewel de overgang van "stand van wetenschap en onderzoek" naar "Stand van de Techniek" relatief gemakkelijk te identificeren is door markttoetreding, is het onderscheid tussen state-of-the-art en "algemeen aanvaarde technologische regels" nogal moeilijk. In het geval van technische maatregelen zijn het vaak nieuwe versies van een beveiligingsoplossing of software in het kader van een product-levenscyclus die duidelijk gelokaliseerd zijn. Als het echter gaat om organisatorische maatregelen, zijn het vaak geschreven normen die elders worden aangeduid als "best practice". Ze hebben zich in de praktijk bewezen en zijn nauwelijks onderhevig aan methodologische modernisering.

Er zijn ook maatregelen die op de markt beschikbaar zijn, ook al is door experts de erkenning daarvan in termen van hun effectiviteit afgenomen. Dit is bijvoorbeeld het geval bij maatregelen die in het gedrang zijn gekomen. Maatregelen die zich aan het einde van hun productlevenscyclus bevinden (eol in PLC) en niet langer worden ondersteund door de fabrikant, behoren ook tot deze categorie. Dergelijke maatregelen mogen niet langer worden gebruikt, omdat hun kwetsbaarheden gemakkelijk door de aanvaller kunnen worden misbruikt.

Als gevolg van de vooruitgang kan een verschuiving worden waargenomen tussen de afzonderlijke technologieniveaus ("innovatiegerelateerde verschuiving"):

1. Een maatregel zal in eerste instantie, in zijn oorsprong, het technologische niveau van "stand van wetenschap en onderzoek" bereiken;
2. bij de marktintroductie wordt het State-of-the-art;
3. en met de toenemende verspreiding en erkenning op de markt zal het uiteindelijk worden toegewezen aan de "algemeen aanvaarde regels van de techniek".
4. Bij verlies van erkenning kan de maatregel niet meer worden gebruikt.

Om het vereiste bewijs te leveren nadat de eigen maatregelen zijn afgestemd op de stand van de techniek, is het niet voldoende om de geïmplementeerde maatregelen één keer te evalueren en door het installeren van patches bij te werken. Dit bewijs kan alleen worden geleverd door de gebruikte maatregel regelmatig en volgens een transparante methode te vergelijken met de op de markt beschikbare alternatieven.

2.2 Methode voor het classificeren van de stand van de techniek

De maatregelen die in deze hand-out worden beschreven zijn beoordeeld aan de hand van een werkbare methodologie, die is gebaseerd op een eenvoudig principe van het beantwoorden van belangrijke vragen over de dimensies "erkenning door deskundigen" en "proeftijd in de praktijk". De gebruikte richtinggevende vragen zijn bewust op een eenvoudige manier geformuleerd en maken een gedetailleerder beeld mogelijk van de twee dimensies van het onderzoek.

Op elke kernvraag werden drie mogelijke antwoorden gegeven. De antwoorden zijn zo geselecteerd dat ze classificatie in een van de drie technologieniveaus mogelijk maken. Elk antwoord moet ook worden gemotiveerd. Hoewel de afzonderlijke vragen indeling in een van de drie technologieniveaus mogelijk maken, hebben ze elk slechts betrekking op deelaspecten en daarom wordt het technologieniveau van een maatregel pas bepaald nadat alle vragen van beide dimensies zijn beantwoord.

De volgende tabel geeft een overzicht van de criteria die door de AK-SdT worden gehanteerd en de interpretatie daarvan voor de evaluatie van de stand van de maatregelen

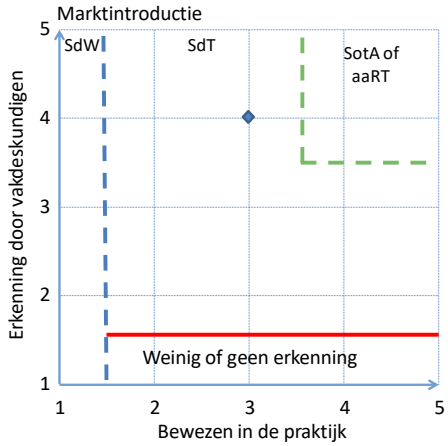
- **Mate van technologische erkenning**

Beoordelingscriterium	Specificatie van het beoordelingscriterium
Welke **documentatie** over de maatregel is openbaar beschikbaar?	Uitsluitend wetenschappelijke publicaties getuigen van een lage mate van maturiteit en een hoge mate van innovatie. Aan de andere kant wijst een sterke aanwezigheid in de massamedia op algemene regels van de techniek. Vakmedia zijn actuele onafhankelijke media waarvan de inhoud gericht is op beveiligingsexperts.
Verwijst de maatregel naar nationale of internationale **normen?**	Dit gaat om de mate van standaardisatie. Als een maatregel al in kaart is gebracht in nationale en internationale normen (ISO/IEC 27001ff, NIST, ENISA) of catalogi van maatregelen (BSI, TR, BSI, IT-GS), dan wordt deze toegewezen als algemeen aanvaarde regels van de techniek. Voor de toepassing van dit document wordt het woord "set of rules" gelijkgesteld met het woord "norm".
Is de maatregel **aanbevolen** door nationale en internationale commissies / verenigingen?	Nationale commissies zijn beroepsverenigingen (TeleTrusT, Bitkom, VDE, enz.), maar ook regelgevers (BSI, BNetzA, enz.). Internationale instanties zijn bijvoorbeeld ENISA, NIST, enz. Als een maatregel nog niet is aanbevolen door commissies, wordt aangenomen dat deze nog onbekend is. Als het daarentegen een maatregel is die door veel commissies is aanbevolen, geniet deze in professionele kringen een hoge mate van erkenning.
Wordt de conceptuele geschiktheid van de maatregel onafhankelijk **gecontroleerd**?	Als de geschiktheid van de maatregel regelmatig door een onafhankelijke instantie (zoals TÜV, DEKRA, BSI, experts) wordt gecontroleerd, moet deze een hoog niveau van volwassenheid hebben bereikt en is daarom toegewezen aan de algemeen aanvaarde regels. Als de geschiktheid van een maatregel nog niet onafhankelijk is geverifieerd, is er onvoldoende standaardisatie en wordt deze vaak meegeteld als onderdeel van de "stand van wetenschap en onderzoek".

- **Mate van proeftijd in de praktijk**

Beoordelingscriterium	Specificatie van het beoordelingscriterium
Hoe moet de mate van **innovatie** van de maatregel worden geclassificeerd?	Een maatregel die efficiëntie bij de detectie of behandeling van bedreigingen verhoogt of nieuwe benaderingen (innovatief) introduceert bij de detectie en behandeling van bedreigingen, moet worden geclassificeerd als een "stand van wetenschap en onderzoek".
Waar is de huidige versie van de maatregel **getest**?	Meestal zijn de maatregelen die wij overwegen bedoeld voor professioneel gebruik. Het doel is hier om een onderscheid te maken tussen een maatregel die nog in ontwikkeling is en een maatregel die al op de markt kan worden aangeschaft.
Zijn er **vergelijkbare** maatregelen op de markt waarmee het vereiste doel effectiever of efficiënter kan worden bereikt?	Als er geen vergelijkbare maatregelen zijn die efficiënter of effectiever zijn, is de kans groter dat de maatregel wordt geclassificeerd als "stand van wetenschap en onderzoek". Aan de andere kant, als er veel alternatieven (maatregelen of bundels van maatregelen) zijn om hetzelfde doel te bereiken, spreekt dit meer in het voordeel van de algemeen aanvaarde regels van de techniek.
Hoe vaak wordt de maatregel **conceptueel bijgewerkt**?	Maatregelen met een hoge mate van volwassenheid worden minder snel conceptueel bijgewerkt. Anderen daarentegen moeten vaker worden aangepast aan de omstandigheden.

Op basis van een puntensysteem (1-5) wordt uitgaande van de gegeven antwoorden een gemiddelde waarde gevormd. Aan de hand van de vastgestelde waarden kan de maatregel in de volgende grafiek worden ingedeeld:



Afbeelding 2: Voorbeeld van de classificatie van de stand van de techniek

De grafiek hierboven toont de beschreven technologieniveaus ""stand van wetenschap en onderzoek", "stand van zaken" en "algemeen aanvaarde Regels van de Techniek".

De "stand van wetenschap en onderzoek" moet links van de markttoetreding worden geplaatst, maar kan zich vanwege mogelijke herkenning door experts uitstrekken over de gehele Y-as.

Als we uitgaan van de hierboven beschreven definitie van "stand van de techniek", wordt onder "stand van wetenschap en onderzoek" verstaan de processen, faciliteiten en werkingswijzen waarvan de toepassing kan bijdragen tot het bereiken van de respectieve doelstellingen van de rechtsbescherming, maar waarvan het effect nog niet in de praktijk is getest.

Dergelijke maatregelen worden bij het betreden van de markt overgebracht naar stand van de techniek. Zij zijn vooruitstrevend en kunnen het meest doeltreffend zijn om de verwezenlijking van de respectieve doelstellingen van rechtsbescherming te waarborgen.

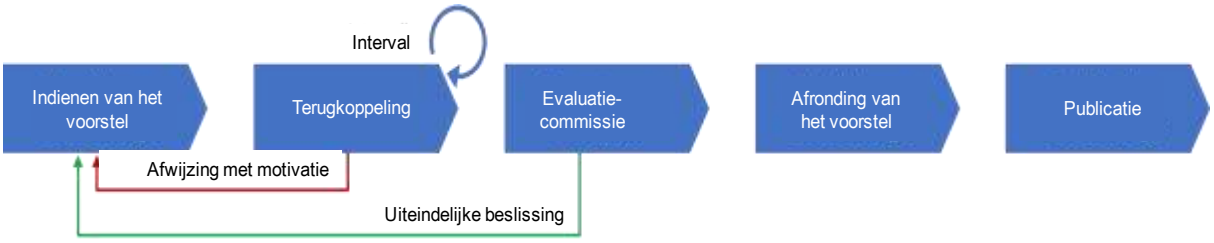
Met toenemende standaardisatie wordt de classificatie van de maatregel naar rechtsboven verschoven. Er zijn beproefde, gestandaardiseerde maatregelen die voldoende zijn om de wettelijke doelstellingen te halen. Ze vormen vaak het basiskader van IT-beveiliging, maar lopen het risico te worden vervangen door meer geavanceerde, efficiënte en effectieve maatregelen. Hun herkenning kan snel omslaan, waardoor ze onderaan in de grafiek komen te staan ("geen of nauwelijks erkenning").

Deze hand-out beschrijft technologieën en maatregelen en classificeert ze volgens de hierboven beschreven methode. Beveiligingsproducten worden niet in de strikte zin beschreven, daarom wordt bijvoorbeeld aangenomen dat de geschiktheid van de hier beschreven maatregelen voor het betreffende doel is vervuld en niet van geval tot geval verder wordt gevalideerd.

In de praktijk van het bedrijfsleven kan een geschikte methode (zoals vergelijkbaar met de hier geschetste), om de gebruikte maatregelen objectief te evalueren, worden aangepast aan de bestaande omstandigheden van de organisatie, te vergelijken met alternatieven en te documenteren voor verificatiedoeleinden.

2.3 Proces voor kwaliteitsborging van de hand-out

De AK-SdT streeft naar een hoge kwaliteit van de inhoud van deze hand-out, om dit te laten slagen is in de AK-SdT een proces vastgelegd waarin de bijdragen verschillende fasen succesvol moeten doorlopen:



Afbeelding 3: Processchets voor de evaluatie van de maatregelen in de werkgroep

Na het indienen van een nieuwe of gewijzigde bijdrage in een gestandaardiseerd sjabloon (zie afbeelding 3), wordt de bijdrage geëvalueerd door IT-beveiligingexperts via een evaluatieplatform met behoud van anonimiteit.

De resultaten die in dit proces worden bereikt, worden besproken en uiteindelijk gestemd door het evaluatiecomité[8] van de AK-SdT, die regelmatig bijeenkomt. Tot de beoordelingscriteria behoren de in het sjabloon gedefinieerde richtinggevende vragen en hun antwoorden, maar ook de technische juistheid en actualiteit van de inhoud.

Als de beoordelingscommissie tot de conclusie is gekomen dat een bijdrage niet de vereiste kwaliteit behaalt, wordt de opname in de hand-out om gemotiveerde redenen afgekeurd en wordt de auteur hiervan op de hoogte gesteld. De auteur heeft dan de mogelijkheid om zijn bijdrage bij te werken of aan te vullen en ter beschikking te stellen voor heronderzoek.

Bijdragen die deze uitgebreide procedure met succes doorstaan, worden in de hand-out opgenomen.

[8] Een lijst van de actieve leden van de werkgroep (evaluatiecommissie) zal worden gepubliceerd op de website van de werkgroep: https://www.teletrust.de/arbeitsgremien/recht/stand-der-technik/

2.4 Vereiste beschermingsdoelen

IT-beveiliging streeft verschillende beschermingsdoelen na om informatie en systemen te beschermen tegen bedreigingen. De drie basisbeschermingsdoelstellingen[9], die ook wettelijk verplicht zijn, zijn:

- **Beschikbaarheid**
  Van beschikbaarheid van informatietechnologiesystemen en -componenten is sprake als ze altijd kunnen worden gebruikt in overeenstemming met hun doel en functiebereik. Om de beschikbaarheid te garanderen, moet rekening worden gehouden met de categorieën fouttolerantie, betrouwbaarheid, robuustheid en herstelbaarheid.

- **Integriteit**
  De integriteit van de verwerking is gewaarborgd als er geen onbedoelde en onopgemerkte wijzigingen in de gegevens optreden. Om de integriteit te waarborgen, moet ook rekening worden gehouden met de categorieën consistentie, nauwkeurigheid, correctheid en volledigheid.

- **Vertrouwelijkheid**
  Geheimhouding is geboden als de beschermwaardige gegevens alleen op de toegestane manier ter beschikking worden gesteld van de bevoegde personen.

Naast deze door de IT-SiG nagestreefde doelstellingen op het gebied van IT-beveiliging zijn er nog andere garantiedoelstellingen op het gebied van gegevensbescherming, die met name worden genoemd in het kader van de hier besproken GDPR. Dit zijn bijvoorbeeld niet-koppelbaarheid (doelbinding), transparantie van de verwerking of interveniabiliteit[10].

Deze extra doelen staan deels haaks op de eerder genoemde beschermingsdoelen van IT-beveiliging. Aangezien de wettelijke vereisten parallel van toepassing zijn, moeten bedrijven streven naar een gezamenlijke duurzame oplossing voor een hoog niveau van IT-beveiliging en gegevensbescherming. Dit kan alleen worden bereikt door samenwerking tussen de IT-beveiligings- en gegevensbeschermingsfunctionarissen.

Terwijl vanuit het oogpunt van IT-beveiliging vooral de bescherming van gegevens en infrastructuur wordt nagestreefd, gaat gegevensbescherming over de bescherming van persoonsgegevens. Het begrijpen van deze verschillende opvattingen is belangrijk om beschermende maatregelen te definiëren en dienovereenkomstig uit te voeren.

[9] Naast deze drie beschermingsdoelen is authenticiteit vaak vereist. Authenticiteit is de eigenschap van authenticiteit, verifieerbaarheid en betrouwbaarheid van informatie. Door de herkomst van de gegevens te verifiëren, kan worden aangetoond dat de informatie kan worden toegewezen aan een gespecificeerde afzender. Digitale handtekeningen maken het mogelijk om de authenticiteit van een bericht te garanderen.
[10] Op basis van het *Unabhängige Landeszentrum für Datenschutz* Schleswig-Holstein (ULD) www.datenschutzzentrum.de/

3 Technische en organisatorische maatregelen (TOM)

Talrijke wettelijke en normatieve vereisten vereisen naleving van, of op zijn minst inachtneming van de stand van de techniek op het gebied van technische en organisatorische maatregelen. Vaak is er geen verdere specificatie van de relevante systemen en componenten, om aan de stand van de techniek te voldoen, daarom moeten alle relevante componenten van de gegevensverwerking, inclusief alle opties voor gegevensoverdracht en -opslag, worden aangenomen.

Omdat IT-infrastructuren sterk afhankelijk zijn van applicaties en industrieën, is in het kader van deze hand-out een volledige lijst van de afzonderlijke componenten niet mogelijk. De auteurs hebben zich daarom gericht op de beschrijving van de essentiële componenten en processen.

3.1 Algemene opmerkingen

In de context van de Wet IT-beveiliging is het gebruik van applicaties soms heel bijzonder. Daarbij gaat het bijvoorbeeld eenvoudige, veilige e-mailcommunicatie om de besturingsfunctionaliteit in een energiecentrale te beveiligen. Om deze reden is het moeilijk om in deze publicatie een volledige lijst van applicaties op te stellen en deze applicaties ook te beschrijven. IT-beveiliging kan op verschillende manieren worden geïmplementeerd. Er is niet één alomvattende manier om een veilige architectuur te creëren, daarom moeten hier essentiële punten worden genoemd die kunnen worden opgevat als State-of-the-art in de zin van de huidige bruikbaarheid van IT-beveiliging.

De respectieve beschermingseis is afhankelijk van de betreffende applicatie. Volgens de IT-Sicherheitsgesetz moet rekening worden gehouden met de IT-beveiligingsdoelen van integriteit, authenticiteit, beschikbaarheid en vertrouwelijkheid, zelfs als deze voor het individuele imago kunnen worden beoordeeld met verschillende beschermingsvereisten. Dit betekent dat met name rekening moet worden gehouden met de volgende beschermingsdoelen:

- Bescherming tegen aanvallen voor het ongeoorloofd lezen, wijzigen en verwijderen van verzonden en opgeslagen gegevens
- Bescherming tegen aanvallen op de beschikbaarheid bij de providers en gebruikers van de respectievelijke diensten en gegevens
- Bescherming van besturings- en toepassingssystemen tegen ongeoorloofde manipulatie, enz.

Bovendien moet, naast de implementatie van passende beschermingsmaatregelen, ook de detectie van aanvallen op IT-systemen, diensten en gegevens, in overeenstemming met de stand van de techniek, worden gewaarborgd.

Bij de uitvoering moet rekening worden gehouden met de geavanceerde procedures, waarbij het gebruik van de specifieke beveiligingsmaatregel of bundel maatregelen de basis moet vormen voor een afzonderlijke analyse van de beschermingsbehoeften. Voorbeelden van beveiligingsmaatregelen zijn:

- Multi-factor authenticatie
- Wederzijdse authenticatie
- Versleuteling van communicatie tijdens transport
- Versleuteling van gegevens (zoals bij de opslag)
- Beveiliging van de private sleutel en softwarecertificaten tegen ongeoorloofd kopiëren
- Gebruik van veilige opstartprocessen
- Veilig softwarebeheer inclusief patchbeheer
- Veilig gebruikersbeheer met actieve vergrendelingsoptie
- Veilige toewijzing van netwerkzones voor extra bescherming op netwerkniveau
- Veilige datacommunicatie tussen verschillende netwerkzones
- Veilig surfen op internet
- Implementatie van het need-to-know-principe
- Implementatie van minimale toegang (inclusief hardening)
- Implementatie van logging-, monitoring-, rapportage- en responsbeheersystemen
- Implementatie van bescherming tegen malware

- Gebruik van veilige back-upsystemen om te beschermen tegen verlies van gegevens
- Redundancy van systemen voor de implementatie van hoge beschikbaarheid,
- Vertrouwelijke gegevensverwerking,
- Implementatie van het Zero Trust principe, etc.

Daarnaast moet naast de afzonderlijke technische functionaliteiten van de applicatie ook rekening worden gehouden met de gehele beveiligingsarchitectuur. Daartoe moeten de volgende punten worden beoordeeld in het kader van de voorwaarden (de BNetzA vereist een risicobeoordeling hoog als standaard of kritisch voor kritieke processen en toepassingen voor de implementatie van de IT-beveiligingscatalogus in overeenstemming met EnWG §11):

■ Het moet voor de gebruiker duidelijk zijn onder welke voorwaarden hij het betreffende systeem in de betreffende veilige configuratie kan gebruiken en implementeren. Als verschillende toepassingsscenario's op één apparaat mogelijk zijn (zoals toegang tot Office-IT via sessie 1 en toegang tot proces-IT via sessie 2, moet dit visueel betekenisvol zijn voor de gebruiker).

■ Een holistische beveiligingsarchitectuur voor het product of dienst en bijbehorende documentatie voor evaluatie door onafhankelijke derden moet bestaan en worden geïmplementeerd.

■ De gebruikte cryptografie moet modern zijn en up-to-date en veilig in kaart kunnen worden gebracht tot het einde van de levenscyclus van het product. Hiervoor beveelt de BSI aan om altijd up-to-date modules met geschikte algoritmen te gebruiken.

■ Het gebruikte product of gebruikte dienst mag geen backdoors bevatten die het mogelijk maken om gegevens en toepassingen te lezen of zelfs te manipuleren.

■ De fabrikant mag geen toegangsinterfaces hebben die onafhankelijk van de bediener kunnen worden gebruikt.

■ Het is raadzaam om de implementatie van de beveiligingsfunctie te laten controleren door vertrouwde derden.

■ De processen die in de applicatie zijn geïmplementeerd (zoals gebruikersautorisatie, sleutelbeheer, enz.) moeten betrouwbaar in kaart worden gebracht.

Om een product te beoordelen op State-of-the-art, zijn andere criteria waaraan moet worden voldaan. Dit zijn de volgende:

■ Het product of de dienst moet voldoen aan internationale normen en, waar deze worden gebruikt, interoperabel zijn met standaardprotocollen.

■ Bij de toepassing moet rekening gehouden worden met eventuele branchespecifieke normen.

■ Het product of de dienst moet een storingsvrije werking van de componenten mogelijk maken (marktgereedheid).

■ Het product of de dienst moet in de praktijk met succes beproefd zijn.

■ Bij de evaluatie moet rekening worden gehouden met het feit dat de oplossing als een eenheid moet worden beschouwd als er sprake is van een koppeling van hardware en software.

■ Het product moet veilig kunnen worden bijgewerkt op het gebied van beveiliging en applicatiefunctionaliteit.

De fabrikant van de oplossing is bij de evaluatie van de oplossing ook onderworpen aan criteria waarmee rekening moet worden gehouden bij het selecteren van de state-of-the-art implementaties. De fabrikant kan investeringszekerheid garanderen voor de betreffende implementatie. Dit betekent dat de volgende tests moeten worden uitgevoerd:

- De financiële achtergrond van de fabrikant garandeert verdere levenscycli van het product.

- Er is een vast productmanagementsysteem voor het betreffende product en, voor de gebruiksperiode door de gebruiker, een routekaart voor de verdere ontwikkeling.

- Het product is tijdens de gebruiksperiode niet bekend als product dat niet meer leverbaar is.

- De fabrikant reageert proactief op bekende kwetsbaarheden die van invloed zijn op zijn product en sluit deze op korte termijn en zorgt onmiddellijk voor de nodige software-updates.

- De fabrikant produceert de betreffende oplossing in een vertrouwde omgeving met vertrouwd personeel.

- De fabrikant beheerst de volledige beveiligingsfuncties zelfstandig en is voor de beveiligingsfuncties niet afhankelijk geworden van andere leveranciers.

Als producten van leveranciers worden gebruikt die een lager betrouwbaarheidsniveau hebben, moeten de beveiligingsarchitectuur van het product en de maatregelen in het productieproces bij de fabrikant ervoor zorgen dat, met betrekking tot de gedefinieerde beschermingsvereisten, de algehele beveiligingsarchitectuur aanwezig blijft.

3.2 Technische maatregelen

3.2.1 Authenticatie

Een gebruiker heeft alleen toegang tot bronnen in het IT-systeem als zijn identiteit is bevestigd en de rechten zijn geverifieerd. Om dit te doen, logt hij in op het systeem met zijn gebruikers-ID, die zijn identiteit verifieert op basis van factoren. Als basis voor authenticatie wordt onderscheid gemaakt tussen drie categorieën:

- Kennis (zoals wachtwoord)
- Bezit (zoals tokens)
- Biometrie (zoals vingerafdruk)

Op kennis gebaseerde factoren zijn bijvoorbeeld wachtwoord, pincode en wachtwoordzin. Idealiter bestaat een wachtwoord uit een willekeurige reeks cijfers, letters en speciale tekens. Aan de andere kant bestaat het persoonlijk identificatienummer (PIN) meestal uit een 4- of 6-cijferige reeks cijfers waarmee de gebruiker zich op een apparaat kan identificeren. Beide methoden worden meestal gebruikt in combinatie met een gebruikersnaam. In vergelijking met een wachtwoord bestaat een wachtwoordzin uit meerdere woorden of een langere, betekenisvolle tekenreeks die voor de gebruiker gemakkelijker te onthouden is, maar die door zijn grotere lengte beter bestand is tegen aanvallen.

Op bezit gebaseerde factoren zijn onder meer FIDO- en OTP-beveiligingstokens, evenals smartphones en klassieke smartcards. Beveiligingstokens worden meestal voor gebruikersaccounts gebruikt om als tweede factor extra beveiliging te bieden, vaak in de vorm van een USB-stick. Ze kunnen uniek worden toegewezen aan een gebruiker en zo worden gepersonaliseerd. Beveiligingstokens genereren een eenmalig wachtwoord (OTP), reageren op aanrakingen, of gebruiken ook een biometrische functie. De smartphone dient als een veelzijdig authenticatiemedium. Zo kan bijvoorbeeld een OTP op het apparaat worden gegenereerd via een authenticatorapplicatie.

De derde categorie authenticatiemethoden zijn biometrische factoren. Het gaat bijvoorbeeld om vingerafdruk- en irisscanners, maar ook om ader- of gezichtsherkenning, typegedrag en spraakherkenning. Hiervan hebben vingerafdrukken en gezichtsherkenning de overhand gekregen.

Een andere methode is de "Voorwaardelijke" / "Adaptieve" authenticatie. Bij deze methode wordt een authenticatiefactor eerst gecombineerd met een gedragspatroon of contextanalyse. Alleen wanneer anomalieën worden gedetecteerd, is een andere factor nodig voor verificatie.

3.2.2 Sterke wachtwoorden beoordelen en afdwingen

De maatregel voert een uitgebreide inventarisatie en evaluatie uit van alle wachtwoorden, inclusief onbekende. Hiervoor worden aanvallen op veilig opgeslagen hash-waarden van inloggegevens/wachtwoorden gesimuleerd en wordt hun objectieve veerkracht gemeten op basis van wiskundige methoden, persoonlijk gedrag, enz. De maatregel bepaalt de mate van naleving van interne bedrijfsrichtlijnen en maakt het mogelijk om beveiligingsrelevante maatregelen uit te voeren, zoals het informeren van medewerkers als onveilige wachtwoorden worden gebruikt. Dit geldt ook voor de verificatie van nieuw ingestelde wachtwoorden.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

Ongeoorloofde toegang tot gebruikersaccounts door:

- het raden van zwakke wachtwoorden door derden
- gebruik van gecompromitteerde wachtwoorden door derden

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Bedrijfsnetwerken gebruiken om gebruikers te verifiëren doorgaans een centrale opslagplaats van gebruikersgegevens (zoals Microsoft Active Directory).

Als wachtwoorden worden gebruikt voor authenticatie, worden ze niet opgeslagen in platte tekst, maar als hash-waarde van het wachtwoord. Dit is bedoeld om te voorkomen dat een aanvaller, door ongeoorloofde toegang tot wachtwoordgegevens, in het bezit komt van wachtwoorden van derden en zo toegang krijgt tot andere systemen of gebruikersaccounts. Hoewel deze hashing-functionaliteit een cruciale bescherming van wachtwoorden is tegen ongeoorloofde toegang, voorkomt het ook dat wachtwoorden worden geëvalueerd op basis van hun sterkte. Dit is echter nodig om passende maatregelen te nemen tegen mogelijke aanvallen, zoals het vergelijken van nieuw ingestelde wachtwoorden met woorden uit een woordenboek, het vergelijken ervan met bekende gecompromitteerde wachtwoorden of het raden van de wachtwoorden op basis van persoonlijke informatie over de beoogde gebruiker.

Het eerste deel van de maatregel, de wachtwoordbeveiligingbeoordeling, identificeert de veerkracht van wachtwoorden door met regelmatige tussenpozen een echte aanval te simuleren met behulp van relevante tools. Hierdoor kunnen mogelijke kwetsbaarheden zoals voorspelbare, zwakke en foutieve cryptografische implementaties worden gedetecteerd. De kerncijfers maken passende bewustmakings- en opleidingsmaatregelen mogelijk en maken de beoordeling en optimalisatie van effectiviteit ervan mogelijk.

Het tweede deel van de maatregel is het afdwingen van sterke wachtwoorden. Het dwingt het gebruik van sterke en veilige wachtwoorden af. De vereiste sterkte van elk nieuw wachtwoord wordt door middel van een reeks regels aangepast aan het beveiligingsniveau van het betreffende gebruikersaccount. Het gedefinieerde beveiligingsniveau is gebaseerd op de mogelijke impact van een beveiligingsinbreuk op dit account. Nieuw ingestelde wachtwoorden worden gecontroleerd aan de hand van een reeks regels die overeenkomen met het beveiligingsniveau en die aan elk account zijn toegewezen. Deze regels omvatten vereisten voor compositie (lengte, tekenset, symbolen, letterreeksen en herhalingen), wiskundige en structurele entropiewaarden, uniciteit (het wachtwoord mag niet worden gebruikt door een ander account op hetzelfde systeem in de organisatie), het gebruik van bekende standaardwachtwoorden en historisch hergebruik van wachtwoorden.

De regels zijn niet beperkt tot de klassieke "zwarte lijst", maar kunnen individueel worden geparametriseerd.

Gegevens in platte tekst worden op geen enkel moment opgeslagen of weergegeven. Als het wachtwoord tijdens de noodzakelijke wachtwoordwijziging is geweigerd, wordt de gebruiker hiervan met de reden op de hoogte gebracht door een individueel bericht.

Idealiter wordt deze maatregel centraal vanuit één interface gebruikt en beheerd voor alle systemen in de organisatie. Dit maakt het mogelijk om coherente, systeemoverschrijdende beleidsregels effectief van kracht te laten worden, voorkomt het meervoudige gebruik van wachtwoorden in verschillende systemen en maakt een centrale registratie van de wachtwoordgeschiedenis mogelijk.

De beschreven maatregel leidt in elk geval tot de centrale handhaving van de juiste wachtwoordsterkte en geeft de organisatie volledige controle, sturing en documentatie over de sterkte van de wachtwoorden die in de organisatie worden gebruikt. Als de maatregelen regelmatig worden toegepast, kan meetbaar worden gemaakt of de regels zoals verwacht functioneren, of dat ze, om in de hele organisatie een passende wachtwoordsterkte te bereiken, indien nodig moeten worden gecorrigeerd.

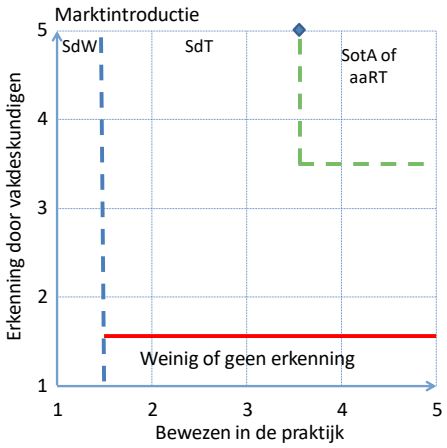
Welke beschermingsdoelen worden door de maatregel afgedekt?

☐ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Classificatie van de stand van de technologie



3.2.3 Multifactor-authenticatie

Multi-factor authenticatie (MFA) verwijst naar het bewijs en de verificatie van de identiteit van een gebruiker. Tijdens het inlogproces presenteert de gebruiker een combinatie van verschillende authenticatiemethoden (zoals wachtwoord + beveiligingstoken, wachtwoord + OTP of wachtwoord + vingerafdruk) om zijn identiteit te bewijzen (authenticatie, zie paragraaf 3.2.1), die op zijn beurt wordt gecontroleerd door een computersysteem (authenticatie).

Multi-factor authenticatie wordt hedendaags beschouwd als gevestigde standaard en moet daarom waar mogelijk worden gebruikt om identiteit in inlogprocessen te beveiligen.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

Als een systeem is beveiligd met slechts één factor (één-factor authenticatie), is de identiteit van de gebruiker onderhevig aan een verhoogd risico op

- identiteitsdiefstal
- misbruik van identiteit, en
- identiteitsfraude.

Eén factor alleen is niet voldoende om gebruikerslogins te beveiligen op computersystemen / applicaties / webapplicaties die bescherming verdienen, de methoden van digitale aanvallers worden steeds geavanceerder en de mogelijke schade als gevolg van toenemende verbindingen en voortschrijdende digitalisering wordt steeds drastischer. "Phishing", het ongeoorloofd toe-eigenen van toegangsgegevens (minstens gebruikersnaam en wachtwoord), wordt door criminelen op een dramatische manier geprofessionaliseerd. Vooral met de inzet van artificiële intelligentie zijn de bijbehorende procesmodellen (e-mailberichten, nepwebsites, etc.) de afgelopen jaren sterk geprofessionaliseerd.

- Menselijke risico's bij het omgaan met wachtwoorden:
  - Onvoldoende kwaliteit van wachtwoorden,
  - Hergebruik dezelfde wachtwoorden in verschillende applicaties,
  - Bewust wachtwoorden delen (zoals delen met andere mensen) of
  - Onbewust wachtwoorden delen (zoals opschrijven).

- Technische risico's bij de omgang met toegangsgegevens:
  - "Man in het midden" aanvallen,
  - Phishing-aanvallen, tegenwoordig sterk op AI gebaseerd en zeer professioneel
  - Keylogger-gebaseerde aanvallen,
  - Brute force aanvallen etc.
  - Beveiligingstekortkomingen in applicaties

Het gebruik van MFA-oplossingen vermindert deze risico's aanzienlijk.

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

MFA-systemen combineren meestal twee methoden uit verschillende categorieën in een authenticatieketen, hoewel sommige MFA-systemen ook de koppeling van een willekeurig aantal methoden mogelijk maken. Het combineren van methoden uit slechts één categorie is niet aan te raden. Opgemerkt moet worden dat niet alle methoden uit de drie categorieën noodzakelijkerwijs gelijkwaardig zijn, zelfs niet in hun combinatie.

Momenteel worden phishing-resistente methoden zoals passkeys, die gebaseerd zijn op de FIDO2 / WebAuthn-standaard, als de veiligste methoden beschouwd. Passkeys vervangen het klassieke wachtwoord volledig door een cryptografisch sleutelpaar, waarbij apparaatgebonden passkeys (sleutelmateriaal dat is opgeslagen in het beveiligde element van het eindapparaat "TPM") en gesynchroniseerde passkeys (sleutelmateriaal wordt opgeslagen in een centraal systeem, zoals cloud). Registratie gebeurt door middel van een bewijs van eigendom (zoals via een smartphone of computer) in combinatie met biometrie (zoals vingerafdruk of gezichtsherkenning) of een pincode.

Elke combinatie, zelfs zonder het gebruik van phishing-resistente methoden, is echter een verbetering ten opzichte van het gebruik van wachtwoorden alleen. De combinatie van authenticatiemethoden kan of moet afhankelijk van de beveiligingsvereisten van de applicatie of de identiteit van de gebruiker worden gekozen, evenals de technische vereisten.

De flexibele combinatie van verschillende authenticatiemethoden stelt de gebruiker in staat om een gebruiksvriendelijke "wachtwoordloze authenticatie" te gebruiken. "Wachtwoordloze authenticatie" kan worden onderverdeeld in twee vormen:

- Aan de systeemkant (technisch) op basis van wachtwoorden, wachtwoordloos vanuit het oogpunt van de gebruiker
  Een systeem vereist op de achtergrond nog steeds een wachtwoord voor authenticatie, maar dit wordt niet actief in het inlogproces van de gebruiker gevraagd/vereist

- Volledig wachtwoordloos
  Noch vanuit technisch oogpunt, noch vanuit het oogpunt van de gebruiker is een wachtwoord vereist. Registratie vindt plaats zonder wachtwoord. In de regel wordt vanuit technisch oogpunt aan de systeemzijde een asymmetrische sleutelmethode gebruikt. Het gebruik van volledige wachtwoordloze authenticatie wordt aanbevolen, maar vanuit het oogpunt van vandaag kan het, vanwege verouderde software, niet in alle doorontwikkelde infrastructuren worden geïmplementeerd.

Bovendien bieden moderne MFA-systemen een dynamische benadering van gebruikersauthenticatie (adaptieve authenticatie). De authenticatiemethode die nodig is voor het aantonen van de identiteit of de combinatie daarvan is hier niet langer statisch, maar situatieafhankelijk en flexibel. De volgende kenmerken kunnen bijvoorbeeld afzonderlijk of in uw combinatie (als risicoscore) worden opgenomen: groeps-/rolaffiliatie, geografische locatie van de gebruiker, bewegingssnelheid, unieke apparaat-ID / apparaat-IP, typische werktijden van de gebruiker, enz.

MFA kan tegenwoordig in veel toepassingen worden geactiveerd of maakt deel uit van de productopties. Als dit voor applicaties die bescherming verdienen niet het geval is of als in een organisatie meerdere applicaties worden gebruikt die bescherming nodig hebben, dan wordt het gebruik van een centrale

authenticatieoplossing voor alle applicaties en gebruikers aanbevolen. Parallelle werking van meerdere oplossingen worden vermeden met het oog op de toenemende complexiteit, hogere kosten en grotere beheerinspanningen, afnemende gebruikersacceptatie en verhoogde beheerinspanningen. Daarom worden moderne MFA-oplossingen met een gecentraliseerde aanpak aanbevolen, aangezien deze, ten opzichte van een breed scala aan authenticatiemethoden, applicaties, gebruikers en systemen en open technische standaarden, zoals Oauth2, OIDC, WS-Fed, SAML en REST-API, een hoge mate van flexibiliteit integreren.

Vanwege de eerder genoemde menselijke en technische risico's van single-factor authenticatie vereisen verschillende nationale en internationale voorschriften zoals DORA, NIS2, PSD2, KRITIS, GDPR of BAFIN het gebruik van MFA om de toegang van gebruikers, tot een computersysteem dat bescherming nodig heeft, te beveiligen.

Houd bij het kiezen van een multi-factor authenticatiesysteem rekening met het volgende:

- Verscheidenheid aan methoden:
  Ondersteuning van verschillende methoden, zoals wachtwoorden, eenmalige wachtwoorden, biometrie en nog veel meer om te voldoen aan de verschillende behoeften van gebruiksscenario's, gebruikersgroepen en rollen
- Integratie en compatibiliteit:
  Het MFA-systeem moet zich naadloos kunnen integreren in de bestaande IT-infrastructuur om logins van welke aard dan ook (besturingssysteem, webgebaseerd, VPN) via open technische standaarden zoals Oauth2 / OIDC, SAML, WS-Fed, RADIUS en Web API te verwerken.
- Gebruiksgemak en beheer:
  Een gecentraliseerd systeem voor het beheren van authenticatiemethoden dat voor zowel beheerders als eindgebruikers gemakkelijk te gebruiken is, 1. functies zoals selfservice-opties voor gebruikers en gedetailleerde rapporten voor beheerders kunnen de efficiëntie en tevredenheid verhogen.
- Efficiënte uitrolprocessen:
  Vereenvoudig uitrolprocessen met een gecentraliseerde MFA-oplossing met een workflowgestuurd registratieportaal dat zich aanpast aan de lay-out van de organisatie om een snelle en eenvoudige registratie van de methoden van een gebruiker mogelijk te maken.
- Schaalbaarheid en toekomstbestendigheid:
  Een MFA-systeem moet, voor effectieve en efficiënte operaties op de lange termijn, schaalbaar zijn om te voldoen aan toekomstige eisen en technologische ontwikkelingen.

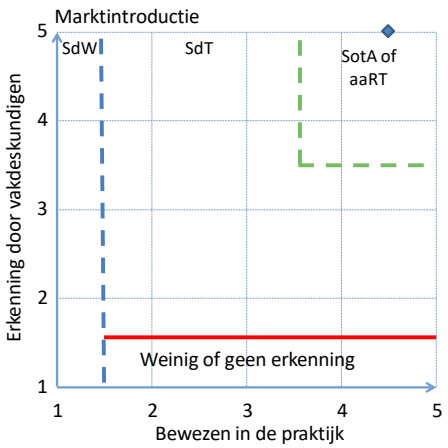
Welke beschermingsdoelen worden door de maatregel afgedekt?

☐ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.2.4 Cryptografische methoden

Cryptografie in de zin van informatiebeveiliging houdt zich bezig met het ontwerpen, definiëren en bouwen van informatiesystemen die zo goed mogelijk bestand zijn tegen manipulatie en ongeoorloofd lezen.

Cryptografische methoden zijn toepasbare methoden om gevoelige inhoud te beschermen. De kwaliteit van de cryptografische methoden hangt met name af van de gebruikte coderingsmethode (zoals AES, ECIES), de geselecteerde sleutellengte (zoals 512 bits), de beveiliging van de sleutel en de geïmplementeerde beveiligingsconfiguratie van de gebruikte producten. Naarmate de sleutellengte toeneemt, neemt het aantal manieren om een versleuteld bericht te ontcijferen toe, waardoor de beveiliging toeneemt.

In de moderne cryptografie worden de gebruikte methoden verondersteld te voldoen aan het Kerckhoff-principe. Dit betekent dat de beveiliging van een versleutelingsmethode gebaseerd is op het geheimhouden van de sleutel. Daarom kan de gebruikte procedure worden vermeld.

Er wordt een onderscheid gemaakt tussen symmetrische en asymmetrische versleutelingsmethoden:

Symmetrische procedures	**Asymmetrische procedures**
▪ Ingewikkelde sleuteldistributie (wanneer een beveiligd communicatiekanaal ontbreekt). ▪ Alle deelnemers die betrokken zijn bij dezelfde communicatie gebruiken slechts één en dezelfde sleutel. Dus dezelfde sleutel wordt gebruikt voor codering en decodering. Voor elke nieuwe communicatie-instantie moet een nieuwe sleutel worden gegenereerd: *n* instanties vereisen $\frac{(n\cdot(n-1))}{2}$ sleutels, wat overeenkomt met kwadratische groei. ▪ Snelle versleuteling van bulkgegevens. ▪ De enige aantoonbaar veilige versleutelingsmethode is Vernam-Cipher / one-time-path. In de praktijk wordt deze methode echter nauwelijks gebruikt. ▪ Spontane versleutelde communicatie zonder een voorafgaande vertrouwensrelatie (ten minste om de sleutel uit te wisselen) is onmogelijk tenzij kwantumcryptografie wordt gebruikt.	▪ Voor onafhankelijk versleutelde communicatiekanalen groeit het vereiste aantal sleutels lineair met het aantal deelnemers (cf. symmetrische encryptie met kwadratische groei). ▪ Alle bekende methoden zijn erg traag in vergelijking met symmetrische encryptiemethoden met een vergelijkbare sleutellengte. ▪ De vereiste sleutellengte is, om dezelfde beveiliging te bieden, meestal langer dan bij symmetrische cryptografie. ▪ Digitale handtekeningen zijn mogelijk. ▪ Eenvoudige sleuteluitwisseling; er zijn twee sleutels (openbaar en private). De public key wordt gebruikt voor de versleuteling, terwijl de private sleutel alleen wordt gebruikt voor de ontsleuteling. Private sleutels worden niet uitgewisseld. ▪ Niet geschikt voor grotere hoeveelheden data.

In het hybride proces, dat in de praktijk meestal wordt gebruikt, worden symmetrische en asymmetrische versleuteling gecombineerd om de voordelen van de respectieve technologie te benutten. In de praktijk wordt het uit te wisselen bericht symmetrisch versleuteld met een sessiesleutel. Deze moet groot genoeg zijn om brute force van de gehele toetsruimte te voorkomen. Vervolgens wordt deze sessiesleutel asymmetrisch versleuteld met de public key van de geadresseerde en toegevoegd aan het versleutelde bericht.

Met de toenemende technische ontwikkeling en de daaruit voortvloeiende toename van rekenkracht, bestaat het risico dat de geheime sleutelinformatie wordt achterhaald en daarmee de tot nu toe gebruikte methoden worden gekraakt. Dit is precies wat met de komst van kwantumcomputers wordt verwacht.

Om deze ontwikkeling aan de coderingskant tegen te gaan, heeft het Amerikaanse National Institute of Standards and Technology (NIST) voor methoden van kwantumresistente cryptografie drie standaarden aangenomen (FIPS-203[11], FIPS-204[12], FIPS-205[13]).

[11] csrc.nist.gov/pubs/fips/203/final
[12] csrc.nist.gov/pubs/fips/204/final
[13] csrc.nist.gov/pubs/fips/205/final

Desondanks is het aan te raden om de gebruikte versleutelingsmethoden regelmatig (zoals jaarlijks) te controleren op hun effectiviteit en actualiteit en, indien nodig, aan de huidige aanbevelingen aan te passen. Dit kan bijvoorbeeld worden gedaan door de sleutellengte te wijzigen (zoals van 256 bits naar 512 bits).

Tegen de achtergrond van de hierboven geschetste ontwikkeling moet er nu al voor worden gezorgd dat op de lange termijn cryptografische methoden voor de bescherming van belangrijke informatie ook in de toekomst kunnen worden uitgewisseld. Deze crypto-wendbaarheid is absoluut noodzakelijk om het vereiste beveiligingsniveau in de toekomst te garanderen.

De coderingsmethoden worden in de technische richtlijn van BSI (BSI TR-02102-1) op een specifieke manier gepresenteerd en afhankelijk van de gebruikte sleutellengte[14] wordt hun gebruiksduur aanbevolen. Ook heeft ENISA[15] verdere aanbevelingen over instrumenten en procedures.

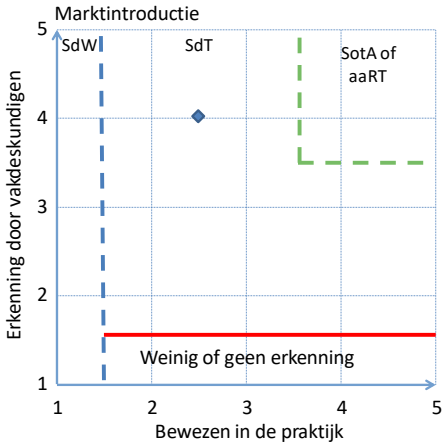
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.2.5 Versleuteling van gegevensdragers

Volledige schijfversleuteling beschermt de gegevensdragers die in een systeem zijn geïnstalleerd of extern zijn aangesloten (zoals magnetische harde schijven of SSD's op basis van flashgeheugen) tegen ongeoorloofde toegang (uitlezen, wijzigen) door derden. De daar opgeslagen informatie is alleen in platte tekst toegankelijk na handmatige of geautomatiseerde authenticatie van de gebruiker of voordat het besturingssysteem van de pc of smartphone of computer is opgestart.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

Deze maatregel beschermt gegevens op harde schijven van onbeheerde, uitgeschakelde apparaten zoals pc's, laptops, tablets of smartphones (zogenaamde "data at rest"). In geval van verlies door onoplettendheid of diefstal, of tijdelijke beschikbaarheid voor onbevoegde derden (hotelkamers), kunnen aanvallers de inhoud van de opgeslagen informatie niet lezen of manipuleren. Het kopiëren van harde schijven die op deze manier zijn beveiligd levert, omdat deze versleuteld zijn, dan alleen nutteloze gegevens op.

[14] www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html

[15] www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

De in een systeem geïnstalleerde gegevensdrager(s), zoals magnetische harde schijven of SSD's op basis van flashgeheugen, waarop het besturingssysteem en de vertrouwelijke bedrijfsgegevens zich bevinden, worden door de maatregel zodanig versleuteld dat het onbevoegd lezen ervan geen platte tekst oplevert. Dit geldt zowel voor het uitlezen wanneer het systeem is uitgeschakeld als voor een verwijderde harde schijf.

In XTS-modus moet als symmetrische codering ten minste AES-256 worden geselecteerd. Een centrale beheertool maakt het veel gemakkelijker om dit te gebruiken op alle pc's in een organisatie. Er mag nooit, zelfs niet voor back-updoeleinden, in de cloud een back-up gemaakt worden van de cryptografische sleutels.

In het geval van volledige versleuteling van de harde schijf moet veel belang worden gehecht aan pre-boot authenticatie, complexe wachtwoorden en 2-factor authenticatie, idealiter door middel van "kennis en bezit", bijvoorbeeld met een extra token (zie maatregel 0 MFA). Dit maakt, in het geval van meervoudige onjuiste wachtwoordinvoer, ook het gebruik van hardwareondersteunde vertragingsmechanismen mogelijk.

Voor zover het apparaat het toelaat, bijvoorbeeld met Windows 10 (en hogere) systemen, moet ook "Secure Boot" worden ondersteund. Dit zorgt ervoor dat tijdens het opstartproces alleen bootloaders met een geldige signature worden geladen en uitgevoerd, zodat de daaropvolgende decodering van de partitie van het besturingssysteem niet kan worden geïnfiltreerd.

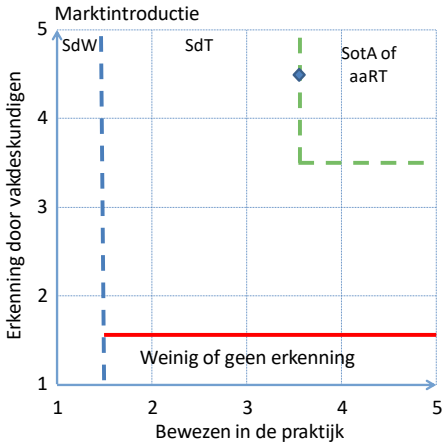
Welke beschermingsdoelen worden door de maatregel afgedekt?

☐ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Classificatie van de stand van de technologie



3.2.6 Versleuteling van bestanden en mappen

Bestands- en mapversleuteling omvat de versleuteling van individuele objecten, zoals containers, mappen en individuele bestanden, dit type versleuteling wordt ook wel objectversleuteling genoemd. Objectversleuteling biedt de mogelijkheid om bestanden en mappen veilig van de ene naar de andere locatie te transporteren en zo ongeoorloofde toegang te voorkomen. De programma's die voor dit doel beschikbaar zijn, decoderen de gegevens automatisch na het inloggen op het besturingssysteem of na een expliciete actie van de gebruiker. Daarna zijn de gegevens transparant beschikbaar, d.w.z. dat de gebruiker met de objecten kan werken alsof ze niet versleuteld zijn.

Dit zorgt ervoor dat niemand behalve de geautoriseerde personen toegang krijgt tot de beschermde informatie. De versleuteling kan persoonsgegevens en, in het ergste geval, het bestaansrecht van een organisatie in gevaar brengen.

Bovendien is objectversleuteling een goede optie bij het gebruik van externe clouddiensten: als de cloud-provider geen toegang heeft tot de gebruikte coderingssleutels, kan dit effectief voorkomen dat de provider de gegevens kan bekijken. Bij de versleuteling van gegevens in de cloud zijn er echter meestal beperkingen met betrekking tot het indexeren van gegevens, zoeken in volledige tekst, antivirusbescherming en bescherming tegen datalekken. Deze kunnen gedeeltelijk worden gereduceerd met aanvullende, complexe technieken zoals het gebruik van encryptiegateways.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

1. Onderschepping en misbruik van gegevens tijdens het transport, zoals per e-mail
2. Ongeoorloofde toegang tot gevoelige gegevens als gevolg van verlies of diefstal van verwijderbare opslagapparaten
3. Misbruik van gegevens die in de cloud zijn opgeslagen

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Bestands- en mapversleuteling omvat de versleuteling van afzonderlijke objecten, zoals containers, mappen of afzonderlijke bestanden. Hierdoor kunnen bestanden en mappen veilig van de ene plaats naar de andere worden getransporteerd, veilig op elke locatie worden opgeslagen en worden voorkomen dat ze door onbevoegden worden bekeken.

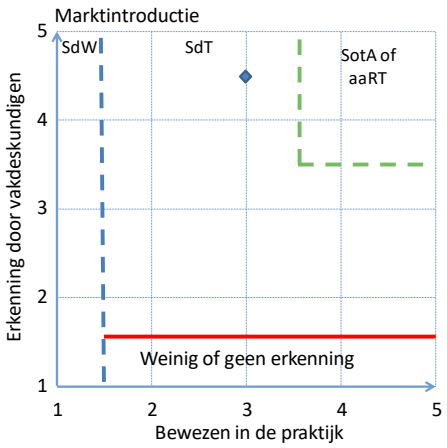
Welke beschermingsdoelen worden door de maatregel afgedekt?

☐ Beschikbaarheid

☐ Integriteit

☒ Vertrouwelijkheid

Classificatie van de stand van de technologie



3.2.7 Versleuteling van e-mailberichtent

Zakelijke e-mailberichtent bevatten vaak belangrijke gegevens die het waard zijn om beschermd te worden, daarnaast zijn e-mailadressen meestal gepersonaliseerd en bevatten e-mailberichtent meestal persoonsgegevens die beschermd moeten worden tegen ongeoorloofde toegang en wijziging. De beschermingsdoelen kunnen over het algemeen worden bereikt door de overdracht van e-mailberichtent en/of de content van de e-mail te versleutelen.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

- Het bespioneren en manipuleren van e-mailberichtent tijdens het transport
- Het bespioneren en manipuleren van opgeslagen e-mailberichtent

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

- Versleutelde verzending van e-mailberichtent (transportversleuteling; TLS)
- Versleuteling van de content van e-mailberichtent (S/MIME en PGP)

De beveiligingseisen voor e-mail worden onder meer bepaald door het soort gegevens dat via het e-mailsysteem wordt verzonden en daarin wordt opgeslagen. In principe kan bij zakelijke transacties ervan worden uitgegaan dat e-mailberichtent op zijn minst voor de organisatie belangrijke informatie bevatten. Bovendien worden e-mailadressen, indien gepersonaliseerd, al als persoonsgegevens beschouwd en daarom kan ervan worden uitgegaan, dat per e-mail persoonsgegevens worden verzonden en opgeslagen. In individuele gevallen en afhankelijk van het respectieve gebruik van e-mail kunnen ook gegevens worden doorgegeven die speciale bescherming vereisen, zoals gezondheidsgegevens, gegevens van klanten, zoals advocaten en bijzonder waardevolle bedrijfsgeheimen, zoals ontwerpgegevens.

Dit resulteert in de volgende beveiligingseisen voor e-mail:

- Bescherming tegen ongeoorloofde inzage en wijziging tijdens transport en opgeslagen e-mailberichtent (beschermingsdoelstelling: vertrouwelijkheid),
- Bescherming tegen latere wijziging van e-mailberichtent in het geval van langdurig gearchiveerde e-mailberichtent (beschermingsdoelstelling: integriteit).

Deze beschermingsdoelen kunnen over het algemeen worden bereikt door middel van versleuteling. Bij het versleutelen van e-mailberichtent moet een onderscheid worden gemaakt tussen versleuteling bij de verzending (transportversleuteling) en versleuteling van de e-mail zelf (end-to-end versleuteling). De beschermingsdoelstellingen vereisen ten minste het gebruik van transportversleuteling voor de verzending van e-mailberichtent via openbare netwerken. De protocollen die worden gebruikt voor de verzending van e-mailberichtent via het internet, namelijk SMTP, POP3 en IMAP, voorzien echter in hun basisvorm niet in een versleutelde gegevensoverdracht. Dit is waarschijnlijk de reden waarom grote delen van het e-mailverkeer, hoewel er al lange tijd voldoende tools beschikbaar zijn voor het versleutelen van e-mailberichtent, onversleuteld worden verzonden.

In e-mailverkeer moet voor transportversleuteling de huidig geldende versie van TLS (Transport Layer Security) worden gebruikt zoals gedefinieerd in RFC 5246. Veilige versleutelingsmethoden (zoals nu AES-256) moeten worden gebruikt en het gebruik van onveilige coderingsmethoden (zoals RC4) moet worden uitgesloten. In het algemeen moet forward-secrecy moet worden geactiveerd, daarnaast is het zinvol om de echtheid en geldigheid van de certificaten van de betreffende wederpartij die in TLS worden gebruikt, bijvoorbeeld met DANE te controleren (RFC 7671). Uitgebreide aanbevelingen over TLS worden gegeven in de technische richtlijn van de BSI: TR-02102-2, deel 2.

Voor de bescherming van bijzonder gevoelige gegevens wordt end-to-end versleuteling wordt. Hiervoor zijn twee standaarden opgesteld: S/MIME (Secure / Multipurpose Internet Mail Extensions, gedefinieerd in RFC 5751) en OpenPGP (Pretty Good Privacy, gedefinieerd in RFC 4880). Beide gebruiken in principe dezelfde cryptografische methoden, ze verschillen echter in de certificering van de public keys en dus in de vertrouwensmodellen en zijn niet compatibel met elkaar.

Wanneer end-to-end versleuteling wordt gebruikt, heeft in het transmissiepad geen enkel systeem toegang tot de content van de e-mail. Dit betekent echter dat volledig moet worden afzien van contentfilters, antivirus, antispam, preventie van gegevensverlies en archivering. Daarom kan het gebruik van contentversleuteling alleen zinvol zijn tussen organisaties; d.w.z. e-mailberichtent worden bij de overgang van het openbare internet naar het privénetwerk van de organisatie (gateway) versleuteld en gedecodeerd (end-to-end encryptie van de organisatie); indien nodig in combinatie met een organisatie-eigen contentversleuteling.

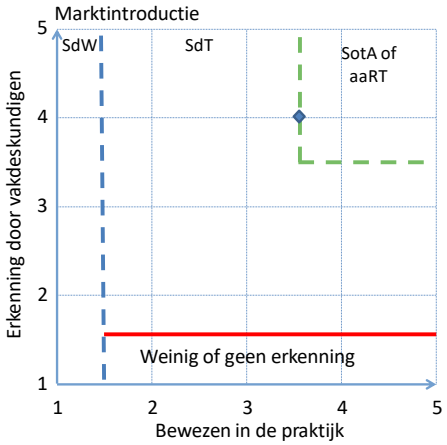
Welke beschermingsdoelen worden door de maatregel afgedekt?

☐ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Classificatie van de stand van de technologie



3.2.8 Elektronisch dataverkeer beveiligen met PKI

Bij elektronisch dataverkeer is het belangrijk dat de identiteit van de communicatiepartners en de authenticiteit van de verzonden content gewaarborgd zijn. Het bewijs van de elektronische identiteit van personen, organisaties en apparaten kan worden gewaarborgd door het gebruik van elektronische certificaten. Elektronische handtekeningen zijn geschikt om de authenticiteit van verzonden documenten en berichten aan te tonen. Op certificaten gebaseerde oplossingen worden ook gebruikt voor veilig versleuteld gegevenstransport. Al deze scenario's vereisen een component voor het genereren, terugroepen, beheren en verifiëren van elektronische certificaten die het bewijs van elektronische identiteiten op een betrouwbare manier garanderen: een public key infrastructure (PKI).

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

- Diefstal van identiteit / valse identiteit
- Manipulatie van de content van elektronische berichten en bestanden
- Het manipuleren van de chronologische volgorde van berichten en bestanden

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

De volgende maatregelen zijn nuttig tegen de hierboven beschreven bedreigingen:

- Het instellen van een eigen PKI of het gebruik van een externe PKI
- Gebruik van elektronische handtekeningen (signatures, certificaten, zegels) van een geaccrediteerde Trust-Center
- Gebruik van gekwalificeerde tijdstempels om de authenticiteit en chronologische volgorde van berichten en documenten te bewijzen

Elektronische certificaten worden uitgegeven door de certificeringinstantie van een PKI-organisatie. Hierbij wordt de term Certificeringinstantie (CA) gebruikt. De geldigheid van publieke sleutels wordt bevestigd door digitale handtekeningen van de CA. Naast de sleutel zelf bevat het digitale certificaat andere informatie, zoals de geldigheidsduur, enz. Als verantwoordelijke autoriteit is de CA het centrale onderdeel van de openbare-sleutelinfrastructuur. Om de betrouwbaarheid van de CA te behouden, is voordat het elektronische certificaat wordt afgegeven een duidelijke verificatie van de identiteit van de aanvragende persoon of organisatie noodzakelijk. Dit wordt gedaan door de Registration Autoriteit (RA).

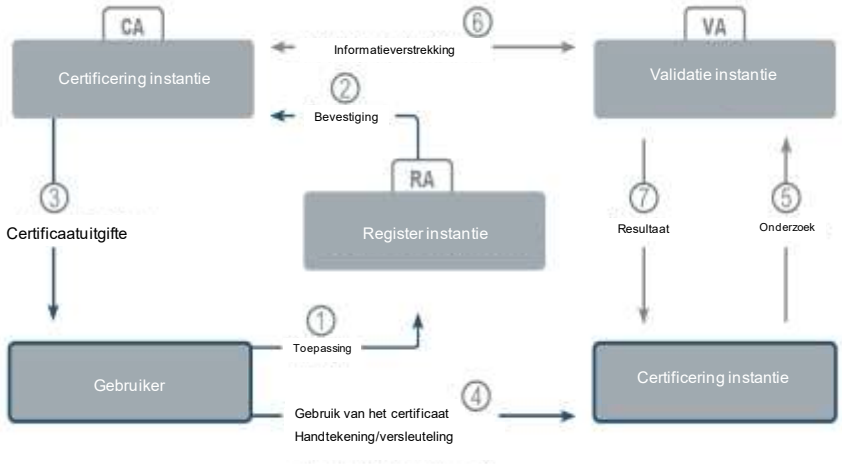
Om de geldigheid van elektronische certificaten te verifiëren, is een validatieservice of validatie-autoriteit (VA) vereist. Doorgaans wordt onderscheid gemaakt tussen controle op basis van een gepubliceerde Certificate Revocation List (CRL) en real-time controle door een OCSP-service (Online Certificate Status Protocol). De keuze van de testvariant vloeit meestal voort uit het betreffende toepassingsscenario. Afhankelijk van de juridische status van de PKI is het in de meeste gevallen nuttig of zelfs noodzakelijk om alle transacties juridisch bruikbaar te loggen in een PKI. Voor sommige toepassingen zijn ook gecertificeerde CA-producten vereist.

De mogelijke toepassingen van PKI-gebaseerde methoden zijn legio. Als voorbeeld worden de volgende toepassingsmethoden genoemd:

- Ondertekening en versleuteling van e-mailberichtent (S/MIME)
- Authenticatie en encryptie in het "Internet of Things"
- Authenticatie en versleuteling op het web (HTTPS)
- Authenticatie en versleuteling voor VPN-services
- Authenticatie en versleuteling in bekabeld of draadloos netwerk (IEEE 802.1X)
- Authenticatie en integriteitborging van uitvoerbare code (code signing)
- Authenticatie en integriteitborging van documenten (digitale handtekening)
- Authenticatie van klanten / gebruikers op internet

Afhankelijk van de status van de provider en de beveiligingsstandaard van het bijbehorende datacenter kan een breed scala aan oplossingen worden opgezet. Dit gaat van een root CA, als zogenaamde root of trust, tot strikt hiërarchische PKI met meerdere sub-CA's. Kruiscertificering met andere PKI's is ook mogelijk.

In het volgende diagram ziet u de basisstructuur en interactie van PKI-componenten in een werkstroom.



Afbeelding 4: Structuur en interactie van PKI-componenten

Het gebruik van certificaten is voor bijna alle gebieden nuttig en nuttig. Naast toepassingsgebieden in de publieke sector zijn ze te vinden in de energie- en gasvoorziening, bij elektronische juridische transacties (met beA, beN, beBPo), in de gezondheidszorg, maar ook in de industriële en non-profit omgeving (zoals verenigingen, verenigingen).

Met name de eIDAS-verordening voorziet in uitgebreide gebruiksscenario's. Identiteitsbewijzen en vertrouwensdiensten worden bijvoorbeeld ondersteund door PKI (zie onderstaande tabel) [16].

[16] Meer informatie is te vinden op www.ebca.de

eIDAS Regelingen/Toepassingen	
Identiteiten	Certificaten
	Elektronische paspoorten
Vertrouwensdiensten	Elektronische zegels
	Elektronische tijdstempels
	Website-authenticatie
	Elektronische bezorgdiensten
	Alarmerende diensten

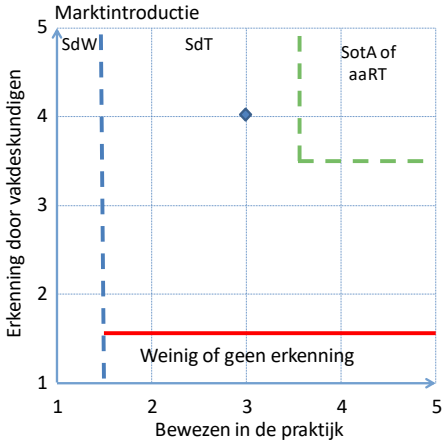
Welke beschermingsdoelen worden door de maatregel afgedekt?

☐ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Classificatie van de stand van de technologie



3.2.9 Gebruik van versleutelde VPN-oplossingen (Layer 3)

Een Layer 3 VPN verwijst naar de verbinding van netwerken op Layer 3 van het OSI-model, d.w.z. in het bijzonder het transport binnen een tunnel van IP-dataverkeer over niet-vertrouwde netwerken. Zelfs als onversleuteld transport mogelijk zou zijn, omvat de huidige algemene opvatting van VPN ook het gebruik van versleuteling. De gevestigde VPN-methoden zijn meestal gebaseerd op open standaarden of specificaties zoals IPSec en open-source implementaties zoals OpenVPN en Wireguard. De tunnel voor datatransport wordt doorgaans opgezet op layers 3 (IP) en 4 (TCP, UDP, ESP).

De klassieke toepassingen in de bedrijfsomgeving van Layer 3 VPN zijn het verbinden van locaties en de verbindingen van mobiele werknemers. Nieuwere toepassingen zijn onder meer netwerkoverlays, bijvoorbeeld in de context van multi-cloudscenario's of de verbinding met cloudgebaseerde zero-trust infrastructuren. Voor particuliere klanten worden ook VPN-diensten op de markt gebracht, zoals voor het veilige gebruik van open Wi-Fi-hotspots en het omzeilen van op GeoIP gebaseerde beperkingen. Deze VPN's voor consumenten worden hieronder niet in aanmerking genomen.

Tegen welke IT-beveiligingsbedreigingen wordt de maatregel ingezet?

Door de externe stations te verifiëren en de gegevens te versleutelen, beschermen VPN's tegen:

- Verlies van integriteit en vertrouwelijkheid van niet-versleutelde en zwak versleutelde verbindingen, mogelijk ook als extra versleutelingslaag in een defense-in-depth architectuur.
- Externe aanvallers die leestoegang hebben tot de getransporteerde gegevens.

- Externe aanvallers die de getransporteerde gegevens kunnen manipuleren.

De gebruikte VPN's zijn ook onderhevig aan andere bedreigingen:

- Afvoer van sleutelinformatie
- Zwakke cryptografie
- Zwakke en onjuiste authenticatie van externe stations
- Denial of Service: Fouten en aanvallen brengen de beschikbaarheid van de VPN in gevaar

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Een Layer 3 VPN verwijst naar de verbinding van netwerken en de verbinding van een client met een netwerk op Layer 3 van het OSI-model. De gegevens die tijdens het proces worden getransporteerd, worden versleuteld en de VPN-eindpunten verifiëren en autoriseren het andere VPN-eindpunt. Het kan bijvoorbeeld worden gebruikt om bedrijfsvestigingen in verschillende landen veilig en vertrouwelijk met elkaar te verbinden via onveilige lijnen van derden, zoals internet of diensten die worden gehuurd van een telecomprovider. In tegenstelling tot een Layer 2 VPN wordt er minder data getransporteerd omdat Layer 2 data, zoals Broadcasts, niet wordt verzonden. In ruil daarvoor kan een Layer 3 VPN in bepaalde (zeldzame) toepassingsscenario's niet transparant worden gebruikt. Complexe topologieën, zoals on-demand VPN-verbindingen, zijn soms alleen of veel eenvoudiger te implementeren met een Layer 3 VPN. Hetzelfde geldt voor VPN-configuraties met een groot aantal endpoints.

Een Remote Access Layer 3 VPN vereist, in tegenstelling tot een Site-to-Site VPN Layer 3 VPN, VPN-toegang voor elke deelnemer. Vaak gebruik wordt hierbij gemaakt van een hub-and-spoke VPN-architectuur, in dat geval wordt de centrale node een VPN-concentrator genoemd. Alternatieven zijn Mesh-architecturen waarin de verschillende deelnemers rechtstreeks met elkaar communiceren. Als centraal onderdeel van een IT-infrastructuur moet speciale aandacht worden besteed aan de configuratie en werking van een Layer 3 VPN.

Een VPN moet de integriteit en vertrouwelijkheid van de gegevens die worden doorgegeven waarborgen. Om dit te doen, moet het apparaat met behulp van algoritmen en parameters die als veilig worden beschouwd versleuteling en authenticatie uitvoeren. Of deze kritieke parameters met voldoende beveiliging zijn geconfigureerd is niet duidelijk voor een gebruiker, aangezien de VPN vaak zelfs als er zwakke punten in de configuratie zijn verbindingen tot stand kan brengen.

Er zijn solide open-source implementaties voor VPN's en fabrikanten vertrouwen er vaak op in hun producten. Naast de beschikbaarheid van ondersteuning en actief patchbeheer bieden commerciële oplossingen over het algemeen minder configuratiecomplexiteit, met name voor grote en complexe omgevingen, betere bescherming tegen onveilige-/ misconfiguratie, betere ondersteuning voor hoge beschikbaarheidseisen en integratie met bedrijfsspecifieke authenticatie. Bovendien bieden sommige fabrikanten goedkeuringen of certificeringen aan die vereist zijn om wettelijke redenen in bepaalde werkomgevingen.

VPN's bevinden zich op een kritieke positie in het netwerk. Fouten in de implementatie van de fabrikant kunnen een aanvaller niet alleen toegang geven tot de communicatie, maar ook tot het interne netwerk. Helaas zijn in het verleden dergelijke kwetsbaarheden en zelfs expliciete backdoors geen geïsoleerde gevallen geweest en hebben ze ook gerenommeerde fabrikanten getroffen. Daarom moet voorkeur worden gegeven aan producten die een hoog niveau van platformbeveiliging en een hoog niveau van zelfbescherming kunnen aantonen, bijvoorbeeld door middel van onafhankelijke tests (certificeringen en goedkeuringen). Vereisten voor de werkomgeving moeten ervoor blijven zorgen dat fysieke toegang tot de VPN-apparaten alleen mogelijk is voor geautoriseerde personen.

Als het gaat om de beschermingsdoelen van integriteit, vertrouwelijkheid en authenticiteit van de verzonden gegevens, is ook de integriteit van het platform cruciaal. VPN-apparaten moeten worden gebouwd op een bijzonder gehard platform, een uitstekende zelfbescherming hebben en vrij zijn van backdoors. Wanneer deze correct zijn geconfigureerd, garanderen de beveiligingsprotocollen, die door een Layer 3 VPN worden gebruikt, ook de integriteit en authenticiteit van de getransporteerde gegevens.

Het beheer en het veilig gebruik van sleutelmateriaal speelt ook een bijzonder belangrijke rol. In dit verband verdient de voorkeur aan oplossingen die het aantoonbaar mogelijk maken om veilig willekeurige getallen te genereren, sleutels veilig op te slaan, private authenticatiesleutels (zoals op chipkaarten) te bewaren en de leeftijd van de gebruikte coderingssleutels te volgen. Een bijzondere

uitdaging is de constructie van VPN-eindpunten in cloudomgevingen, zowel voor een zekere kans als voor de bescherming van sleutelmateriaal.

Om de beschikbaarheid van de Layer 3 VPN te waarborgen, zijn voor de hardware en software passende maatregelen nodig van de VPN-endpoints (zoals VPN-concentrators). De hardware moet beschikken over redundante voedingen en ventilatoren, evenals over voldoende rekenkracht. Aangezien in de praktijk deze maatregelen alleen niet voldoende zijn om hardwarestoringen te voorkomen, moet ook de mogelijkheid van redundante bediening worden gegeven (configuratie met hoge beschikbaarheid). Monitoring speelt ook een centrale rol om ervoor te zorgen dat defecte hardware op tijd wordt gedetecteerd. Hier moeten de producten een passende monitoring ondersteunen, bijvoorbeeld door middel van SNMP. Voorts moet bijzondere aandacht worden besteed aan de bescherming tegen denial-of-service aanvallen. Natuurlijk is ook hier een bijzonder veilig platform een belangrijke voorwaarde, evenals gecontroleerde toegang tot de locaties waar de VPN-eindpunten (VPN-concentrators) in het LAN worden gebruikt.

Op de apparaten van een Layer 3 VPN verzamelen zich loggegevens. Deze gegevens zijn bij uitstek belangrijk om aanvallen op het netwerk te kunnen detecteren. Daarom moeten deze gegevens echter authentiek zijn, ook is het belangrijk dat beheerwijzigingen traceerbaar zijn en dat deze loggegevens bindend en controleerbaar zijn. Daartoe moeten er manieren zijn om dergelijke loggegevens op een fraudebestendige manier op te slaan. Dit kan bijvoorbeeld worden gewaarborgd door lokale append-only bestanden, door een interface met externe logservers, of SIEM-systemen.

Opmerking: Hoewel er geen twijfel bestaat over de fundamentele noodzaak van het gebruik van VPN's, leveren fabrikanten regelmatig innovaties om hun beveiligingsniveau, gebruiksgemak en bruikbaarheid te verhogen. De stand van de techniek in VPN's wordt daarom niet alleen bepaald door hun aanwezigheid, maar door de vorm van deze kwaliteiten.

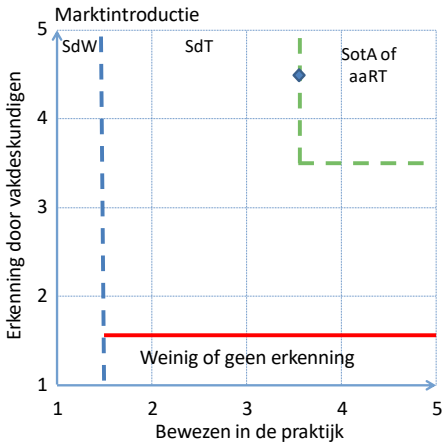
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Classificatie van de stand van de technologie



3.2.10 Versleuteling op Layer 2

Layer 2-encryptie is een beveiligingsoplossing als alternatief voor Layer 3 VPN's die wordt toegepast op de payload van Ethernet-frames in plaats van op IP-pakketten. De IP-headers hoeven niet te worden verwerkt (tijdwinst) en de lijncapaciteit wordt aanzienlijk minder belast door encryptie overhead dan bij encryptie op Layer 3 of hoger.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

Opname en evaluatie van enorme hoeveelheden gegevens, van site-verbindingen via de backbone van het bedrijfsnetwerk of de cloudverbinding, als gevolg van beveiligingslekken in netwerkhardware, netwerkserviceproviders, niet-gecontroleerde ondergrondse of onderzeese kabels en microgolf- of satellietverbindingen, en ook DDoS-aanvallen op versleutelde Layer 3-verbindingen.

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Veilige WAN-communicatie tussen bedrijfssites en datacenters met behulp van versleuteling. Gebruik van low-delay en bandbreedte-neutrale crypto-oplossingen voor Layer 2 WAN backbones en directe links (zoals dark fiber, Satcom).

Layer 2-encryptie is een beveiligingsoplossing die in bepaalde toepassingsscenario's een handig alternatief is voor Layer 3 VPN's. Het wordt toegepast op de payload van Ethernet-frames in plaats van IP-pakketten. De IP-headers hoeven niet te worden verwerkt (tijdwinst) en er is geen encryptie-overhead (lijnbandbreedte is volledig beschikbaar). Voorwaarde voor het gebruik is een op ethernet gebaseerd netwerk (point-to-point, hub-spoke of fully meshed) via eigen kabels (koper / glasvezel) en Layer 2-services van netwerkproviders (zoals carrier ethernetservices) die speciale Ether-typen ondersteunen.

Typische toepassingen voor Layer 2-encryptie zijn de bescherming van (ook internationale) WAN-backbonelijnen en datacenterverbindingen binnen het bedrijfsnetwerk en vertrouwde cloud- en colocatie providers en ook voor de bescherming van campus-backbonelijnen die buiten gebouwen en over het terrein van derden lopen.

De prestatievoordelen betalen zich vooral terug voor de invoering van centrale IT-diensten, grootschalige desktopvirtualisatie, consolidatie van datacenters, gedistribueerde en redundante opslagsystemen (SAN/NAS), die een grote hoeveelheid kleine en/of real-time relevante IP-pakketten hebben (zoals VoIP, IoT, Smart Grid) en waar IPsec-overhead en vertraging niet acceptabel zijn.

Bij het gebruik van deze netwerkcoderingtechnologie is het niet nodig om de bestaande IP-routeringsconfiguratie te wijzigen. Dit type versleuteling is transparant voor vrijwel alle netwerkdiensten en -toepassingen van OSI-Layer 3 en hoger en heeft geen meetbare impact op de prestaties van het netwerk.

De synchronisatie en authenticatie van de crypto-peers, evenals de periodieke wijziging van de cryptografische sleutels, is geautomatiseerd. Het genereren en distribueren van sleutels in de Layer 2 crypto-apparaten is gedecentraliseerd, waardoor belangrijke servers als single-point-of-failure worden vermeden en zo de beschikbaarheid van het netwerk wordt verhoogd. Er zijn BSI-goedgekeurde oplossingen beschikbaar.

MACsec is een veelgebruikt protocol voor Layer 2-encryptie. Het is gespecificeerd in de IEEE-802.1AE-standaard en is ontworpen om Ethernet-verkeer te beschermen tegen sabotage en afluisteren. De gegevens worden versleuteld verzonden op de verbindingen tussen naburige netwerkaccounts (hop-by-hop codering). Veel Layer 2-encryptieoplossingen die in de praktijk worden gebruikt, zijn gebaseerd op het MACsec-protocol, maar maken end-to-end encryptie mogelijk.

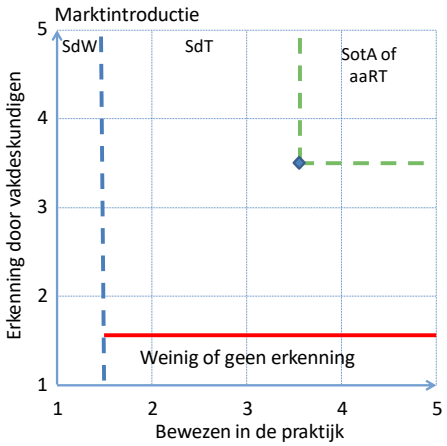
Welke beschermingsdoelen worden door de maatregel afgedekt?

☐ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Classificatie van de stand van de technologie



3.2.11 Bescherming van bestanden die in de cloud zijn opgeslagen

Met de voortschrijdende digitalisering en geografisch verspreide werkwijzen hebben in de IT-omgeving cloudgebaseerde bestandsuitwisselingdiensten steeds meer toepassing gevonden (zoals Dropbox, OneDrive, Google Drive). Om dergelijke diensten veilig te gebruiken en te beschermen tegen de bekende bedreigingen, moeten passende maatregelen worden genomen.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

De gegevens die zijn opgeslagen in een cloudgebaseerde service voor het delen van bestanden, zijn onderhevig aan de volgende bedreigingen:

- Ongeoorloofde toegang en inzage door de provider van de dienst
- Ongeoorloofde toegang en inzage door derden tijdens verwerking of opslag
- Ongeoorloofde toegang en inzage door derden tijdens het transport van de gegevens via het internet
- Diefstal en ongeoorloofd gebruik van de identiteit die is overeengekomen met de cloudservice

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

De volgende maatregelen zijn nuttig om de opgeslagen gegevens te beschermen:

1. Versleutelde overdracht van bestanden van en naar de bestandsuitwisselingservice
2. Versleuteling van de gegevens onafhankelijk van de bestandsuitwisselingservice door
   a. Client-side (end-to-end) versleuteling van de gegevens vóór overdracht naar cloudopslag (zoals door middel van encryptie van in de bestandsuitwisselingservice geïntegreerde clientsoftware die tot de cloudopslag behoort of door afzonderlijke end-to-end encryptiesoftware op de client)
   b. Gateway-versleuteling
   (zie hoofdstuk "Gegevensopslag in de cloud")

In het bijzonder moeten de volgende vragen worden overwogen:

1. Wie exploiteert de dienst en heeft de provider toegang tot de gegevens?
2. Wat zijn de wettelijke openbaarmakings-/informatieverplichtingen van de provider met overheidsinstanties (zoals U.S. Cloud Act)?
3. Hoe worden de gegevens beschermd tijdens de verwerking / bestandsopslag?
4. Hoe worden de gegevens beschermd tijdens het transport van en naar de provider?

Als de dienst wordt beheerd door een vertrouwde autoriteit, kan onder bepaalde omstandigheden worden afgezien van end-to-end versleuteling van de gegevens zelf, maar in principe is het ook bij betrouwbare providers nuttig.

Er zijn bestandsuitwisselingsdiensten beschikbaar waarbij gegevens transparant, zonder enige speciale actie van de gebruiker, worden versleuteld voordat ze worden geüpload, versleuteld door clientsoftware die door de provider van de dienst wordt geleverd en weer worden gedecodeerd na het downloaden. De cloudprovider ziet dan alleen versleutelde gegevens. In dit geval moet echter de provider van de filesharingservice worden vertrouwd als leverancier van de software en moet ervoor worden gezorgd dat de provider geen toegang heeft tot de gebruikte sleutels. Als alternatief kan versleutelingsoftware aan de clientzijde worden gebruikt, die zorgt voor end-to-end versleuteling van de gegevens vóór het uploaden of na het downloaden. Deze oplossingen vergen echter meestal extra inspanning voor de gebruiker. Als het gaat om versleuteling, moet aandacht worden besteed aan het gebruik van veilige methoden voor versleuteling en het genereren van sleutels en sleutelopslag.

In geen geval mag worden afgezien van de versleuteling van gegevens tijdens het transport van en naar de provider (transportversleuteling, meestal de huidige versie van TLS).

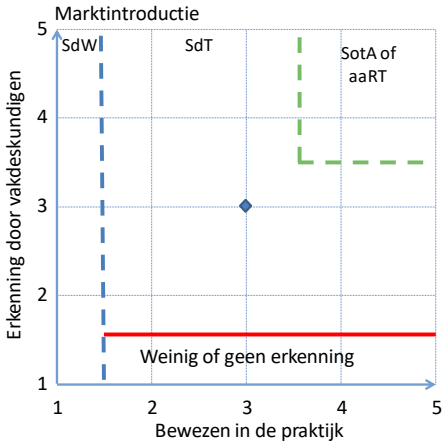
Welke beschermingsdoelen worden door de maatregel afgedekt?

☐ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.2.12 Gegevensverwerking in de cloud

Zodra (zeer) gevoelige gegevens een veilige, interne omgeving verlaten om in de cloud te worden opgeslagen, moeten deze, naast de transportversleuteling, vóór de overdracht worden versleuteld: De versleuteling moet uitsluitend onder controle van de gebruikersorganisatie blijven om ongeoorloofde toegang tot gegevens, zelfs door externe beheerders, uit te sluiten. Dit komt omdat iedereen die de gegevens versleutelt (bijvoorbeeld in het geval van BYOK-aanbiedingen) automatisch toegang heeft tot de niet-versleutelde gegevens. En dat zou alleen de gebruikersorganisatie moeten zijn. Een state-of-the-art oplossing moet daarom een overeenkomstige, volledig intern gecontroleerde gegevensversleuteling of tokenisatie mogelijk maken. State-of-the-art oplossingen die belangrijke functionaliteit mogelijk blijven maken, zoals het zoeken en filteren van gegevens, rapportage en geautomatiseerde verwerking van versleutelde gegevens in cloudtoepassingen.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

Zodra gevoelige gegevens worden doorgegeven aan en verwerkt door SaaS-applicaties, zijn deze onderhevig aan specifieke bedreigingen, waaronder met name:

- Ongeoorloofde toegang tot opgeslagen of verwerkte gegevens door externe en interne actoren, zoals cloudbeheerders.

- Onderschepping van data in transit tussen de organisatie en de cloud (man-in-the-middle aanvallen).
- Vervalsing en verwijdering van gegevens tijdens de overdracht naar de cloud.
- Data-exfiltratie bij succesvolle aanvallen op de cloudprovider of via toegang met speciale rechten.
- Diefstal en ongeoorloofd gebruik van de identiteit die is overeengekomen met de cloudservice.

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Om gevoelige gegevens in de cloud effectief te beschermen, wordt aanbevolen om deze versleuteld over te brengen naar de cloudapplicatie en daar uitsluitend in versleutelde vorm te verwerken. De versleuteling mag de functionaliteit van de applicatie, zoals zoeken, filteren en analyse, niet beperken.

Naast versleuteling aan de clientzijde (zie het vorige hoofdstuk van deze hand-out), is het gebruik van encryptiegateways hiervoor een bewezen technische oplossing:

Een encryptiegateway fungeert als een proxy tussen de interne omgeving en de cloudtoepassing. Het zorgt voor de versleuteling en pseudonimisering van gevoelige gegevens voordat deze naar de cloud worden verzonden en decodeert retourzendingen alleen voor geautoriseerde gebruikers. De cryptografische sleutels blijven volledig onder de controle van de gebruikersorganisatie. Noch cloudproviders, noch hun beheerders hebben dus toegang tot gegevens in platte tekst. Door de functionaliteit aan de kant van de encryptiegateway selectief te versleutelen en opnieuw te implementeren, kunnen relevante functies van de cloudtoepassing nog steeds worden gebruikt, zoal zoeken, sorteren en geautomatiseerde verwerking.

De gebruikte oplossing moet, om toekomstbestendig te zijn, aan de volgende criteria voldoen:

- Het sleutelbeheer moet, om misbruik en fouten te voorkomen, intern kunnen worden verdeeld over verschillende verantwoordelijke personen.
- De oplossing moet, om een constant hoog beveiligingsniveau voor alle cloudapplicaties mogelijk te maken, ook geschikt zijn voor meerdere clouds, d.w.z. meerdere cloudproviders ondersteunen en, indien nodig, voor zelfgeschreven applicaties in de cloud.
- Bovendien moet de oplossing tokenisatie ondersteunen om formaatbehoudende vervangingswaarden te genereren (zie bijbehorende hoofdstuk van deze hand-out), en, om indien nodig algoritmen uit te wisselen ook vereisten voor Crypto Agility (zie bijbehorende. Hand-out van TeleTrusT) ondersteunen.
- Het moet ook kunnen worden gehost met behulp van confidential computing. Gevoelige gegevens worden verwerkt in een beveiligde, op hardware gebaseerde, uitvoeringsomgeving (Trusted Execution Environment, TEE). De data is binnen deze omgeving alleen in platte tekst beschikbaar, zodat zelfs systeembeheerders er geen toegang toe hebben (zie ook de "Cloud Security" hand-out van TeleTrusT).

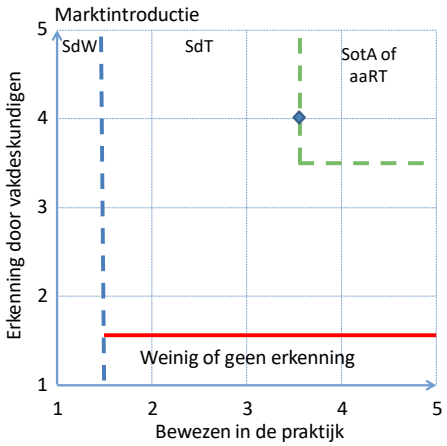
Welke beschermingsdoelen worden door de maatregel afgedekt?

☐ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.2.13 Bescherming van mobiele spraak- en datadiensten

Mobiele telefoongesprekken en gegevensoverdrachten kunnen gemakkelijker worden afgeluisterd dan vaste telefonie. Versleuteling van mobiele spraak en gegevensoverdracht, evenals hardening en configuratie aan de apparaatzijde beschermen hiertegen.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

Klassieke vaste en mobiele telefonie is vandaag de dag, ondanks chat- en webconferentietoepassingen, nog steeds een van de meest directe en persoonlijke communicatiemiddelen. Het heeft echter enkele kwetsbaarheden en biedt potentiële aanvalsvectoren. De meeste oproepen vanaf een vaste telefoon betreft een mobiele telefoon.

- Het bespioneren van mobiele telefoongesprekken en dataverkeer in het netwerk van mobiele en telefonienetwerkproviders, dat de basisstations met elkaar en met vaste lijnen verbindt en dat onder andere gebaseerd is op IP-technologie
- Het bespioneren van mobiele telefoongesprekken en dataverkeer en deze, via malware die op de mobiele telefoon is geïnstalleerd, doorsturen naar de Command and Control-servers van de aanvallers en die vervolgens misbruik maakt van kwetsbaarheden in het besturingssysteem en de app om directe toegang te krijgen tot de microfoon, luidsprekers, het toetsenbord en het touchscreenscherm, waardoor de versleutelingsapp wordt uitgeschakeld
- Niet-versleutelde mobiele telefoongesprekken en dataverkeer kunnen met goedkope hardware draadloos worden onderschept. Om dit te doen, hoeven aanvallers de mobiele telefoon niet te infecteren of in te breken in het communicatienetwerk. Ze moeten zich echter wel in de ontvangstzone van de betreffende mobiele telefoon bevinden. Aanvallers doen zich bijvoorbeeld voor als onderdeel van het mobiele netwerk om de mobiele telefoon in te loggen op hun afluisterapparaat en vervolgens rechtstreeks gesprekken en dataverkeer op te nemen en te analyseren.

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

De vertrouwelijkheid van gesprekken kan worden gewaarborgd met behulp van spraak- en data-encryptie op OSI Layer 7 (in de communicatie-apps). Hier worden het gesproken woord, de chatgegevens en, indien nodig, de bestandsoverdracht in realtime op het apparaat versleuteld en door de ontvanger gedecodeerd en opnieuw afgespeeld.

De volgende beschermende maatregelen worden aanbevolen:

- Versleuteling van spraak- en datacommunicatie op applicatieniveau door, geschikte en vertrouwde apps en hardware die end-to-end versleuteling uitvoeren volgens de huidige versleutelingsstandaarden en de toepasselijke regels voor gegevensbescherming
- Daarnaast, met behulp van Mobile Device Management (MDM/EMM)-systemen, de centrale configuratie van de eindapparaten door de uitgevende of BYOD-ondersteunende organisatie

om ongewenste gebruikersacties en app-activiteiten te voorkomen die kunnen leiden tot infecties van mobiele telefoons
- Voor een hoger niveau van vertrouwen, het gebruik van mobiele telefoons met een gehard besturingssysteem, dat zorgt voor het exclusieve gebruik van de microfoon en luidspreker door de coderingsapp en het voorkomen van het bespioneren van de cryptosleutels door eventuele aanwezige malware.

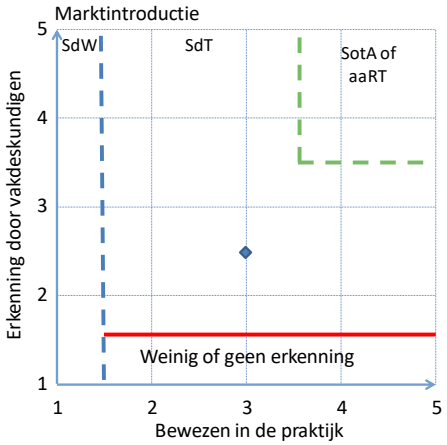
Welke beschermingsdoelen worden door de maatregel afgedekt?

☐ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Classificatie van de stand van de technologie



3.2.14 Bescherming van Instant Messenger communicatie

Instant messaging is de naam die wordt gegeven aan een vorm van digitale communicatie waarbij twee of meer partijen met elkaar converseren door middel van snel verzonden tekst-, beeld- en spraakberichten. Om dit te doen, gebruiken de gesprekspartners een instant messenger om de berichten via een netwerk te verzenden. Als een communicatiepartner niet online is op het moment dat een bericht wordt verzonden, wordt het meestal op een later tijdstip bij de ontvanger afgeleverd. Secure Instant Messaging is bedoeld om instant messages te beschermen tegen ongeoorloofde toegang en wijziging.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

Wanneer informatie wordt uitgewisseld via instant messaging, moet rekening worden gehouden met de volgende bedreigingen:

- Opname, evaluatie en wijziging van de content door een onbevoegde derde partij (man-in-the-middle aanval)
- Identiteitsdiefstal binnen een communicatiesysteem
- Diefstal van een apparaat om instant messaging gegevens achteraf en zonder toestemming te kunnen evalueren
- Onbekende/ongeautoriseerde deelnemers aan een groepschat

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

1. Secure Instant Messaging omvat technische beveiligingsmaatregelen om de vertrouwelijkheid en integriteit van de communicatiecontent te behouden:

- Beveiliging van berichtoverdracht met behulp van up-to-date TLS tijdens het transport
- Gebruik van asymmetrische end-to-end encryptie met een beveiliging die vergelijkbaar is met ten minste RSA 4096 bits
- Ondanks het bezit van de lange-termijn sleutel moet Forward Secrecy, om de gegevens te beschermen tegen latere decodering, ook deel uitmaken van de architectuur g,.

2. Betrouwbare verificatie / authenticatie van identiteiten

3. Beveiliging van toegangsopties en toegangspaden tot de content:

   - Schermvergrendeling op het gebruikte mobiele apparaat (met sterk wachtwoord)
   - Ingeschakelde apparaatversleuteling
   - De gebruikte communicatie-app moet een onafhankelijke veilige opslag van de gegevens bieden en deze beschermen tegen extractie door onbevoegden.

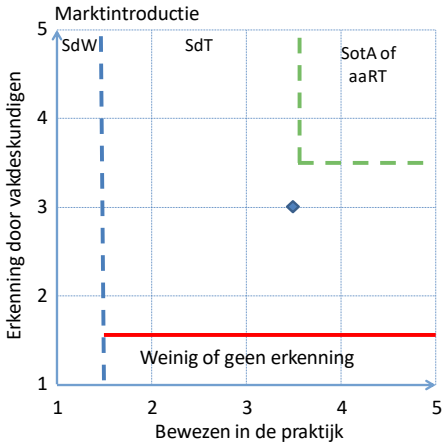
Welke beschermingsdoelen worden door de maatregel afgedekt?

☐ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Classificatie van de stand van de technologie



3.2.15 Bescherming van mobiele apparaten

Het gebruik van Mobile Device Management (MDM) oplossingen vermindert de veiligheidsrisico's die voortvloeien uit het ongecontroleerde, voor zakelijke doeleinden, gebruik van mobiele apparaten. MDM-oplossingen maken het mogelijk om de gebruikte mobiele apparaten centraal te beheren en te configureren.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

1. Gegevensverlies: Als gevoelige gegevens op de mobiele apparaten worden opgeslagen en het apparaat verloren gaat of wordt vernietigd, moet de organisatie mogelijk onherstelbaar gegevensverlies accepteren.
2. Gegevensdiefstal: Als een mobiel apparaat wordt gestolen of gegevens via onveilige applicaties of communicatiekanalen worden gelekt, is de vertrouwelijkheid van bedrijfsgegevens niet langer gegarandeerd.
3. Malware: Mobiele apparaten kunnen worden geïnfecteerd met malware door openbare wifi-netwerken te gebruiken, updates niet te installeren en op een ongecontroleerde manier applicaties van dubieuze bronnen te installeren.

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

MDM-oplossingen stellen bedrijven en organisaties in staat om beleid af te dwingen om onder andere de beveiliging van apparaten en bedrijfsgegevens te verbeteren. MDM-oplossingen voorkomen onveilige communicatie door het gebruik van VPN's, het veilige gebruik van wifi-netwerken en het gebruik van gedeelde applicaties van bekende bronnen. De beveiliging van het apparaat wordt gewaarborgd door afgedwongen sterke authenticatie, nalevingcontroles (zoals het controleren van systeeminstellingen en toegestane applicaties) en de actualiteit van het besturingssysteem en de geïnstalleerde applicaties. In het geval van verlies van het apparaat kunnen op afstand apparaten worden vergrendeld en gegevens worden gewist. De beschikbaarheid en bescherming van gegevens op de apparaten wordt bereikt door de centrale configuratie van de versleuteling en regelmatige gegevensback-up.

Om te voldoen aan de verhoogde functionaliteiteisen voor het gebruik van mobiele apparaten die voor zakelijke doeleinden worden gebruikt, hebben sommige fabrikanten de bestaande MDM-functies met Mobile Application Management (MAM) en Mobile Information Management (MIM) functies, inclusief cloudverbinding, uitgebreid tot Enterprise Mobility Management (EMM)-oplossingen.

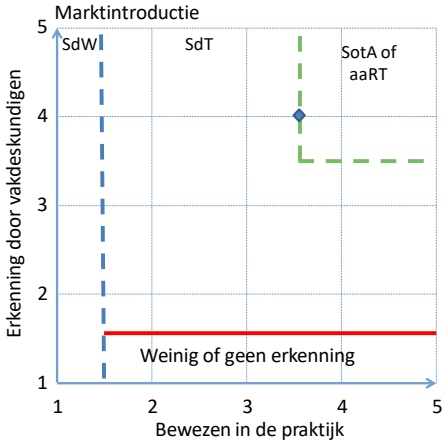
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Classificatie van de stand van de technologie



3.2.16 Router beveiliging

Routers zijn centrale infrastructuurcomponenten die de uitwisseling van netwerkpakketten tussen meerdere netwerken mogelijk maken.

In de context van zakelijke klanten worden routers niet alleen gebruikt als internettoegangsapparaat en voor het routeren van gegevens. In de meeste gevallen worden hiermee ook VPN-netwerken opgezet. Deze toepassingen maken de router tot een bedrijfskritisch onderdeel met specifieke beveiligingsvereisten.

De wereldwijde verspreiding in zowel bedrijfs-, organisatie- als privénetwerken maakt routers het doelwit van verschillende aanvalsmethoden die moeten worden afgeweerd door passende beschermingsmaatregelen. In dit gedeelte worden de bedreigingen voor routers opgesomd en worden de huidige beveiligingen beschreven en beoordeeld.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

Routers worden verondersteld gegevens betrouwbaar en veilig door te sturen en te beschermen tegen ongeoorloofde toegang tot deze gegevens. De volgende bedreigingen/risico's brengen deze doelen in gevaar:

1. Manipulatie van de configuratie
2. Aanvallen die misbruik maken van bekende en niet-gepatchte kwetsbaarheden
3. Aanvallen met behulp van zero-day exploits
4. Aanvallen via IP-telefonieverbindingen
5. Diefstal (vooral routers buitenshuis / mobiele telefoons)
6. Beschikbaarheid aanvallen (DoS-aanvallen)
7. Toegang via ongedocumenteerde interfaces (backdoors)
8. Uitvoeren van foreign code en integreren in botnets
9. Manipuleren van Routeringinformatie

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Voor de bovenstaande bedreigingen zijn er verschillende beveiligingsmaatregelen om risico's te beperken en die hieronder worden samengevat als maatregelbundel "Router Security":

1. Wachtwoordbeveiliging: gebruik van beveiligde toegangsgegevens die zijn beschermd tegen ongeoorloofde toegang en het vermijden van het gebruik van standaard logins
2. Regelmatige bijwerking van de firmware van de router
3. Servicecontracten met de hardwarefabrikant en een gedefinieerde maximale responstijd in het geval dat een ernstige kwetsbaarheid bekend wordt.
4. Als een routerfabrikant geen updates levert nadat een kwetsbaarheid bekend is geworden, moet worden overwogen om fallback-apparaten van derden te gebruiken die niet door de kwetsbaarheid worden getroffen.
5. De router moet op een beveiligde locatie worden geplaatst, bijvoorbeeld een afsluitbare ruimte met gecontroleerde toegang door verantwoordelijke beheerders. Buiten is het vaak niet mogelijk om de router op een beveiligde locatie te plaatsen, daarom moet de router in een dergelijk geval worden uitgerust met een GPS-functie. De router moet zo worden geconfigureerd dat hij controleert of hij zich, bijvoorbeeld na een stroomstoring, nog op de beoogde locatie bevindt. Is dit niet het geval, dan moet hij zijn functie onderbreken.
6. Ter bescherming tegen DoS-aanvallen, moet volgens RFC 2267 gefilterd worden op ongeldige adressen en moeten blokkadelijsten worden ingesteld in de firewall.
7. Alle open en onnodige poorten en interfaces moeten worden gesloten.
8. Indien mogelijk moet de router, om de aanvalsperiode te verkorten, automatisch worden uitgeschakeld tijdens inactiviteit (zoals 's nachts). De installatie van updates mag door deze maatregel niet worden beperkt.
9. Om de impact van succesvolle aanvallen op routers tot een minimum te beperken, moeten verschillende netwerkzones worden ingesteld (netwerksegmentatie).
10. VPN-router: Indien mogelijk moeten VPN-verbindingen niet tot stand worden gebracht via vooraf gedeelde sleutels, maar op basis van certificaten
11. Router als VoIP-gateway: gebruik van apparaten met een geïntegreerde Session Border Controller. Firewalls zijn niet in staat om op toepassingsniveau de SIP-signalering en de RTP-pakketten met de ingesloten spraakinformatie te inspecteren. Hierdoor ontstaat het risico van een aanval via Voice-over-IP-verbindingen. De werking van de router moet centraal worden gecontroleerd.
12. De gebruikte routeringprotocollen moeten cryptografische methoden gebruiken om de ontvangen dynamische routeringinformatie te controleren en ook uitgaande routeringinformatie dienovereenkomstig te voorzien van authenticatie-informatie.

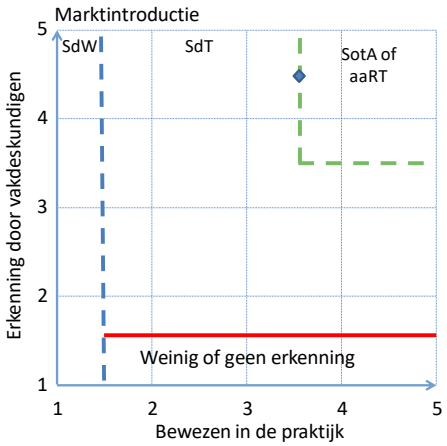
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Classificatie van de stand van de technologie



3.2.17 Netwerkbewaking met IDS

Intrusion Detection Systemen (IDS) en Intrusion Prevention Systemen (IPS) zijn IT-systemen voor het detecteren en loggen van potentiële bedreigingen in het IT/OT-netwerk, waarbij een IPS ook geautomatiseerd verdedigingsmaatregelen initieert.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

- Informatielekken door onderschepping van gevoelige gegevens
- Misbruik van diensten en communicatieprotocollen
- Toegang van IT-systemen van derden tot het IT-netwerk
- Benutting van de mogelijkheden voor netwerk toegang tot IT-systemen
- Knoeien met informatie of software
- Verspreiding van malware in het IT-netwerk

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Een IDS of IPS detecteert en registreert aanvalsactiviteiten en anomalieën in IT- en OT-netwerken. Het doel van beide systemen is om ongeoorloofde toegang en aanvalstypische acties (verkenning, zijwaartse beweging, persistentie) en de introductie van malware zoveel mogelijk te detecteren voordat er schade optreedt. In tegenstelling tot IDS, dat alleen informatie over verdachte en kwaadaardige activiteiten weergeeft en alarmen genereert, kan een IPS ook geautomatiseerd ingrijpen om aanvallen te beperken. Daardoor is het mogelijk specifieke aanvalsvectoren (zoals gemanipuleerde query's die misbruik maken van een bepaalde softwarekwetsbaarheid) te behandelen, bijvoorbeeld door pakketten op netwerkniveau verwijderen. Opgemerkt moet worden dat, bijvoorbeeld in het geval van industriële en productie-installaties en volledig geautomatiseerde vraag-/aanbodprocessen, en ook berichten- en veiligheidsprocessen (zoals brandbeveiliging), directe interventie door een IPS rechtstreeks van invloed is op de beschikbaarheid en kan leiden tot false-positive detectie en ongewenste storingen

Netwerkgebaseerde IDS/IPS-systemen worden als stand-alone oplossingen, maar ook als functie van UTM en Next Generation Firewalls aangeboden. In het geval van client/server-side IDS- en IPS-oplossingen in kantoor-IT worden de functies nu ook afgedicht door moderne EDR-oplossingen (zie ook 3.2.22 Endpoint Detection & Response), die anomaliedetectie, procesgedrag, informatie over cyberdreigingen en bescherming tegen exploits combineren.

Allereerst moeten IDS/IPS-systemen inzicht krijgen in het verkeer. Voor dit doel wordt voor op hardware gebaseerde systemen aanbevolen, om de productieve gegevens te extraheren met behulp van een Test Access Point (TAP) om overeenkomstige overboekingen en interpretaties, zoals kan gebeuren met SPAN-poorten op switches te voorkomen. Om de belasting van de IDS/IPS te verminderen kunnen ook Network Packet Brokers (NPB) worden gebruikt om de relevante gegevens te filteren. Ze stellen je bijvoorbeeld in staat om header/metadata of specifieke pakketlengtes te begrenzen. Of header/metadata voldoende is, en ook de positionering van de IDS/IPS in het netwerk, is afhankelijk van de toepassing.

De detectie van anomalieën is gebaseerd op twee verschillende methoden. Bij "pattern matching" wordt reeds bekende malware gedetecteerd op basis van patronen (signatures), en wordt het misbruiken van een kwetsbaarheid door netwerkpakketten herkend. Nieuwe aanvalspatronen moeten zo snel mogelijk worden geanalyseerd en hun signatures moeten onmiddellijk op een fraudebestendige manier worden opgenomen, anders blijven aanvallen op basis daarvan onopgemerkt.

De tweede methode is gebaseerd op het detecteren van door een aanval veroorzaakte veranderingen in het communicatiepatroon van netwerkcomponenten. Elke communicatie die buiten een verwacht verkeersprofiel valt, wordt beschouwd als een anomalie. Hierdoor kunnen ook nieuwe aanvallen worden gedetecteerd. Het is niet nodig om aanvalspatronen in een database bij te houden. Er moet echter worden gedefinieerd welke communicatiepatronen tot het normale dataverkeer behoren. Hier helpt de toepassing van door machine learning ondersteunde methoden met name om de inspanning die nodig is om handmatige regels op te stellen en te onderhouden, te verminderen of te vermijden, op voorwaarde dat de kwaliteit en kwantiteit van de trainingsgegevens voldoende is.

Een IDS moet in het geval van de detectie van malware of van een aanval, of in het geval van afwijkingen van de geldige Soll-situatie van de communicatie, automatisch overeenkomstige eventmeldingen genereren. Alle eventmeldingen moeten gedurende een voldoende lange periode voor analysedoeleinden in het systeem worden bewaard en indien nodig kunnen worden geëxporteerd in een open of gestandaardiseerd formaat. De eventmeldingen moeten alle relevante informatie bevatten voor de analyse van het event en het initiëren van tegenmaatregelen, zoals gedetecteerde signatures en opvallende communicatieverbindingen. Daarnaast moeten ook gedetailleerde netwerkpakketanalyses mogelijk zijn voor verdere evaluaties. De alarmmeldingen moeten op de beheerconsole duidelijk herkenbaar zijn, bovendien moeten alarmen geautomatiseerd naar gedefinieerde ontvangers worden gestuurd en indien nodig moeten de gedetailleerde gegevens over een vermoedelijke aanval via een exportinterface (syslog, API, webhook, enz.) beschikbaar worden gesteld aan een overkoepelend Security Information en Event Management Systeem (zie hoofdstuk "Attack Detection and Evaluation (SIEM)") voor correlatie en verdere contextuele verrijking (zoals met gegevens van EDR-systemen).

Een IPS moet ook automatisch alle communicatie in het netwerk die de basis vormt van een aanvalspoging blokkeren. Daarbij moet ervoor worden gezorgd dat zoveel mogelijk geen communicatie wordt tegengehouden die niet duidelijk kan worden toegeschreven aan aanvallend gedrag.

Een IDS/IPS moet componenten bevatten om alle communicatie bij netwerkovergangen en binnen interne IT-netwerken te analyseren. In het geval van een tijdelijke uitval van IDS/IPS-componenten moeten de gegevens tijdelijk worden opgeslagen en kunnen ze na gebruik worden samengevoegd en opnieuw geëvalueerd worden. Ongevraagde communicatie van de IDS/IPS-componenten naar derden mag niet worden toegestaan. Bovendien moeten alle IDS/IPS-componenten in het netwerk onherkenbaar zijn, geen invloed hebben op het dataverkeer, geen diensten aanbieden (buiten het beheernetwerk) en zelf beschermd zijn tegen compromittering. De communicatie tussen de afzonderlijke componenten moet vertrouwelijk en integer zijn.

Naast de pure implementatie van een IDS/IPS is ook een holistisch concept voor het monitoren van het netwerk belangrijk. Network Security Monitoring (NSM) is een uitbreiding van IDS/IPS voor een uitgebreider overzicht van alle activiteiten en met bijbehorende contextuele gegevens in het netwerk. De focus ligt op het beschikbaar stellen en voorbereiden van transactie-, sessie- en contentgegevens die kunnen worden gebruikt voor de analyse van het betreffende event.

De door IDS/IPS verzamelde gegevens moeten zo worden opgeslagen, dat ze kunnen worden gebruikt voor verdere analyses (zoals forensisch onderzoek). De bewaartermijnen van de gegevens zijn afhankelijk van de individuele specificaties van de betreffende organisatie.

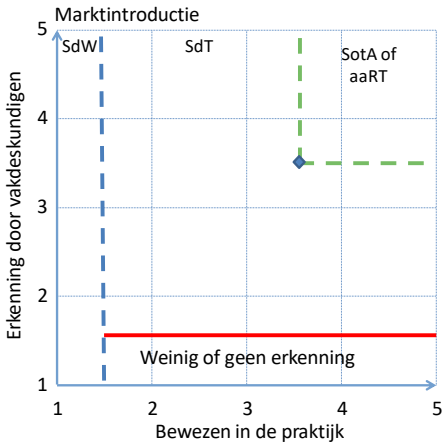
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Classificatie van de stand van de technologie



3.2.18 Beveiliging van webverkeer

Webservers zijn een van de belangrijkste verspreidingsplaatsen van malware. Vanuit geïnfecteerde websites wordt bij gebruikers, meestal zonder dat ze het merken, malware gedownload en uitgevoerd. Als verkeer, als onderdeel van een proxyserver of firewall, tijdens het browsen langs een webfilter wordt geleid, kunnen dergelijke aanvallen worden gedetecteerd en gestopt.

Tegen welke bedreiging(en) voor de IT-beveiliging wordt de maatregel ingezet?

Webservers zijn een van de belangrijkste verspreidingsplaatsen voor malware. Vaak worden geïnfecteerde webservers gebruikt waarbij de provider niet direct betrokken is bij de aanval. Een groot percentage van de webservers heeft permanent beveiligingslekken en kan worden aangevallen door hackers, die vervolgens malware, meestal rootkits, op het systeem plaatsen.

Deze websites worden normaal door de gebruikers bezocht. Wanneer een geïnfecteerde website wordt bezocht, wordt vervolgens onopgemerkt door de gebruiker malware gedownload naar en geactiveerd in het lokale systeem (drive-by downloads).

Daarnaast worden door aanvallers speciaal ter beschikking gestelde webservers gebruikt, die vaak een andere webserver imiteren. In het geval van phishing worden dergelijke valse kopieën van bekende websites aangeboden met als doel gevoelige informatie van de gebruiker, veelal gebruikersnaam en wachtwoord, en bankgegevens, creditcardgegevens, adresgegevens, enz., te verkrijgen

Vaak wordt het werkelijke doeladres (URL met kwaadaardige code of de URL van de geïnfecteerde of neppagina) verhuld door, vaak meerdere keren, geautomatiseerde omleidingen, en via URL-verkorters (Bit.ly, Tiny URL, enz.), maar deze zijn niet betrokken bij de daadwerkelijke aanval. Gebruikers worden naar de speciaal daarvoor bestemde websites geleid via gerichte links in e-mailberichtent, sociale media, enz.

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Om zich tegen dergelijke aanvallen te beschermen, wordt het webverkeer via webfilters geleid. Webfilters beschermen tegen deze aanvallen door de getroffen websites te blokkeren en de door websites geladen gegevens te analyseren op schadelijke code. Webfilters kunnen centraal gebruikt worden, als webfilters in de cloud, als lokaal apparaat, of als software die lokaal op het systeem van de eindgebruiker wordt bediend.

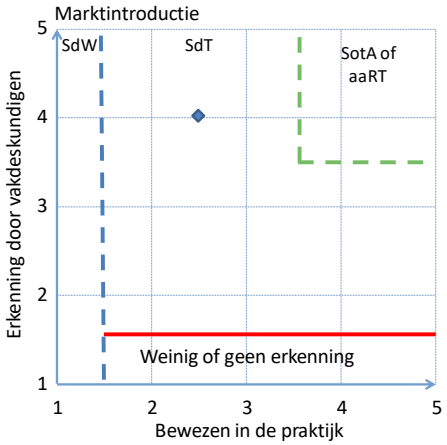
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Classificatie van de stand van de technologie



3.2.19 Beveiliging van webapplicaties

Een web application firewall (WAF) beschermt webapplicaties (homepages, online shops, portals voor thuisbankieren, enz.) tegen aanvallen. De WAF onderzoekt de communicatie tussen gebruiker en webapplicatie op applicatieniveau en blokkeert potentieel kwaadaardig verkeer, zoals SQL-injectie of cross-site-scripting. De term Web Service Firewall (WSF) wordt ook gebruikt voor machine-to-machine communicatie.

In tegenstelling tot een netwerkfirewall, die werkt op OSI Layers 3 en 4, verwerken werken WAF's op OSI Layer 7-Dataverkeer om te beschermen tegen bedreigingen die gericht zijn op het misbruiken van kwetsbaarheden in de beveiliging van applicaties.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

Aanvallen op webapplicaties of webservice-interfaces, zoals

- SQL-injectie
- Cross-site-scripting (XSS)
- Lekken van informatie
- Command-injection
- Andere OWASP-bedreigingen

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Gebruik van een web application firewall (WAF of WSF) stroomopwaarts van de webserver.

Een web application firewall (WAF) onderzoekt de communicatie tussen de gebruiker en de webapplicatie op applicatieniveau en blokkeert potentieel schadelijk dataverkeer. In het geval van beveiligingslekken in de webapplicatie die op korte termijn moeten worden gedicht, is een aanpassing van de WAF meestal voldoende. Een aanpassing of patching van de te beveiligen webapplicatie kan dan achteraf en met voldoende doorlooptijd voor testen worden gepland. Vaak wordt voor aanvallen een combinatie van verschillende kwetsbaarheden misbruikt. Door een centrale kwetsbaarheid via WAF te blokkeren, kunnen dus veel aanvallen snel worden afgeweerd.

De Web Services Firewall (WSF) is een soort WAF speciaal voor machine-to-machine communicatie en wordt ook via http / https afgehandeld. De aanvalsvectoren voor WAF en WSF lijken erg op elkaar. In het navolgende geldt voor het WSF hetzelfde als voor de WAF.

Moderne webapplicaties en -diensten bieden vaak een Application Programming Interface (API) die brede functionaliteit biedt voor flexibel machinegebruik en daarom zelden optimaal beveiligd is.
De WAF beëindigt het versleutelde dataverkeer aan de gebruikerszijde, analyseert de inhoud ervan en stuurt verzoeken die als onschadelijk zijn geclassificeerd in versleutelde vorm door naar de webserver. Schadelijke verzoeken worden geblokkeerd.

De werking van webapplicaties zonder het gebruik van een, als appliance of virtuele, upstream WAF kan niet langer worden beschouwd als state-of-the-art.

Opmerking: In een technische context (softwareontwikkeling) kan SQL in een chat een normale toepassing zijn en moet dan, op basis van risico, worden aangepast bij het configureren van de WAF.

Een WAF moet de volgende kenmerken hebben:

- Overdracht van loggegevens naar SIEM- en anomaliedetectiesystemen met de mogelijkheid om wachtwoorden, creditcardgegevens, enz. te verbergen.
- Clustercapaciteit voor hoge beschikbaarheid en load-balancing
- Bescherming tegen OWASP Top 10-aanvallen, zoals SQL-injectie, Cross-Site Scripting (XSS) en directory traversal via blacklisting, whitelisting en patroonherkenning
- Sterke authenticatie van gebruikers van webapplicaties en services
- Sessiebeheer door sessiecookies te controleren en te manipuleren
- Broken Access Control voorkomt ongeoorloofde toegang tot paden (path traversal), bestanden en API-functies
- Filteren van onnodige http-headers
- Bescherming tegen Cross-Site Request Forgery (CSRF) door header-evaluatie van http-verzoeken, zoals verwijzingsinformatie
- Beveiliging van de Websocket-verbindingen

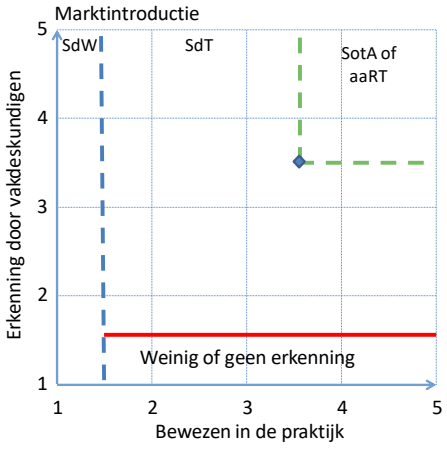
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Classificatie van de stand van de technologie



3.2.20 Bescherming van externe toegang tot netwerken

Externe netwerken moeten voor service- en software-updates toegankelijk zijn via internet. In de industriële omgeving zijn deze deelnemers machinebesturingscomponenten zoals PLC's, aandrijvingen en bedieningsapparaten. In geval van onderhoud en software-updates moet de remote beheerder online met zijn leverancierstools (zoals PLC-programmeersoftware) toegang krijgen tot deze systemen.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

- Ongeoorloofde toegang tot het bedrijfsnetwerk
- Ongeoorloofde toegang tot de doelsystemen
- Geen traceerbaarheid van toegang tot remote onderhoud
- Aftappen of impact van gegevens tijdens een remote onderhoudssessie

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Om onderhoud op afstand mogelijk te maken, worden de doelsystemen meestal via routers met internet verbonden. Deze gebruiken dit vervolgens om een VPN-verbinding tot stand te brengen met een zogenaamde bemiddelingsserver. Deze uitwisseling is het verbindingspunt tussen het doelsysteem en de externe provider die ook een VPN-verbinding met de bemiddelingsserver tot stand heeft gebracht. Aangezien beide plaatsen hun eigen verbinding hebben, heeft elke deelnemer op elk moment de mogelijkheid om deze te beëindigen. De taak van de bemiddelingsserver is om alleen de goedgekeurde doelsystemen vrij te geven voor de betreffende externe provider. Idealiter moet het mogelijk zijn om de externe provider en het doelsysteem te beperken tot Layer 3 (IP, poort, protocol). Dit zorgt voor de toepassingsspecifieke verbinding met het doelsysteem. Afhankelijk van de toepassing kunnen via onderhoud op afstand ook zuivere terminalverbindingen tot stand worden gebracht. Denk hierbij bijvoorbeeld aan web-, RDP-, VNC- of SSH-toegang. Dit is afhankelijk van de beschikbaarheid op het doelsysteem. In het bijzonder moet echter een directe 1:1-netwerkkoppeling van de externe provider naar het netwerk van het doelsysteem worden vermeden.

Versleutelde VPN-verbindingen zorgen voor gegevensintegriteit en bescherming tegen het aftappen van gegevens. 2-Factor-authenticatie moet beschikbaar zijn voor de autorisatie van de remote provider.

Elke remote onderhoudssessie moet worden gelogd. Dit is nodig om, in geval van een beveiligingsincident, de laatste toegangen tot het netwerk en de router te kunnen detecteren. In dit geval moeten de identificatie van de externe provider (IP-adres, naam), het tijdstip en de duur van de verbinding worden vastgelegd. Idealiter wordt dit opgeslagen op de bemiddelingsserver.

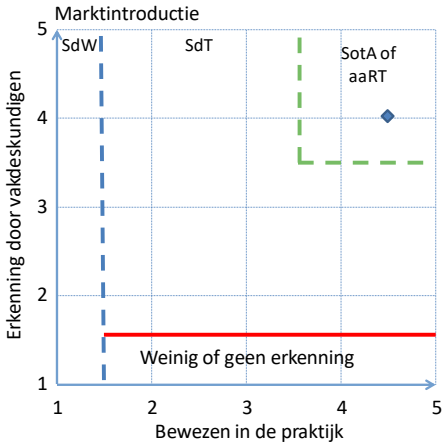
Welke beschermingsdoelen worden door de maatregel afgedekt?

☐ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Classificatie van de stand van de technologie



3.2.21 Hardenen van het systeem

Een effectieve maatregel om het aanvalsoppervlak van IT-systemen te verkleinen, is systeem hardening. Systeem hardening voert, ongeacht of het een fysiek, virtueel of cloudgebaseerd systeem is, een zo veilig mogelijke configuratie uit van het besturingssysteem en de toepassingen van het IT-systeem. Een holistische hardeningaanpak voor de gehele infrastructuur (on-premise en cloud) wordt aanbevolen. IT-systemen van welke aard dan ook kunnen worden gehard. Dit omvat met name client- en serversystemen, maar ook hardwareapparaten (zoals firewalls). Ook het Privileged Access Workstation (PAW), dat wordt gebruikt als een bijzonder geharde client voor beheer met zeer uitgebreide rechten, speelt een speciale rol.

Gangbare besturingssystemen (zoals Microsoft Windows of Linux) hebben standaard geen sterk beperkende beveiligingsconfiguratie en zijn potentieel uitgerust met niet gebruikte componenten. Het zijn juist deze niet gebruikte en niet-geconfigureerde functionaliteiten die vaak worden misbruikt als gateway voor aanvallers. Tijdens hardening van het systeem worden deze functionaliteiten en hun interfaces uitgeschakeld of beperkt en wordt een sterke beveiligingsconfiguratie tot stand gebracht. Dit verhoogt de veiligheid van de systemen aanzienlijk. Daarom moet systeem hardening een integraal onderdeel zijn van de technische beveiligingsstrategie van de organisatie.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

De belangrijkste bedreigingen voor niet-geharde systemen zijn:

- Manipulatie van persoonsgegevens en gevoelige bedrijfsgegevens
- Uitstroom van gegevens (zoals dumps van volledige databases uit databasesystemen)
- Manipulatie of sabotage van bedrijfs- en productieprocessen en verstoring van operationele functies (zoals DDoS)
- Diefstal van identiteiten (zoals overname van accounts met sterke rechten en serviceaccounts)
- Introductie en verspreiding van malware, van welke aard dan ook, naar andere systemen (inclusief ransomware)
- Misbruik van de systeemcapaciteit voor processen van de aanvaller (zoals crypto-mining, het verzenden van spam)
- Uitbuiting als Jump-system voor aanvallers om vervolgens andere systemen aan te vallen (zoals zijwaartse beweging, supply-chain aanval)

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Met name voor het hardenen van systemen moeten de volgende maatregelen in acht worden genomen:

1. Deactivering van componenten

    - Regelmatige beoordeling of geactiveerde services nog steeds voor de werking nodig zijn
    - Deactivering of verwijdering van onnodige componenten / services (inclusief achtergrondservices) van het besturingssysteem,
    - Verwijdering van onnodige software
    - Uitschakeling van onnodige autostart- en geplande processen
    - Deactivering van onnodige, technisch verouderde en onveilige interfaces en protocollen
    - Deactivering van transmissies (zoals telemetriegegevens), voor zover deze niet nodig zijn voor centrale bewaking, met een gecoördineerde richtlijn
    - Uitschakeling van ongebruikte bestandshares
    - Deactivering en beperking van de toegang tot beheerwebsites
    - Indien nodig, deactivering van onnodige poorten en andere fysieke verbindingen
    - Indien nodig, deactivering of beperking van accounts die niet nodig zijn
    - Speciale monitoring voor dual-use tools, ook in de cloud, voor geheime activiteiten (LOL-bins).

2. Activering van hardware gerelateerde beveiligingsfuncties

    - Activering van CPU-beveiligingsfuncties en verificatie van de goede werking van applicaties (zoals Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP) en Control Flow Guard CFG)
    - Activering van het BIOS-toegangswachtwoord, beperking van de opstartvolgorde tot de benodigde apparaten

- Indien nodig, activering van beschermingsprocedures tegen side-channel aanvallen
- Indien nodig, activering van veilige opstartprocedures

3. Beveiliging van de configuratie

   - Het gebruik van communicatieprotocollen om ervoor te zorgen dat gevoelige gegevens en authenticatie-informatie in versleutelde vorm uitgewisseld worden
   - Het gebruik van certificaten om cryptografische sleutels uit te wisselen
   - Deactivering van autostartmechanismen (zoals voor USB-media)
   - Activering van een screensaver met wachtwoordbeveiliging
   - Activering van een sterk gebruikersaccountbeheer (zoals Windows User Account Control)
   - Activering van malwarebescherming op het systeem tijdens het opstartproces (Secure Boot)
   - Verwijdering van onnodige certificaten uit vertrouwde opslag
   - Voorkoming van verwijzingen naar geïnstalleerde services of versienummers
   - Uitschakeling of vervanging door neutrale foutmeldingen van fout- en foutopsporingsberichten voor eindgebruikers
   - Uitvoering van actieve services slechts met een eigen gebruiker en met minimale rechten en waar mogelijk, uitvoering van processen in een geïsoleerde omgeving
   - Activering van logging
   - Beveiliging van toegangspunten voor remote toegang en externe gebruikers
   - Indien nodig, geautomatiseerde installatie van patches en updates
   - Veilige configuratie van software (zoals deactivering van macro's en JavaScript in Office-toepassingen) en browser
   - Speciale bescherming van de Active Directory

4. Minimale toewijzing van autorisaties (need-to-know-principe, least-privilege principe)

   - Regelmatige controle van toegewezen autorisaties
   - Minimale toewijzing van rechten voor beheeractiviteiten
   - Minimale toewijzing van rechten voor bestandssysteem en externe gegevensinterfaces
   - Minimale toewijzing van rechten voor onderhoudsinterfaces / gateways
   - Beperking van de toegang tot de configuratiebestanden van het besturingssysteem
   - Beperking van de toegangsautorisatie tot de fysieke server (vooral om het aansluiten van niet-geautoriseerde externe schijven te voorkomen)

5. Accounts en wachtwoorden

   - Het gebruik van een sterk uniform wachtwoordbeleid voor gebruikerswachtwoorden (zoals wachtwoordlengte, verschillende wachtwoorden voor alle accounts, complexiteit, vergrendelingsteller, wijzigingscyclus, enz.) en gebruik van 2-factor authenticatie (zie hoofdstukken 3.2.1 - 3.2.3)
   - Bescherming van alle accounts met ten minste een wachtwoord dat voldoet aan het wachtwoordbeleid
   - Wijziging van alle bestaande standaardwachtwoorden met een wachtwoord dat voldoet aan het wachtwoordbeleid
   - Vergrendeling van het lokale beheerdersaccount zodra het wachtwoord meerdere keren onjuist is ingevoerd
   - Deactivering of hernoeming van de standaard gebruikersaccounts
   - Deactivering van de lokale gastaccounts
   - Blokkering van het via het netwerk inloggen van lokale gebruikersaccounts
   - Deactivering van de standaard-, test- en anonieme accounts voor alle geïnstalleerde services/softwarecomponenten

6. Netwerkcomponenten

   - Beperkingen op netwerkinstellingen (zoals TCP/IP-configuratie), het uitschakelen van ongebruikte en onveilige netwerkprotocollen (zoals Telnet, FTP, HTTP, SSL)
   - Uitschakelen van ongebruikte netwerkpoorten
   - Voorkomen van een downgrade van de versie tijdens het tot stand brengen van de verbinding ('handshake'), zoals downgrade van TLS 1.3 naar TLS 1.0
   - Tot het vereiste minimum beperken van het aantal verbindingen via een service

- Indien nodig, activering van pakketfilters / firewall en het openen van de minimaal vereiste toegangen

Voor veelgebruikte besturingssystemen zijn publiekelijk op internet gedetailleerde beveiligingsrichtlijnen beschikbaar:

- CIS-benchmarks (Center for Internet Security, Inc.): www.cisecurity.org/cis-benchmarks
- STIG's (Security Technical Implementation Guides): public.cyber.mil/stigs/
- Richtlijnen voor Microsoft-beveiliging: blogs.technet.microsoft.com/secguide/

Een groot aantal van de genoemde hardening maatregelen kan worden geïmplementeerd door technische instellingen. Er kunnen bijvoorbeeld scripts worden gebruikt die het hardenen geautomatiseerd op de systemen uitvoeren. Om in Windows-infrastructuren geautomatiseerde distributie van hardeninginstellingen mogelijk te maken, kan groepspolicy worden gebruikt. Bij het hardenen van bestaande systemen kan hardening leiden tot het falen van functionaliteiten, dus er moet een data back-up gemaakt worden en de hardening moet uitgebreid getest worden.

Een eenmalige systeemhardening zonder continu onderhoud van het beschermingsniveau is niet effectief. Het kan met name worden bereikt door de volgende maatregelen:

- BOM/DSL
- Verandermanagement
- Probleem-/patchbeheer
- Beheer van releases

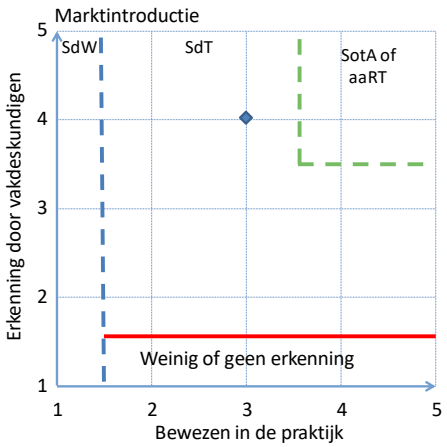
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Classificatie van de stand van de technologie



3.2.22 Endpoint Detection & Response Platform

De bescherming van eindapparaten (zoals pc's, laptops, smartphones of tablets) vereist tegenwoordig veel meer dan alleen een antivirusprogramma. Moderne oplossingen (Endpoint Detection & Response Platforms, EDR) combineren de nieuwste beveiligingstechnologieën om alle soorten cyberaanvallen op client- en serversystemen in verschillende besturingssystemen te stoppen en de daders te identificeren. In tegenstelling tot conventionele oplossingen is er geen specifieke voorkennis, zoals signatures of een eerste slachtoffer, vereist.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

- Malware
- Exploitatie
- Kwaadaardige scripts
- Activiteiten van hackers
- Misbruik van beheertools en van tools met kwade bedoelingen

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

EDR-platforms combineren effectieve detectie- en preventietechnieken om te voorkomen dat clients en servers worden gecompromitteerd, zelfs over de beperkingen van computers en besturingssystemen heen, en zelfs om actieve aanvallers op computernetwerken te ontmaskeren.

Lichtgewicht agents leveren de aanvalsrelevante procestelemetrie gegevens, gebruiken lokaal effectieve machine learning-modellen (kunstmatige intelligentie) en correleren en visualiseren op holistische wijze tactieken, technieken en procedures.

Met behulp van een moderne sensorarchitectuur wordt op signatures gebaseerde bedreigingsdetectie aangevuld met een detectiebenadering voor anomaliedetectie. Dit betekent:

- Detectie van bekende malware via op signatures gebaseerde beschermingscomponenten (veiliger, rekentijd besparend)
- Signatuurloze detectie en actieve blokkering van kwaadaardige code, idealiter via gesuperviseerde machine learning-modellen (bij voorkeur lokale runtime)
- Audit en registratie programma-activiteit in verschillende procesketens en optioneel blokkering van kwaadaardig gedrag
- Bescherming tegen misbruik van kwetsbaarheden binnen legitieme applicaties (exploits en geheugenmanipulatie)
- Idealiter worden gegevens uit verschillende bronnen genormaliseerd en worden detecties gecorreleerd en worden de techniek en tactieken (inclusief gebruikte tools zoals malware, Trojaanse paarden en PowerShell-scripting) en het doelwit van de aanvaller gepresenteerd (exfiltratie van gegevens, plaatsen van backdoors, zijwaartse beweging (verspreiding en verplaatsing) binnen de organisatie, escalatie van bevoegdheden, enz.)
- Optioneel kan bedreigingsinformatie aantonen wie de vermoedelijke actor/tegenstander is (cybercriminaliteit of door een natiestaat gemotiveerde aanval) en welke doelen en industrieën de aanvallers nastreven.

EDR-platforms richten zich op de volledige levenscyclus van een aanvalspoging. Dit is de enige manier om conclusies te trekken over de actoren en hun motivaties, die (NB: conclusies) idealiter contextueel worden aangevuld met actuele dreigingsinformatie. Bovendien kunnen, door externe experts, systeemtelemetriegegevens op schadelijke indicaties worden gecontroleerd.

Naast het detecteren van beveiligingsgerelateerde events, bieden EDR-oplossingen opties voor handmatige en geautomatiseerde reactie op deze bedreigingen, zoals automatische isolatie van het apparaat en deactivering van gebruikersaccounts. Daarnaast zijn er functies ter ondersteuning van responseonderzoeken, zoals mogelijkheden voor externe toegang en het verstrekken van aanvullende gegevens bij het aanbieden van triagepakketten.

Bovendien moet hieraan worden toegevoegd dat, voor een holistische bescherming van eindhulpmiddelen, met name de volgende punten in acht moeten worden genomen:

- Rechten / Rollen (trefwoord: beheerrechten)
- Updatemechanismen (besturingssysteem en software)
- Beperkingen / controle van de geïnstalleerde software (applicatiebeheer)
- Versleuteling van de eindapparaten
- Voorschriften/richtlijnen voor het toegestane gebruik (privégebruik, gebruik in niet-bedrijfsnetwerken, reizen, gebruik van datadragers, opslag van data, back-up, etc.); in het bijzonder wanneer de gebruiker beheerrechten heeft (apparaatbeheer)
- Gebruik van authenticatieprocedures (gebruikersnaam / wachtwoord, pincode, biometrie, enz.)

In de markt is een verdere ontwikkeling naar Extended Detection and Response (XDR) oplossingen is waar te nemen. De combinaties variëren van patchbeheer, apparaatbeheer, back-uptools, versleuteling tot aan netwerkgebaseerde detectie.

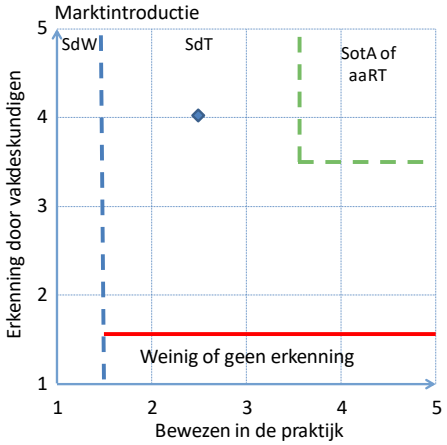
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Classificatie van de stand van de technologie



3.2.23 Webisolatie van internetgebruik

Webisolatie scheidt het werkstation van de gebruiker van de browsersessies en maakt veilig internetgebruik zonder beperkingen op inhoud of functies mogelijk. Browsergebaseerde cyberaanvallen, datalekken/-verlies en de daarmee gepaard gaande productiviteitsbeperkingen en imagoschade worden effectief voorkomen.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

Infectie van de werkplekcomputer, bijvoorbeeld door:

- Kwetsbaarheden in de browser, drive-by downloads, besmettelijke websites
- Ransomware, APT, Trojaanse paarden, virussen, wormen
- Zero-Day exploits
- Kwaadaardige links in e-mailberichtent

en dus de verspreiding van malware in het bedrijfskritische netwerk.

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Het isoleren van browsersessies kan op verschillende manieren worden gedaan. Doorslaggevend hierbij zijn de gebruikte architectuur en de bijbehorende beveiligingsmechanismen. Voorbeelden zijn de "op afstand bestuurbare" browseromgevingen en lokale meerlaags browserisolaties.

Een eenvoudige isolatie van de browseromgeving (bijvoorbeeld via eenvoudige virtualisatie op basis van Hyper-V of browser-sandboxing) biedt een onvoldoende hoog niveau van bescherming tegen de bovengenoemde bedreigingen, aangezien het standaard geen veilig gehard besturingssysteem heeft waarin de browser draait; geen gebruik maakt van extra beveiligde netwerksegmentatie; Veilig kopiëren en plakken niet toegestaan is en geen gebruik maakt van extra beveiligingsfuncties zoals gegevensvergrendelingen. Daarom is deze methode niet geschikt voor het afweren van bedreigingen.

Op afstand bediende browseromgevingen op basis van ReCoBS

Het Remote-Controlled Browser System (ReCoBS) scheidt het internetgebruik op fysiek niveau van het apparaat van de gebruiker. Elke browsersessie wordt uitgevoerd in een speciaal afgesloten omgeving buiten het gevoelige netwerkgebied, binnen een speciaal gehard systeem en op afzonderlijke hardware in een afzonderlijk netwerksegment (DMZ).

Over een technisch beveiligd communicatiekanaal wordt de browser via een videostream vanaf het werkstation op afstand op het externe systeem bediend. De meeste gerichte aanvallen op Windows gebaseerde kwetsbaarheden worden al met succes beperkt in de geharde Linux-omgeving. Andere beveiligingsmechanismen en zones in de algehele architectuur bieden betrouwbare bescherming tegen aanvallen, zelfs als de browser is gecompromitteerd. De fysieke scheiding van het werkstation en het browsersysteem biedt ook bescherming tegen hardware-gerelateerde aanvallen (Spectre, Meltdown, Zombie Load en kwetsbaarheden in de hypervisor).

Met regelmatige tussenpozen (volgens de norm eenmaal per dag) moet het externe systeem via een systeemimage in de oorspronkelijke staat worden hersteld zodat eventuele kwaadaardige code effectief wordt verwijderd. Het is belangrijk om ervoor te zorgen dat het systeembeeld integer blijft.

Het werkstation van de gebruiker heeft op geen enkel moment directe toegang tot het internet nodig en is daarom extra beschermd, bijvoorbeeld tegen het opnieuw laden van kwaadaardige code door besmettelijke documenten die op andere manieren, zoals per e-mail of USB-stick, op de computer zijn terechtgekomen.

Aangezien de ReCoBS-architectuur inhoudt dat vanwege het principe de gangbare standaardfuncties van de browser op het externe systeem worden uitgevoerd, zijn aanvullende ontwikkelingen nodig voor de gebruikersacceptatie, zodat de op afstand bestuurbare browser zich onbeduidend onderscheidt van het lokale browsergebruik en in principe alle gebruikelijke functies zoals persoonlijke bladwijzers, kopiëren en plakken, afdrukken of downloaden en uploaden worden aangeboden.

Voor de optionele overdracht van bestanden (browser downloaden / uploaden) tussen het externe systeem en het werkstation, moet in extra controlemechanismen worden voorzien die verdachte bestanden in quarantaine plaatsen en beheerders op de hoogte stellen. Een voorbeeld van zo'n controlemechanisme is virusbescherming in het dataslot.

Daarnaast is een centraal beheer van de totaaloplossing aan te bevelen, zodat bijvoorbeeld een bestaande directoryservice kan worden gekoppeld en gebruikt om gebruikersrollen te beheren.

Webisolatie op basis van de lokale virtualisatie van de browsertoepassing

Een andere benadering van webisolatie is gebaseerd op de lokale inkapseling van de browsertoepassing door middel van veilige virtualisatie in combinatie met een Windows-gebruikersaccount met beperkte rechten, een beveiligd gastbesturingssysteem en scheiding van internet en intranet via een afzonderlijke VPN-tunnel naar de internetgateway. Dit sluit directe toegang van de browsersessie tot de PC-hardware uit.

Een voordeel van lokale browserisolatie is de mogelijkheid van stand-alone gebruik op mobiele werkstations. Het gebrek aan fysieke scheiding tussen het gevoelige werkstation en het browsersysteem kan het echter mogelijk maken om lokale beveiligingslekken in de processorhardware en -software te misbruiken om via een alle beschermingslagen omvattend exploitpakket in te breken in het eindapparaat.

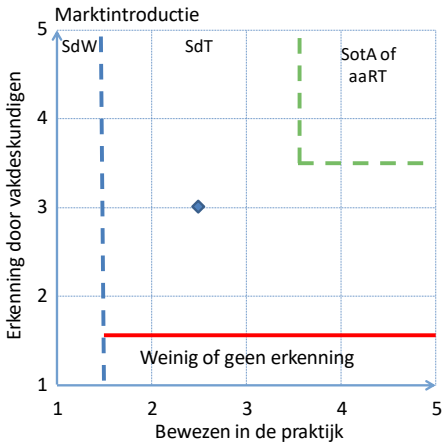
Welke beschermingsdoelen worden door de maatregel afgedekt?

☐ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Classificatie van de stand van de technologie



3.2.24 Inbraakdetectie en -evaluatie (SIEM)

Security Information and Event Management Systems worden gebruikt om afwijkingen te evalueren en aanvallen op de bedrijfsinfrastructuur te detecteren. Ze maken het mogelijk om op holistische wijze beveiligingskritieke gebeurtenissen van de IT-infrastructuur in realtime te detecteren en (deels geautomatiseerd) passende maatregelen uit te voeren.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

SIEM kan helpen tegen de volgende bedreigingen:

- Aanvalsactiviteiten van externe partijen (hackeraanvallen)
- Bedreigingen van insiders (zoals ongeoorloofde toegang tot gegevens van andere afdelingen, computersabotage)
- Compliance overtredingen

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Een SIEM verzamelt centraal log- en eventgegevens van apparaten, netwerkcomponenten, applicaties en beveiligingssystemen. In de SIEM kunnen bijvoorbeeld de volgende gegevensbronnen in kaart worden gebracht:

- Logbestanden van besturingssystemen
- Events van netwerkfirewalls
- Alarmen van inbraakdetectie- en preventiesystemen (IDS/IPS)
- Intelligente netwerksensoren/netwerkbewakingssystemen met informatie over gedetecteerde activa/apparaten, kwetsbaarheden, nalevingsschendingen en afwijkend netwerkgedrag
- Authenticatieservices voor directoryservices (zoals systemen voor eenmalige aanmelding)
- Endpoint Detection & Response Systemen (EDR/XDR)
- Indicatoren voor de identificatie van aanvallers en aanvallen, zoals IP-adressen, hashes, hostnamen, enz. (feeds met informatie over bedreigingen), en bijvoorbeeld ook contextuele informatie over aanvallers voor verrijking

Het beveiligingsteam in de organisatie heeft, door middel van gerichte aggregatie en analyse van beveiligingsrelevante event- en systeemlogfiles, de mogelijkheid om in realtime een holistisch beeld te krijgen van wat er in de IT-oplossing/infrastructuur gebeurt. Hierdoor worden aanvallen, afwijkende patronen en risicovolle processen zichtbaar. Op basis van de opgedane inzichten zijn bedrijven in staat om snel en accuraat te reageren op acute bedreigingen. Op basis van de beschikbare data kunnen de patronen in de nasleep van een aanval worden geanalyseerd (forensisch onderzoek) en kunnen de bestaande maatregelen worden verbeterd.

Moderne SIEM-tools bevatten robuuste en kant-en-klare detectieregels die kunnen worden aangepast aan nieuwe bedreigingsgevallen. De werking van een SIEM-oplossing vereist de integratie van

geschikte bronnen, maar ook de terbeschikkingstelling van aanzienlijke systeembronnen (zoals graph-databases, data-lakes en servers voor exploitatie en beheer). Tegelijkertijd wordt door de continue uitwisseling van gegevens een aanzienlijk gebruik van de bandbreedte gerealiseerd. De daarmee gepaard gaande beheercomplexiteit en de aanschaf- en exploitatiekosten zijn vrij hoog, waardoor klassieke SIEM-oplossingen meestal worden gebruikt in grote en zeer grote bedrijven.

Cloudgebaseerde en door derden beheerde oplossingen zoals SIEM as a Service (SIEMaaS) zijn een eigentijds alternatief met eenvoudig te berekenen kosten. Ze maken het ook mogelijk om de technologie te gebruiken in kleine en middelgrote bedrijven. Ook kan een modern endpoint detection & response platform (EDR/XDR) met zijn interfaces voor Security Orchestration, Automation and Response (SOAR), User and Entity Behavior Analytics (UEBA), netwerkbeveiligingsproducten, zoals next-generation firewalls en geïntegreerde threat intelligence, een verstandig alternatief zijn.

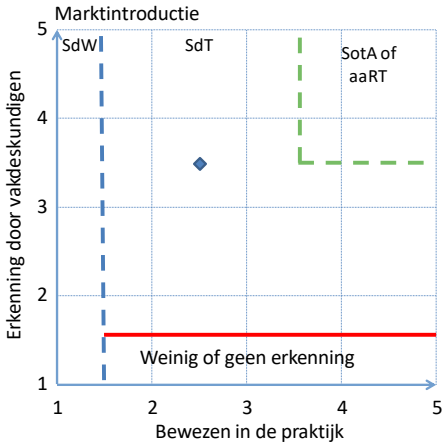
Welke beschermingsdoelen worden door de maatregel afgedekt?

☐ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Classificatie van de stand van de technologie



3.2.25 *Vertrouwelijke gegevensverwerking in de cloud*

Toegang, met de uitgebreide rechten van beheerders, tot gegevens tijdens de verwerking is van oudsher alleen beveiligd tegen misbruik van de toegangsrechten door middel van organisatorische of reactieve maatregelen. Met behulp van confidential computing zijn deze gegevens fraudebestendig en preventief beschermd tegen ongeoorloofde toegang. Dit is belangrijk voor toepassingen op het gebied van cloud computing. Vertrouwelijke gegevensverwerking voldoet aan de behoefte aan bescherming wanneer clouddiensten worden gebruikt voor kritieke infrastructuren of voor gevoelige gegevensverwerkingactiviteiten, zoals in de geneeskunde, de industrie of gereguleerde gebieden.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

Cloudbeheerders zijn verantwoordelijk voor de probleemloze werking van hun systemen. Om deze taak te kunnen vervullen, krijgen ze tal van toegangsrechten. Ze kunnen bijvoorbeeld de systeemconfiguratie aanpassen en de inhoud van het geheugen uitlezen. Dit betekent dat gegevens op weg naar de cloud, in cloudopslag en tijdens verwerking in de cloud niet alleen kunnen worden gecompromitteerd door aanvallen van derden, maar ook door onwettige handelingen van medewerkers van cloudservice providers.

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Eerdere benaderingen van gegevensback-up waren gebaseerd op gegevens in rust (opslag) en gegevens tijdens het transport (netwerk). Confidential Computing richt zich op de bescherming van gegevens tijdens de verwerking. Dit is een van de buitenwereldgebied afgeschermde omgeving of capsule (virtuele machine, applicatie of functie), waarin de volledige gegevensverwerking in een niet-versleutelde toestand plaatsvindt. Deze afscherming kan direct op de processorchip van de servers worden geïmplementeerd (hardware-based trusted execution environment) en/of over meerdere servers tegelijk. Om de gegevens te kunnen verwerken, moet de benodigde sleutel in de capsule aanwezig zijn. Als een aanvaller zou proberen toegang te krijgen tot het ingekapselde gebied, worden onvermijdelijk de daar verwerkte niet-versleutelde gegevens uit voorzorg verwijderd. Om de veiligheid te vergroten, kunnen de capsules na voorafgaande verificatie door onafhankelijke auditors worden met behulp van bekende cryptografische geheimen verzegeld.

In het geval van gegevensverwerkingsystemen die zijn uitgerust met de maatregelen die zijn samengevat onder de algemene term "confidential computing", kan één enkele beheerder geen toegang krijgen tot de gegevens die op de server worden verwerkt. Alleen door een kwaadwillige coalitie van verschillende onafhankelijke partijen (zoals een systeembeheerder samen met een onafhankelijke auditor) kunnen de technische maatregelen overruled worden. Dit verkleint de kans op oneigenlijke toegang met enkele ordes van grootte.

De vertrouwelijke gegevensverwerking

- maakt het mogelijk gegevens in centrale infrastructuren te verwerken, zonder deze bloot te stellen aan de mogelijkheid van kennis door de providers van deze centrale infrastructuur,
- biedt gebruikers meer controle en, afhankelijk van de audit, transparantie
- biedt nieuwe graden van vrijheid, omdat er nieuwe toepassingen denkbaar zijn die op grond van conventionele gegevensbeschermings- en veiligheidsoverwegingen niet op een wettelijk conforme manier zouden kunnen worden geïmplementeerd.

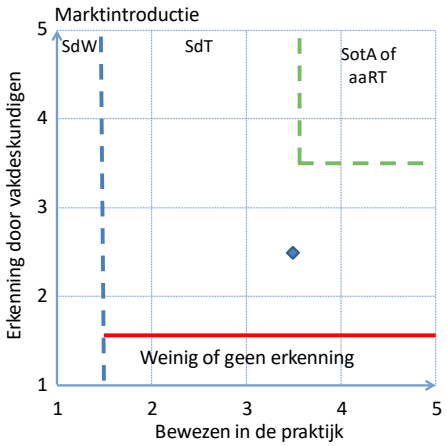
Welke beschermingsdoelen worden door de maatregel afgedekt?

☐ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.2.26 Sandboxing voor analyse van kwaadaardige code

Sandbox-technologie wordt gebruikt om potentieel gevaarlijke bestanden uit te voeren in een geïsoleerde omgeving en te controleren op kwaadaardig gedrag. Uitvoeren in een separate omgeving voorkomt mogelijke infecties.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

- Hackeractiviteiten in de brede zin van het woord
- Malware (virussen, Trojaanse paarden, enz.)
- Phishing

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Het gebruik van de sandboxing-methode voor geautomatiseerde malware-analyse is in twee gebruiksscenario's gebruikelijk.

Perimeter Sandboxing

In het kader van perimeter sandboxing worden bestandsbijlagen (zoals documenten uit de actieve omgeving, maar ook embedded content zoals scripts) uit e-mailberichten meestal geautomatiseerd uitgevoerd. De sandbox-analyse genereert bij de e-mailgateway voor de gebruiker meestal een latentie in de toegang tot de onderzochte bestandsbijlage die varieert van enkele seconden tot minuten.

Sandboxen kunnen ook worden gebruikt bij de webgateway (next-generation firewall of proxy), bijvoorbeeld om gedownloade programma's te controleren. Ook hier wordt, totdat het bestand wordt afgeleverd bij de gebruiker vertraging veroorzaakt, daarnaast beïnvloedt het gebruik ervan ook het gedrag van de browser en webgebaseerde software. Daarom wordt naast de klassieke sandbox methode (eerst controleren, dan met een vertraging afleveren) het bestand met een parallelle controle ook afgeleverd bij het eindapparaat. Als in deze laatste procedure kwaadaardige code wordt geïdentificeerd, worden vervolgmaatregelen genomen. Deze omvatten netwerkisolatie en blokkering van "command and control"-adressen die zijn bepaald tijdens de uitvoering van de sandbox.

Sandbox voor forensisch onderzoek van bestanden als onderdeel van een opsporing of onderzoek

Door de sandboxen te verbinden met Next-Generation Antivirus producten (op machine learning gebaseerde antivirus) en EDR-oplossingen (endpointdetectie en -respons), kunnen bestanden met een kwaadaardige prognose of van gedetecteerde en actief verhinderde aanvalsketens veilig buiten de actieve omgeving worden uitgevoerd. De uitvoering maakt het vervolgens mogelijk om verdere relevante indicatoren te extraheren (bestanden/hashes, URL's, IP-adressen, registeractiviteit, enz.), waardoor een onderzochte zaak meer context kan krijgen en zelfs de toewijzing van een vermoedelijke aanvaller mogelijk is.

Omdat sandbox-oplossingen vrij wijdverspreid zijn, proberen aanvallers detectie in een sandbox steeds weer te voorkomen. Bij het uitvoeren van hun kwaadaardige code proberen ze bijvoorbeeld te bepalen of het een gevirtualiseerde runtime-omgeving is, zoals gebruikelijk is in sandboxen, of een actieve omgeving met bepaalde programma's/processen en andere specifieke kenmerken. De kwaadaardige code zal zich dan, om detectie te voorkomen, meestal onschadelijk gedragen. Ook dit gedrag kan echter worden gedetecteerd in de sandbox en worden gebruikt om verdachte inhoud te identificeren (kat-en-muis principe).

De exploitatie van "0-day exploits" / zero-day threats, d.w.z. kwetsbaarheden die voorheen onbekend waren bij het publiek, kan ook leiden tot sandbox-bypasses. Het kan ook gebeuren dat de geëmuleerde runtime-omgeving niet overeenkomt met het slachtoffersysteem en dat het gedrag bij uitvoering in de sandbox dus anders is, dan dat op het doelsysteem van een aanval. Het is daarom noodzakelijk om deze tactieken, bekend als Sandbox-Evasion, onder de knie te krijgen, bijvoorbeeld door statische en dynamische analyse te combineren.

Sandboxen blijven grote voordelen bieden vanwege hun hoge mate van automatisering om de noodzaak van handmatige analyse van kwaadaardige code (malware reverse engineering) door een expert enorm te verminderen.
Er is een groot aantal commerciële en open-source sandboxen. Deze worden meestal als kostenintensieve hardwareoplossingen aangeboden, maar ook als publiek of privaat aangeboden cloudoplossingen. Sinds enige tijd wordt sandbox-technologie ook gebruikt in browsers om veelvoorkomende soorten aanvallen in een vroeg stadium te detecteren.

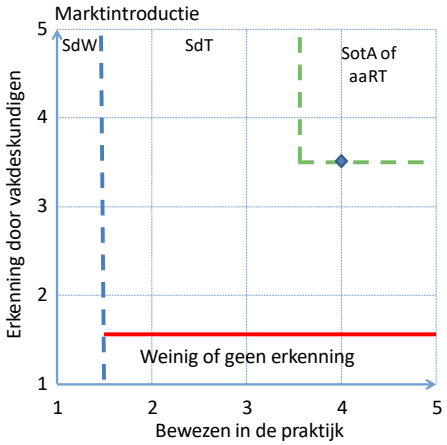
Welke beschermingsdoelen worden door de maatregel afgedekt?

☐ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.2.27 Cyber Threat Intelligence

Cyber threat intelligence is een belangrijke basisbouwsteen van de moderne verdedigingsstrategieën en biedt indicatoren, rapporten en diensten om zich te informeren over de huidige aanvalssituatie, om cyberaanvallen te detecteren, om de vermoedelijke daders identificeren en om tegenmaatregelen af te leiden.

Cyber Threat Intelligence is onderverdeeld in drie toepassingsgebieden:

- Tactical Cyber Threat Intelligence, dit omvat, hun effectiviteit te vergroten, malware-analyse en de import van enkelvoudige, statische en gedragsmatige dreigingsindicatoren in defensieve IT-beveiligingsoplossingen zoals netwerk-, endpoint- en applicatiebeveiligingoplossingen om. Indicatoren die worden verkregen door informatie over cyberdreigingen kunnen een belangrijke rol spelen bij maatregelen zoals het patchen van systemen.
- Operational Cyber Threat Intelligence, dit wordt gebruikt om de kennis over een aanvaller, zijn vaardigheden, infrastructuren en aanvalstactieken, en ook technieken en procedures (TTP's) te verbeteren. Deze informatie kan worden gebruikt om cybersecuritymaatregelen zoals incidentanalyse, incidentrespons en proactieve threat-hunting veel gerichter uit te voeren. Dit verbetert de prestaties van cyberbeveiligingspersoneel (zoals van het Security Operation Center of CERT), experts op het gebied van threat hunting, vulnerability managers, incident response analisten en insider threat-defense experts.
- Strategische dreigingsinformatie maakt het mogelijk om een beter inzicht te krijgen in de huidige dreigingsituatie (dreigingsanalyse), het afleiden van trends en de motivatie van individuele aanvalgroepen. Het ondersteunt strategische zakelijke beslissingen om de cyberbeveiliging te verbeteren.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

Cyber Threat Intelligence informeert over alle soorten huidige en potentiële cyberdreigingen en helpt zich ertegen te verdedigen.

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Tactische informatie over cyberdreigingen (TM)

Integratie van dreigingsindicatoren (feeds) in bestaande endpoint- en netwerkdetectie- en responssystemen, systeembeheeroplossingen, firewalls, IDS/IPS- en SIEM/SOAR-oplossingen, met als doel echte aanvallen te identificeren en analyses (inclusief retro hunting) te ondersteunen en compromittering te voorkomen. Voor een optimale effectiviteit moeten de indicatoren voor het detecteren en voorkomen van cyberaanvallen geautomatiseerd kunnen worden gebruikt. De bronnen voor indicatoren voor dreigingsinformatie kunnen het mogelijk maken conclusies te trekken over de betrouwbaarheid ervan en worden gedifferentieerd in:

- Open-source Intelligence (OSINT),
- events van particuliere honeypot-systemen,
- inzichten uit aanvalsanalyses van echte klantomgevingen, of het
- onderzoekswerk door inlichtingendeskundigen

Operationele Cyber Threat Intelligence (TM/OM)

Organisaties die een Security Operation Center (SOC) exploiteren en mogelijk een eigen Computer Emergency Response Team (CERT) hebben, gebruiken dreigingsinformatie operationeel om zich continu te informeren over de actoren en hun TTP's. Naast toegang tot indicatoren bieden uitgebreide platforms voor bedreigingsinformatie ook verschillende rapportformaten (nieuwsberichten, situatierapporten en aanvallerprofielen) en toegang tot malwaredatabases, sandbox-technologie voor geautomatiseerde malware-analyse en reverse engineering van malware. Verder moet er de mogelijkheid zijn om rechtstreeks bij de aanbieder contact op te nemen met analisten en om onderzoeksverzoeken (RFI's) in te dienen.

Strategische Threat Intelligence (OM)

Zowel op het gebied van informatiebeveiliging als de algemene/groepsbeveiliging van grote bedrijven maken gebruik van threat intelligence om een zo compleet mogelijk beeld van de situatie te creëren. De focus ligt op de geopolitieke situatie en op branchespecifieke en wereldwijde trends in het dreigingslandschap. Toegang tot een gespecialiseerde medewerker bij de provider breidt uw eigen team virtueel uit en zorgt ervoor dat directe toegang tot de datapool wordt geboden en ook dat klantspecifiek onderzoekswerk optimaal wordt uitgevoerd.

Aanbieders van moderne IT-beveiligingsoplossingen leveren, integreren en automatiseren bedreigingsinformatie, zodat dreigingsindicatoren en relevante aanvalstelemetrie op zinvolle wijze aan elkaar worden gekoppeld, preventieve maatregelen worden geautomatiseerd en attributie van aanvallers mogelijk wordt gemaakt zonder dat er extra systemen en zelfs human resources nodig zijn.

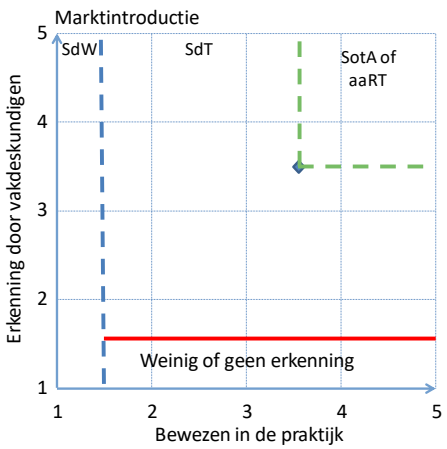
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.2.28 Beveiliging van IT-beheersystemen

IT-beheersystemen zijn clients en servers die andere IT-systemen met behulp van beheertoepassingen beheren en bewaken. In vergelijking met standaard werkstations bevinden IT-beheersystemen zich meestal in speciale netwerksegmenten waarin aanvullende netwerkprotocollen worden gebruikt en van waaruit de beheerinterfaces van systemen kunnen worden bereikt. Door dit bijzondere gebruik van IT-beheersystemen vormen deze systemen een risico met een groot potentieel voor schade (zoals toegang door onbevoegden). Daarom moeten er voorschriften en maatregelen worden genomen die op dit risico zijn afgestemd, om te beschermen tegen ongeoorloofde toegang en om een veilig IT-systeembeheer te handhaven, in het bijzonder met betrekking tot de bescherming van de accounts met speciale rechten die op de systemen worden gebruikt en tot de noodzakelijke verbindingen.

Vereisten voor IT-beheersystemen

IT- beheersystemen moeten worden beveiligd in overeenstemming met de maatregel voor systeemhardening (zie hoofdstuk 3.2.21).

Er moeten voorschriften en maatregelen worden vastgesteld voor het gebruik en de behandeling van IT-beheersystemen en voor de bescherming ervan. Alvorens toegang te verlenen aan een gebruiker, moet de gebruiker eerst deze regels aanvaarden en zich ertoe verbinden deze na te leven. Een overtreding van de gedefinieerde voorschriften moet worden vastgesteld en gevolgen hebben.
Toegang tot IT-beheersystemen mag alleen worden verleend aan gekwalificeerde medewerkers en voor hen worden goedgekeurd. IT-beheersystemen mogen uitsluitend worden gebruikt voor het beheer van systemen en moeten in overeenstemming met hun beschermingsvereisten worden beveiligd met hardening maatregelen en sterke authenticatiemethoden. Hun beschermingsvereisten moeten worden geïdentificeerd en door passende maatregelen worden beschermd.

Toegang tot IT-beheersystemen is moet alleen na succesvolle authenticatie via een beveiligde inlogprocedure, voor geautoriseerde beheerders mogelijk zijn. Dit vereist een geschikte authenticatieprocedure voor de identificatie van de gebruiker, die voldoet aan de beschermingsvereisten van het te beheren systeem (zoals multi-factor authenticatie, zie hoofdstuk 3.2.3). Bij het invoeren van toegangsgegevens, zoals wachtwoorden en pincodes, mogen deze gegevens niet door het systeem worden weergegeven. Bij het via het netwerk inloggen op IT-beheersystemen moeten de gegevens die worden gebruikt om de gebruiker te authenticeren in gecodeerde vorm worden met behulp van beveiligde protocollen uitgewisseld. Inactieve externe sessies moeten na een bepaalde periode automatisch worden uitgelogd/beëindigd.

Als het beheer een verbinding vereist met een netwerksegment met systemen met een hoge of zeer hoge beveiligingseis (zoals naar een netwerksegment met SCADA/ICS-systemen), moeten het beheer en de netwerkverbinding via een jumpserver/proxyserver in een DMZ tussen deze netwerksegmenten plaatsvinden.

Er moeten minimumnormen komen voor wachtwoorden voor de IT-beheersystemen. Deze systemen moeten ook worden geïntegreerd in de modernste autorisatiesystemen, waarbij de verbinding en het autorisatiesysteem zelf bijzonder beveiligd/gehard moeten zijn. Verder moeten er gepersonaliseerde accounts worden gebruikt, die uniek aan een persoon kunnen worden toegewezen. Standaardgebruikers en wachtwoorden mogen niet worden gebruikt.

Er moet voor worden gezorgd dat op IT-beheersystemen alleen toegestane softwarecomponenten, programma's en scripts worden uitgevoerd. Als een toevoeging van softwarecomponenten, programma's of scripts nodig is, moet als onderdeel van een overeenkomstig proces de goedkeuring worden gegeven voordat dit wordt gebruikt en moet het gebruik worden gedocumenteerd en gecontroleerd.

Op IT-beheersystemen moeten de inlogprocessen en activiteiten van de beheerders worden gelogd, zodat kan worden herleid welke activiteiten door welke personen (accounts) zijn uitgevoerd. Om de traceerbaarheid van de uitgevoerde activiteiten te garanderen, mogen beheerders de logfile- en auditlogfiles van hun eigen activiteiten (met hun accounts) niet wijzigen of verwijderen. Voor kritieke beheeractiviteiten moet het meer-ogen principe worden toegepast.

Als voorbeelden voor de inrichting worden de volgende maatregelen voor een passende bescherming worden aanbevolen:

- ISO/IEC 27002
  De norm bevat aanbevelingen voor de implementatie van de maatregelen die vereist zijn in ISO/IEC 27001 Annex A voor toegangscontrole en voor de operationele beveiliging van systemen die ook van toepassing zijn op IT-beheersystemen. Als certificering conform ISO/IEC 27001 wordt nagestreefd, dan moeten deze maatregelen binnen het toepassingsgebied van ISMS worden geïmplementeerd. Implementatie-instructies voor deze maatregel zijn voornamelijk te vinden in de secties 9 "Toegangscontrole" en 12 "Operationele beveiliging".
- BSI IT-Grundschutz-Kompendium
  Het BSI IT-Grundschutz-Kompendium beschrijft in de modules SYS.1, SYS.2 en IND.1 talrijke maatregelen voor de bescherming van systemen. Deze bouwstenen zijn ook relevant en toepasbaar op IT-beheersystemen. Implementatie van de genoemde eisen voor een hoge of zeer hoge bescherming in de bouwstenen wordt aanbevolen.
- BDEW whitepaper: Eisen voor veilige controle- en telecommunicatiesystemen
  De BDEW whitepaper bevat ondersteunende informatie voor het beveiligen van IT-beheersystemen, zoals het gebruik van veilige protocollen en jump servers voor (remote) access en het plaatsen van systemen in dedicated netwerkzones.

De vereisten voor operationele beveiliging en toegangsbescherming van IT-beheersystemen moeten periodiek (ten minste jaarlijks) worden getoetst op volledigheid en geschiktheid en worden in overeenstemming met een toegangs- of toegangscontrolebeleid bijgewerkt.

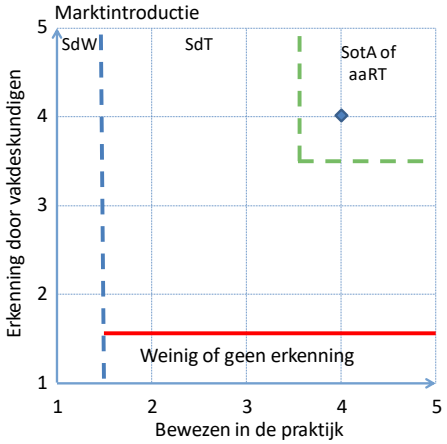
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.2.29 *Monitoring van directoryservices en segmentatie op basis van identiteit*

Bij een groot deel van de ernstige cyberaanvallen door staatsgemotiveerde actoren en cybercriminelen zijn directoryservices en gebruikersaccounts betrokken. Het gaat onder meer om complexe aanvallen via de supply-chain en als gevolg daarvan spionage en sabotage. Het is daarom essentieel voor bedrijven en organisaties om hun aanvalsoppervlak te verkleinen en onnodige risico's in een vroeg stadium te identificeren en te vermijden. Aanvalspogingen en ongebruikelijke toegang moeten worden gedetecteerd zodra ze zich voordoen en in realtime worden ingeperkt, zelfs als de aanvaller gebruikmaakt van vastgelegde, geldige toegangsgegevens en Endpoint Protection en IPS-systemen die mislukken.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

- Aanvallen die misbruik maken van gevangen/gelekte gebruikersnamen en wachtwoorden (zoals inloggegevens die na een inbreuk zijn verhandeld op het dark-web) en waarbij geen malwarecomponent betrokken is
- Misbruik van kwetsbaarheden in directoryservices (onvoldoende beveiligde service accounts)
- Zijwaartse beweging van een aanvaller in de organisatie
- Compromittering en misbruik van accounts met speciale rechten en escalatie van bevoegdheden

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Beoordeling / audit van directory services: Moderne beveiligingsoplossingen combineren de hygiënestatus van directoryservices zoals Microsoft Active Directory, Microsoft Entra ID en andere "Identity as a Service"-oplossingen om kwetsbaarheden profylactisch te behandelen en om risicoprofielen op te stellen. Waaronder:

- Detectie van slecht beveiligde serviceaccounts
- Identificatie van verborgen toegangsrechten die verder gaan dan groepslidmaatschap, zoals delegatie en misbruik van geprivilegieerde SID's,
- Detectie van aanvalspaden naar accounts met speciale rechten die doorgaans alleen worden ontdekt in het kader van complexe audits (zoals via tools zoals SharpHound / Bloodhound)
- Monitoring van bedreigingen met darknet-monitoring

Real-time monitoring en analyse van al het relevante authenticatieverkeer, zowel lokaal, zoals Kerberos, NTLM, LDAP, RDP, RPC, enz., als van cloudgebaseerde IDaaS- en federatiediensten om aanvalspogingen en het gebruik van zogenaamde verkenningstools te detecteren en het Security Operation Center te voorzien van uitgebreide en verrijkte informatie. Integratie met cloudgebaseerde services kan ook geolocatie gerelateerde afwijkingen vastleggen en afwijkingen van het normale gebruik detecteren.

Op basis van de individuele beschermingsbehoeften van de betreffende organisatie kan vervolgens, rekening houdend met de risicoprofielen, een identiteitsgerelateerde set van regels worden geïmplementeerd, die bijvoorbeeld voorkomen dat gebruikersaccounts met een slechte risicoscore toegang krijgen tot kritieke applicaties en lokale kritieke bronnen. Het moet ook mogelijk zijn om geautomatiseerd te reageren op ongewoon gebruikersgedrag en maatregelen te eisen, zoals het aanvragen van een extra authenticatiefactor (MFA). Dit maakt bescherming mogelijk die de focus van gespecialiseerde klassieke oplossingen zoals Privileged Access Management (PAM) combineert met die van User & Entity Behavior Analytics en tegelijkertijd eenvoudig in de praktijk kan worden toegepast, bijvoorbeeld door een sensortoepassing op de directoryservers te implementeren, en ook API-gebaseerde integratie in Federation Services en Cloud Directory Services. Hier vermindert de toepassing van machine learning-modellen de inspanning aanzienlijk[17].

De consistente segmentatie van identiteiten binnen identity providers, bijvoorbeeld in de veelgebruikte directoryservice Microsoft Active Directory, is een effectieve maatregel om zijwaartse verplaatsing over gebiedsgrenzen te voorkomen. Alle identiteiten en hun bijbehorende bronnen (zoals gebruikersgroepen en computeraccounts) zijn geordend in logisch gescheiden lagen binnen de identity provider en strikt van elkaar gescheiden. In het geval van compromittering kan de toegang van een aanvaller tot de identiteiten binnen een enkele laag niet worden uitgesloten, maar segmentatie voorkomt dat deze zich naar andere lagen verspreidt. Dit houdt niet-aangetaste gebieden beschermd en vermindert het risico op een volledige compromittering van het identiteitssysteem aanzienlijk. Deze benadering is conceptueel gebaseerd op netwerksegmentatie, de afbakening is echter niet fysiek, maar logisch binnen de identity store, bovendien moeten passende richtlijnen worden opgesteld en gehandhaafd om een overgang tussen de ploegendiensten te voorkomen. De implementatie van dit principe is in de praktijk vaak bekend onder de termen "tier model" en in uitgebreide vorm als "plane model"; Microsoft verwijst hier ook wel naar als het "Enterprise access model" (EAM).

Let op: Alle bovengenoemde deelgebieden zijn belangrijke bouwstenen en dragen actief bij aan de implementatie van een Zero-Trust Framework. Toegangsrechten kunnen effectief worden geïmplementeerd, zelfs zonder of in aanvulling op beperkingen aan de netwerkzijde (firewalls). Hier

[17] Zie ook hoofdstukken: 3.2.1 Authenticatie, 3.2.3 Multifactorauthenticatie en 3.2.24 Inbraakdetectie en -evaluatie (SIEM)

moet ook rekening worden gehouden met het aspect gegevensbescherming, vooral als het gaat om de analyse van gebruikersactiviteiten.

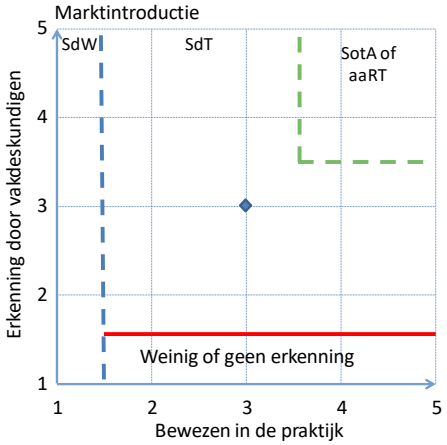
Welke beschermingsdoelen worden door de maatregel afgedekt?

☐ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.2.30 Segmentatie en scheiding van netwerken

Het splitsen van netwerken door middel van netwerksegmentatie en -scheiding is een effectieve maatregel om bedreigingen voor de beschikbaarheid, vertrouwelijkheid en integriteit van netwerken en de systemen die ze bevatten te verminderen. Segmentatie en scheiding ondersteunen ook bescherming als onderdeel van de defense-in-depth aanpak.

Netwerksegmentatie is het proces waarbij een netwerk wordt opgedeeld in verschillende segmenten, die elk functioneren als afzonderlijk subnetwerk. De communicatie tussen deze segmenten wordt beperkt via gedefinieerde zonegrenzen (Boundary Protections) met een controle/bewaking van de netwerkverbindingen. Zonegrenzen tussen netwerken, zoals tussen informatietechnologie (IT) en operationele technologie (OT), verminderen veel van de risico's die samenhangen met het IT-netwerk, zoals malwarebedreigingen. Zonescheiding of segmentatie beperkt de toegang tot systemen, gegevens en applicaties en beperkt de communicatie tussen netwerken. Deze aanpak beschermt segmenten in het netwerk tegen aanvallen van al aangetaste segmenten.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

- Laterale beweging van aanvallers in het netwerk (Network Lateral Movement)
- Ongehinderde verspreiding van malware in netwerken
- Bedreigingen van insiders (zoals ongeoorloofde toegang tot systemen vanaf andere afdelingen of locaties).
- Ongeoorloofd en kwaadwillig verkeer kan moeilijker te identificeren zijn vanwege de netwerkgrootte en datavolumes
- Benutting van de mogelijkheden voor toegang tot IT-systemen in een netwerk
- Verlies van beschikbaarheid, integriteit en vertrouwelijkheid van een groot aantal systemen als deze in een plat netwerk werken en worden gecompromitteerd
- Verlies van beschikbaarheid van kritieke systemen in het netwerk als gevolg van aanvallen op niet-kritieke systemen die minder beveiligingsmaatregelen hebben

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Voor netwerksegmentatie moet een netwerk worden opgedeeld in verschillende zogenaamde netwerkzones (of subnetwerken), waarbij een netwerkzone een logische groep vormt van apparaten, applicaties en systemen met gemeenschappelijke beveiligingseisen (dezelfde beschermingseisen). Het gebruik van kritische en niet-kritische systemen in een netwerkzone, zelfs als ze thematisch kunnen worden gegroepeerd of een hoge mate van communicatie met elkaar hebben, is niet toegestaan.

Netwerkzones kunnen logisch (zoals door VLAN's) en/of fysiek (zoals door een speciale Switch-infrastructuur voor de zone) worden gescheiden. De beslissing of een fysieke scheiding nodig is, moet worden genomen op basis van wettelijke vereisten en met behulp van een risicogebaseerde aanpak.

Al het dataverkeer tussen de verschillende netwerkzones moet via gedefinieerde en passende zoneovergangen plaatsvinden en moet vooraf worden vrijgegeven. Bij zone-overgangen moet beperking, controle en bewaking van het netwerkverkeer met zoals firewalls / IPS / ACL worden geïmplementeerd. Mechanismen voor het detecteren van veiligheidsrelevante events in netwerkverkeer (zoals firewall / IPS, logging op netwerkapparaten en sensoren / IDS) moeten op basis van risico's worden geïmplementeerd en kunnen bijvoorbeeld door een SIEM worden geanalyseerd en geëvalueerd.

Voor zoneovergangen moet een whitelisting-aanpak worden gebruikt. Al het verkeer wordt standaard geblokkeerd en alleen gedefinieerd verkeer wordt toegestaan (standaard weigeren, toestaan bij uitzondering). Netwerkverbindingen tussen systemen in de verschillende netwerkzones (vooral met verschillende beveiligingsvereisten) moeten tot het noodzakelijke minimum worden beperkt en, indien nodig, moeten afzonderlijke overdrachtsinterfaces in afzonderlijke zones (zoals DMZ) worden geïmplementeerd.

Er moet een architectuur op basis van het defence-in-depth principe worden gepland en geïmplementeerd voor netwerksegmentatie. Hiervoor moeten zones voor externe of onbetrouwbare netwerken (zoals internet en WLAN's voor bezoekers), zones voor DMZ-systemen (zoals proxysystemen en jumpservers voor externe toegang) en zones voor interne systemen (zoals servers, clients, printers, enz.) ter beschikking worden gesteld. Er moeten aparte zones zijn voor systemen die moeten worden geïsoleerd (zoals systemen zonder beveiligingsupdates / onderhoud). Industriële netwerken, iSCSI/storage-netwerken en IT-netwerken moeten altijd fysiek van elkaar gescheiden zijn.

Al het netwerkwerkverkeer met derden-netwerken (zoals internet voor het downloaden van updates, externe toegang van externe serviceproviders) moet in een DMZ-zone worden beëindigd door proxies, jumpservers, VDI-omgevingen, enz. en het netwerkverkeer moet worden gecontroleerd. Directe communicatie van derden-netwerken naar interne netwerkzones is niet toegestaan.

Afhankelijk van de behoefte aan bescherming en kriticaliteit moeten voor de afzonderlijke zones de nodige beschermings-/hardingsmaatregelen worden gedefinieerd en geïmplementeerd.

Afgezien van actieve netwerkapparaten moet elk systeem zich logischerwijs in slechts één zone bevinden. In principe moet het routeren van netwerkverkeer naar hosts / VM's tussen netwerkadapters of het plaatsen van systemen in meerdere netwerken (multihoming) worden vermeden en dit mag alleen, nadat een risicoanalyse is uitgevoerd, plaatsvinden in goedgekeurde en gedocumenteerde situaties en met de nodige beschermende maatregelen en zoneovergangen om te voorkomen dat er ongecontroleerde overgangen tussen zones ontstaan. Bovendien moet split-tunneling worden voorkomen, voor externe apparaten die verbinding maken met bedrijfssystemen. Met split-tunneling kan een persoon of apparaat op afstand een verbinding tot stand brengen met een beveiligd netwerk en tegelijkertijd via een andere verbinding communiceren met een bron in een extern/onveilig netwerk. Uitzonderingen waarin split-tunneling bedoeld is, zoals voor videoconference oplossingen die zonder tunnel toegang mogen krijgen tot centrale cloudsystemen, moeten worden gedefinieerd.

Voor beheersystemen moeten speciale netwerken worden opgezet die alleen voor beheeractiviteiten mogen worden gebruikt. Beheertoegang tot out-of-band netwerken op beheerinterfaces van servers, netwerkapparaten of KVM-systemen mag alleen mogelijk zijn vanaf netwerken voor beheersystemen.
In combinatie met het Zero-Trust principe wordt steeds vaker gebruik gemaakt van zogenaamde microsegmentatie. Hier wordt het aanvalsoppervlak verkleind door het netwerk op te delen in segmenten die nodig zijn om een applicatie uit te voeren (zoals virtuele machines, containers, services).

Voor de uitvoering van de maatregel worden de volgende normen aanbevolen:

- **BSI IT-Grundschutz Kompendium**
  De BSI IT-Grundschutz Kompendium beschrijft in de module NET.1.1 "Network Architecture and Design" de eisen voor de specificatie, planning, implementatie en het testen van netwerksegmentaties en voor het beveiligen van de netwerkcommunicatieverbindingen die via de zones plaatsvinden.
- **ISO/IEC 27002:2022**
  De ISO/IEC 27002 norm bevat aanbevelingen voor de implementatie van maatregelen op het gebied van netwerkbeveiliging (Control 8.20), beveiliging van netwerkdiensten (Control 8.21) en het scheiden van netwerken (Control 8.22).
- **IEC 62443-3-3**
  De norm IEC 62443-3-3 bevat specificaties voor netwerksegmentatie en voor de besturing van netwerkzoneovergangen in industriële communicatienetwerken in FR 5 "Restricted Data Flow".

Periodiek en op ad-hocbasis moeten audits worden uitgevoerd om na te gaan of de bestaande netwerken en netwerksegmenten voldoen aan de gedefinieerde specificaties en voorschriften en ook aan de huidige documentatie.

De gedocumenteerde richtlijnen, procedures en controlemaatregelen voor netwerkscheiding die essentieel zijn voor de bedrijfsvoering, moeten periodiek worden herzien op volledigheid, effectiviteit, geschiktheid en ook op gewijzigde randvoorwaarden en, indien nodig, worden bijgewerkt.

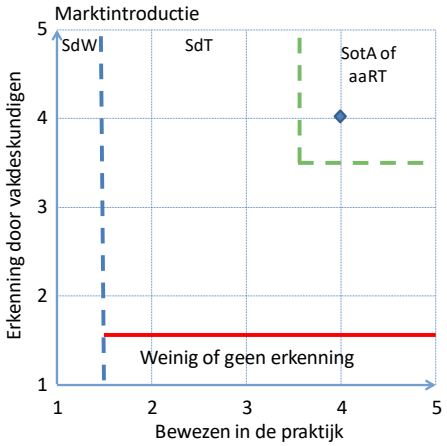
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.2.31 Cloud security platform

Een cloud security platform is een technische maatregel die de risico's en bedreigingen bij het creëren en exploiteren van infrastructuur en applicaties bij cloud service providers afdekt. Het wordt vaak het Cloud Native Application Protection Platform (CNAPP) genoemd en omvat afzonderlijke gebieden, zoals Container-Scanning, Cloud Workload Protection (CWP / CWPP), Cloud Security Posture & Compliance en actieve workloadbeveiliging, waardoor een holistische kijk op cloudbeveiliging mogelijk is. Cloudbeveiligingplatforms kunnen de operationele overhead verminderen en snellere en nauwkeurigere detectie, respons en herstel van beveiligingsincidenten mogelijk maken door anders geïsoleerde beveiligingsinformatie automatisch te koppelen.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

- Misconfiguraties in cloud-infrastructuurcomponenten en hun configuratie worden voortdurend bewaakt. Instellingen en eigenschappen die niet voldoen aan de aanbevelingen van erkende best-practices op het gebied van beveiliging, zoals CIS-benchmarks en nalevingkaders zoals ISO27001, SOC2, enz., evenals de eigen gedefinieerde vereisten, worden geëvalueerd en de verantwoordelijken worden dienovereenkomstig gewaarschuwd. Dit omvat ook de analyse van Infrastructure as Code (IaC). Infrastructure as Code kan bijvoorbeeld Terraform HCL, Cloud Formation, CDK, Docker Files, Kubernetes Manifests zijn
- Kwetsbaarheden (Vulnerability management): kwetsbaarheden in applicaties in alle fasen van de Development Lifecycle, van ontwikkeling, in Testing / Staging tot en met productie met prioritering door actieve pakketten en images door met behulp van runtime-monitoring te detecteren
- Kwaadwillige inbraken door onbevoegde derden in accounts van cloudproviders en aanvallen, gedetecteerd door User & Entity Behavior Analytics (UEBA). Dit wordt gedaan door middel van continue analyse van Cloud Audit Logs, Kubernetes Activity Logs voor bekende en voorheen onbekende aanvalsactiviteiten, zonder enige concrete voorkennis van de aanvalsvector (kwetsbaarheid, patroon, IoC)
- Misconfiguratie en bewaking van beveiligingseigenschappen van serverloze functies, containers, containerorkestratie en virtuele machines die, voor en tijdens uitvoering worden afgehandeld (CWPP)
- Onnodig hoge rechten (CIEM) door het weergeven en oplossen van complexe autorisatieketens van accounts en resources.

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Een cloudbeveiligingplatform bestrijkt de volledige levenscyclus van cloudapplicaties, van applicatieontwikkeling tot provisioning en productieruntime. Dit maakt het mogelijk om kwetsbaarheden en misconfiguraties te ontdekken voordat deze operationeel zijn en om hulp te bieden aan ontwikkelaars en DevOps-teams om onnodige en onaanvaardbare risico's te voorkomen. Tegelijkertijd wordt de naleving van de voor de gebruiker relevante compliance-kaders gecontroleerd. De controle kan worden uitgevoerd door scanners te integreren in de softwarepijplijnen en ook kunnen bijbehorende beleidshandhavingmaatregelen (zoals Kubernetes Admission Controller) op uitvoeringsniveau geïmplementeerd worden.

In productie zorgen sensoren op de compute instances (VM) en Kubernetes worker-nodes voor een continue monitoring van de beveiligingsgerelateerde workload en de netwerkverbindingen om aanvalspogingen en kwaadaardige activiteiten in een vroeg stadium te detecteren. Op machine learning gebaseerde methoden kunnen de beveiligingsteams ontlasten door de noodzaak om sets regels te creëren en voortdurend aan te passen grotendeels te elimineren en aanvallen kunnen, zelfs zonder specifieke voorkennis (gedrag / bestandhashes / IP-adressen, enz.), worden gedetecteerd. Deze incidenten worden contextueel verrijkt. Dit zorgt voor een betere classificatie, evaluatie en prioritering. Sensoren, in de vorm van agents op de respectievelijke hostsystemen in het eigen datacenter van de organisatie, ondersteunen hybride architecturen en cloudmigratieprojecten. Agentloze maatregelen zorgen voor volledige bescherming in omgevingen waar een agent niet kan worden ingezet. Vereisten zoals Host Intrusion Detection, File Integrity Monitoring, Malware Scanning en de detectie van geheimen (zoals SSH-sleutels) en de detectie van mogelijke aanvalspaden zijn belangrijke basisfuncties en zijn zelf belangrijke maatregelen om aan de compliance-eisen te voldoen.

Een cloudbeveiligingsplatform dat onafhankelijk is van de provider van de cloudinfrastructuur maakt het mogelijk om multi-cloudarchitecturen te beveiligen. Tegelijkertijd voorkomt de onafhankelijkheid van cloudprovider-specifieke tools een vendor-lock-in, d.w.z. technologische afhankelijkheid van een specifieke cloudserviceprovider. De naadloze integratie in bestaande workflows en tools (zoals ticketing, alerting, enz.) maakt interdisciplinaire samenwerking tussen teams en projecten mogelijk.

Samenvattend zijn de aanbevolen acties van een cloud security platform ten minste:

- Testen van Infrastructure-as-Code voordat de resources worden ingericht (compliance, misconfiguraties (IaC / Code Security)
- Nalevingcontrole en detectie van misconfiguraties in Cloud (CSPM) en Kubernetes (KSPM) resources aan de hand van relevante compliance- en aanbevolen best-practices frameworks
- Geprioriteerde kwetsbaarheidanalyse van ontwikkeling tot runtime (vulnerability management)

- Visualisatie van mogelijke aanvalspaden, chaining van kwetsbaarheden, autorisatiesleutels en misconfiguraties (CASM)
- Inventarisatie van componenten van de cloudinfrastructuur
- Autorisatie check (CIEM)
- Gedragsanalyse en vroege detectie van kwaadaardige activiteiten binnen Cloud Accounts (UEBA)
- Onmiddellijke detectie van kwaadaardige activiteiten via sensoren binnen actieve workloads, waaronder malwaredetectie en File Integrity Monitoring (CWPP)

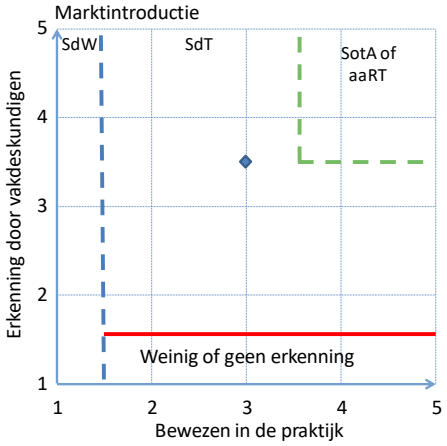
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.2.32 Tokenisatie

Tokenisatie is een methode van gegevenspseudonimisering die kan worden gebruikt als alternatief voor codering. Hier wordt een willekeurig gegenereerde vervangingswaarde toegewezen aan een oorspronkelijke waarde en worden beide waarden, om de oorspronkelijke waarde indien nodig te herstellen, (versleuteld) als een link opgeslagen in een toewijzingstabel.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

- Inbreuk op de vertrouwelijkheid van (zeer) gevoelige gegevens, zoals klantgegevens, werknemersgegevens en gegevens uit productie en ontwikkeling (bijvoorbeeld tegen beheerders en softwareontwikkelaars die geen toegang mogen hebben tot productieve gegevens)
- Volgens de General Data Protection Regulation (GDPR) van de EU minimaliseert pseudonimisering het risico dat persoonsgegevens in verkeerde handen vallen. Dit geldt in het bijzonder voor ongeoorloofde toegang en gebruik. Tokenisatie als een specifieke pseudonimiseringsmethode beschermt zeer gevoelige gegevens in cloudgebaseerde omgevingen en tijdens verzending.

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Tokenisatie beschrijft een proces voor gegevenspseudonimisering dat wordt gekenmerkt door de mogelijkheid om het formaat van de doelwaarden te behouden. Het is daarom bijzonder geschikt voor

het genereren van testgegevens en het beschermen van gegevens in cloudgebaseerde toepassingen (zie ook hoofdstuk 3.2.11, Cloudgebaseerde gegevensuitwisseling).

In de meeste gevallen is tokenisatie complementair aan versleuteling, omdat het niet superieur is aan versleuteling op zich, maar toch enkele voordelen biedt:

1. Behoud van formaat: De gegenereerde vervangingswaarde moet overeenkomen met een vooraf gedefinieerd formaat, zodat veldvalidatie, bijvoorbeeld voor e-mailadressen en bankgegevens, nog steeds succesvol zijn.
2. Statistische verdeling: De statistische verdeling van de gegenereerde vervangende waarden komt overeen met die van de oorspronkelijke waarden, wat bijvoorbeeld voordelig kan zijn bij statistische onderzoeken (denk aan postcodes, bloedwaarden, etc.). Een tokenisatietool moet echter de mogelijkheid bieden om dit gedrag te configureren voor maximale flexibiliteit.
3. Wiskundige onafhankelijkheid: Omdat, in tegenstelling tot op algoritmen gebaseerde codering, geen enkele wiskundige berekening de oorspronkelijke waarde en de vervangende waarde met elkaar verbindt, maar alleen de toewijzingstabel kennis heeft van deze relatie, kan, zolang de tokendatabase vertrouwelijk blijft, tokenisatie moeilijker gepasseerd worden. Volgens de aanbeveling van het Europees Comité voor gegevensbescherming moeten, om ervoor te zorgen dat de toewijzing van tokens aan originele gegevens alleen mogelijk is door geautoriseerde partijen, technische en organisatorische maatregelen worden geïmplementeerd. Daarom is het daarnaast aan te raden om een HSM te gebruiken om de originele waarden in de toewijzingstabel te versleutelen.

Tokenization biedt echter ook nadelen ten opzichte van data-encryptie:

1. Om de prestaties tijdens de verwerking te behouden, is de juiste rekenkracht vereist. Daarom is voor grote hoeveelheden data encryptie op basis van algoritmes vaak de betere keuze.
2. Er moet een zogenaamde Token Vault worden aangemaakt waarin de originele waarden veilig worden opgeslagen en versleuteld naast de vervangende waarden. Dit kan resulteren in grotere hoeveelheden gegevens, waarvoor de juiste opslagcapaciteit nodig is.
3. De tokenruimte is eindig: Hoe strenger de eisen voor het formaat van de vervangende waarden, hoe kleiner de mogelijke hoeveelheid vervangende waarden die moeten worden gegenereerd.
4. Een ander aspect is dat gepseudonimiseerde gegevens nog steeds als persoonlijk worden beschouwd als het mogelijk is om de vervangingswaarden genereren. Daarom moet deze informatie speciaal worden beschermd en gescheiden worden gehouden.

Ondanks al zijn voordelen is tokenization geen doel op zich: de focus ligt op de bescherming van gegevens, daarom moeten softwareoplossingen voor tokenization de volgende gemakskenmerken hebben:

1. Onafhankelijke oplossing: er zijn geen wijzigingen nodig in de doelapplicaties waar de tokenized gegevens zich bevinden.
2. Mogelijkheid om, naast de basisfunctionaliteit die tokens biedt via moderne interfaces, individuele waarden te tokeniseren in bestanden, databases en in webapplicaties.
3. Beschikbaarheid van complexe tokenprofielen zoals het Luhn-algoritme voor het correct genereren van creditcardnummers en de mogelijkheid om uitspreekbare strings als vervangende waarde te genereren.

Mogelijkheid om selectief te tokeniseren, zodat, afhankelijk van de gevoeligheid van de gegevens en het beveiligingsniveau dat in elk geval vereist is, velden kunnen worden beschermd en in platte tekst kunnen worden bewaard.

Tokenization voldoet aan de eisen van gegevensbescherming door technisch ontwerp volgens GDPR Art. 25 als het wordt gecombineerd met passende technische maatregelen, bijvoorbeeld door het gebruik van cryptografische methoden of de implementatie van een hardwarebeveiligingsmodule (HSM). De effectiviteit hangt af van de scheiding van de pseudonimiseringscomponent van de gegevensverwerking.

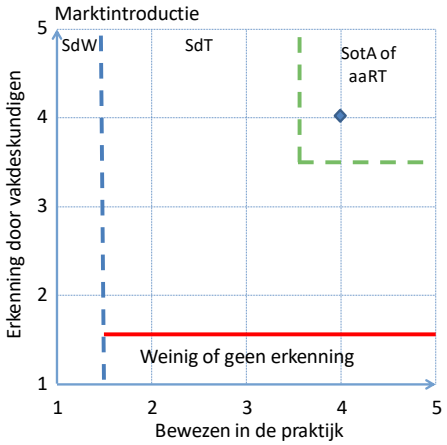
Welke beschermingsdoelen worden door de maatregel afgedekt?

☐ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.2.33 VOIP-versleuteling met SIPS/SRTP

De telecommunicatie van vandaag is gebaseerd op IP-gebaseerde netwerken. Het Session Initiation Protocol (SIP) wordt gebruikt om de verbindingen (zoals het tot stand brengen en verbreken van de verbinding, doorschakelen en wijzigingen in verbindingsparameters), de signalering te regelen. Het Real-time Transport Protocol (RTP) wordt gebruikt voor het uitwisselen van de gedigitaliseerde stem. Beide werken normaal gesproken onversleuteld en zijn daarom in eerste instantie kwetsbaar voor de dreiging van inzage, afluisteren, manipulatie en verstoring van de beschikbaarheid door onbevoegde derden. Daarnaast kunnen ook communicatiepatronen worden afgeleid.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

- Afluisteren en soms opname van telefoongesprekken (zelfs een kleine hoeveelheid spraakgegevens kan worden gebruikt om met AI stemmen te klonen)
- Het simuleren van valse identiteiten en het ongeoorloofd doorsturen van gesprekken door middel van manipulatie (spoofing van nummerherkenning)
- Injectie van ongeoorloofde spraakgegevens of van stilte
- Met ruis bedekte spraakgegevens kunnen worden bediend door spraakgestuurde apparaten
- Het tot stand brengen van ongeoorloofde verbindingen
- Denial-of-Service aanvallen

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Om de signalering te versleutelen, kan transportversleuteling op basis van SIP over TCP en TLS in combinatie met het SIPS URI-schema worden gebruikt. Het Secure Real-time Transport Protocol (SRTP) wordt gebruikt voor versleutelde spraakoverdracht.

SRTP maakt de versleutelde overdracht mogelijk van spraakgegevens met alle gevoelige en persoonlijke inhoud die deze bevat. Het protocol biedt integriteit, vertrouwelijkheid en bescherming tegen replay-aanvallen. Het maakt gebruik van symmetrische codering op basis van de Advanced Encryption Standard in Counter Mode (AES-CM). Afhankelijk van de sleutelwissel procedure kunnen sleutellengtes tot 256 bits worden gebruikt. Er moet echter worden opgemerkt dat alleen de gebruikersgegevens worden versleuteld. De header is alleen geverifieerd. HMAC-SHA1 met 80 bits dient als hashing-methode om de integriteit te waarborgen.

Het gebruik van Security Descriptions for Media Streams (SDES) voor sleuteluitwisseling heeft alleen zin in combinatie met TLS-gecodeerde SIP-signalering, omdat in dit geval de sleuteluitwisseling voor SRTP in platte tekst binnen de signalering plaatsvindt en anders zou latere decodering mogelijk zijn.

Datagram Transport Layer Security (DTLS) is de op UDP gebaseerde tegenhanger van TLS. Het is dus een transportversleuteling die voortbouwt op X.509-certificaten om de sleutels en algoritmen voor SRTP uit te wisselen. De overdracht van de gebruikersgegevens vindt echter niet plaats via DTLS, maar via SRTP. De symmetrische SRTP-sleutels worden rechtstreeks via het mediapad uitgewisseld en niet binnen de signalering. De eindpunten verzenden als authenticatie een vingerafdruk van de certificaten in SIP-signalering. Alleen de media-eindpunten hebben toegang tot de sleutels.

De versleuteling van signalering via SIP-TLS werkt in principe " hop by hop ". Dit betekent dat de versleuteling in eerste instantie slechts tot de volgende SIP-proxy wordt gegarandeerd. Deze volgende SIP-proxy kan de gegevens ontcijferen en op basis van de signalering in platte tekst doorsturen. SIP-TLS op basis van het SIPS URI-schema gaat nog iets verder. Versleuteling tot aan het doeldomein wordt gebruikt en moet daarom bij voorkeur worden gebruikt.

Authenticatie kan in principe zowel puur server gebaseerd (via SIP-proxy of SBC) als onderling tussen client en server (wederzijds TLS) worden uitgevoerd. Wederzijdse authenticatie verdient de voorkeur.

Voor SIP-TLS mag alleen versie TLS 1.3 worden gebruikt. De bijbehorende algoritmen en hashing-methoden moeten conform BSI-aanbeveling TR-02102[18] worden geselecteerd. DTLS in combinatie met SRTP mag ook alleen DTLS 1.3 gebruiken. Vanwege het feit dat persoonsgegevens worden doorgegeven, moet geheimhouding worden gebruikt om latere decodering te voorkomen.

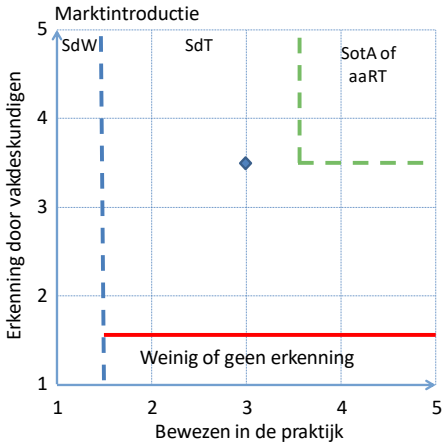
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.2.34 Versleuteling (Layer 1)

De onderste netwerklaag van het OSI-model wordt gebruikt voor de fysieke overdracht van berichten via een medium tussen twee punten. Versleuteling is bedoeld om ervoor te zorgen dat de verzonden informatie niet kan worden onderschept door onbevoegden. Alle verbindingen en protocollen van de bovenstaande netwerklagen zijn beveiligd door gemeenschappelijke encryptie op Layer 1. Layer 1-bescherming is met name handig voor transmissiemedia met gemakkelijke toegang of grote

[18] Technische Richtlijn TR-02102-2: Gebruik van Transport Layer Security (TLS)

hoeveelheden gegevens die worden getransporteerd. In de "VS Product Catalog" van het BSI" is een aparte productklasse aangewezen voor producten met encryptie op Layer 1[19].

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

Fysieke toegang tot een transmissiemedium stelt een aanvaller in staat om de verzonden informatie af te luisteren. Er is een groot risico, met name bij media die gemakkelijk toegankelijk zijn, zoals koperen kabels, hoogspanningskabels met Powerline of Radio. Ook optische vezels, die worden gebruikt om grote hoeveelheden gegevens over lange afstanden te transporteren, zijn een aantrekkelijk doelwit voor afluisteren. Glasvezelkabels worden aangelegd in routes, waarvan sommige zeer gemakkelijk toegankelijk zijn.

De versleuteling van de payload op de laagste netwerklaag zorgt voor de vertrouwelijkheid van de verzonden informatie. In combinatie met hash-functies en digitale handtekeningen kan ook de integriteit van de gegevens worden gewaarborgd.

Layer 1-encryptie beschermt alle gegevens van de hogere netwerklagen inclusief metadata, zoals IP- en MAC-adressen. Als gevolg hiervan is het voor een aanvaller niet mogelijk om informatie te verkrijgen over communicatierelaties of gedragspatronen van de gebruikers van het netwerk. In de high-security sector wordt Layer 1-encryptie ingezet om verkeersverbindingen te verbergen.

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Layer 1-encryptie zorgt voor de bescherming van alle informatie die tussen de eindpunten van de fysieke verbinding wordt verzonden. De twee eindpunten moeten zich op betrouwbare wijze authenticeren en het eens worden over een gemeenschappelijke, geheime sleutel of op een beschermde manier een sleutel uitwisselen tussen de eindpunten. De sleutel wordt vervolgens gebruikt om de gebruikersgegevens met behulp van een symmetrisch algoritme te versleutelen of te ontsleutelen. Het wordt aanbevolen om de geheime sleutel met regelmatige tussenpozen te vernieuwen om de mogelijkheid van decodering van gegevens die in het verleden en in de toekomst zijn verzonden, te voorkomen.
Een verbinding op de onderste Layer van het Layer-model kan geaggregeerd verkeer transporteren van veel verbindingen op hogere layers. De hogere bit-rate van geaggregeerd verkeer zorgt voor een snellere verwerking van de codering, wat in vergelijking met encryptie van individuele verbindingen op hogere netwerklagen, resulteert in geringere vertraging in encryptie op Layer 1. De lage latency van Layer 1-encryptie is vooral belangrijk voor tijdkritische toepassingen, zoals toepassingen in de financiële sector en voor de overdracht van zeer nauwkeurige tijdinformatie.

In de praktijk worden Layer 1-transmissiesystemen vaak voor langere tijd gebruikt dan IT-toepassingen op de hogere netwerklagen en die aan aanzienlijk kortere innovatiecycli onderhevig zijn. Ze moeten ontworpen zijn voor een lange levensduur en dus ook voorbereid zijn op de potentiële dreiging van toekomstige quantumcomputers. Het wordt tegenwoordig aanbevolen om te vertrouwen op kwantumveilige methoden voor sleuteluitwisseling. Hiervoor zijn verschillende opties beschikbaar waaronder post-kwantumcryptografie, QKD-technologie en hybride methoden die gevestigde methoden en kwantumveilige methoden combineren. Bij gebruik van het AES-algoritme met een sleutellengte van ten minste 256 bits is de versleuteling van de payload kwantumveilig[20].

Een belangrijk toepassingsgebied voor Layer 1-encryptie zijn glasvezelnetwerken die grote hoeveelheden gegevens over lange afstanden verzenden. Door de uitgebreide infrastructuur kan de toegang tot het transmissiemedium niet op betrouwbare wijze verhinderd worden. Door koppelingselementen die tijdens de installatie of het gebruik als glasvezel- of buigkoppelingen worden ingebracht, wordt toegang tot de optische signalen in de glasvezel mogelijk gemaakt. Hierdoor kan de verzonden informatie worden gelezen en kunnen storende en vervalste optische signalen worden ingevoerd.

Voor praktische oplossingen voor Layer 1 encryptie van optische links vormen de OTN-specificaties de basis. Hierdoor kunnen gestandaardiseerde interfacemodules worden gebruikt. Het gebruik van optische versterkers maakt een bereik van meer dan 1.000 km mogelijk. De sleuteluitwisseling vindt plaats via een hulpkanaal, waardoor een vermindering van de doorvoer in het nuttige kanaal wordt

[19] VS productcatalogus van de BSI, versie 1.8 van 18.04.2024; Bundesamt für Sicherheit in der Informationstechnik
[20] Cryptografie kwantumveilig maken: basisprincipes, ontwikkelingen, aanbevelingen; Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Bro21/01

voorkomen. Geaggregeerd verkeer op Layer 1 wordt versleuteld zonder overhead, waardoor 100 procent doorvoer wordt gegarandeerd.

De hoge bandbreedte van OTN-signalen zorgt voor een snelle frequentie van de encryptor, wat resulteert in een zeer lage latentie.

Versleuteling op netwerk Layer 1 maakt de veilige overdracht van een breed scala aan protocollen en interfaces in de payload mogelijk. OTN-technologie biedt de mogelijkheid om veilig een verscheidenheid aan protocollen en interfaces in de payload te verzenden, waaronder OTN, SDH, IP/Ethernet. Het maakt het ook mogelijk om speciale protocollen tussen datacenters of videostudio's te transporteren.

Het Bundesamt für Sicherheit in der Informationstechnik (BSI) heeft voor het transport van geclassificeerde informatie goedgekeurde overdrachtssystemen met Layer 1-encryptie.

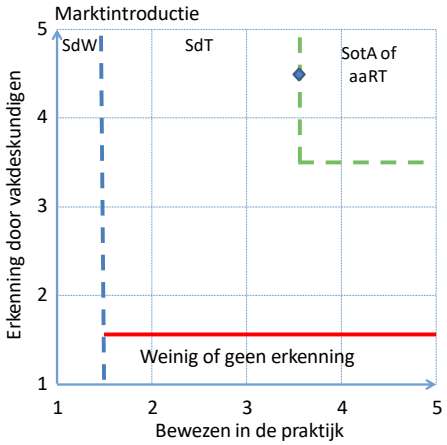
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.3 Organisatorische maatregelen

Aangezien informatie- en communicatiefaciliteiten niet altijd fundamenteel zijn ontworpen voor beveiliging en technische beveiliging alleen effectief is als deze op de juiste manier wordt geflankeerd door organisatorische en personele maatregelen, heeft elke organisatie een systeem van procedures, procedures en regels nodig voor het beheren van operationele informatiebeveiliging, d.w.z. een Information Security management System (ISMS).

Een ISMS stelt regels vast en implementeert deze voor de classificatie en verwerking van informatie die bescherming verdient. Het ISMS is een belangrijk onderdeel van het algemene interne veiligheidsbeheer van de organisatie en loopt door alle belangrijke onderdelen van de organisatie. Het ISMS bevat procedures voor het regelmatig evalueren en documenteren van organisatorische en technische veranderingen.

Een belangrijk aandachtspunt van het ISMS is het in aanmerking nemen van informatiebeveiligingeisen bij geplande wijzigingen en het onderhoud van de belangrijke elementen van de IT-infrastructuur. Een ander aspect is de regelmatige opleiding en sensibilisering van medewerkers. Bovendien specificeert het beheersysteem voor informatiebeveiliging hoe de voorbereiding op noodsituaties moet worden uitgevoerd en hoe moet worden gereageerd op eventuele beveiligingsincidenten. Het doel van het ISMS is om permanent te voldoen aan en een efficiënt en altijd passend veiligheidsniveau te garanderen.

TeleTrusT heeft in haar document "Information - Praxisleitfaden für Manager " een bruikbare gids voor informatiebeveiligingbeheer gegeven. Het document laat zien dat informatiebeveiligingbeheer en de bijbehorende compliance- en risicocultuur een strategisch controle-instrument kunnen zijn dat de beveiligingssituatie in één oogopslag illustreert.

3.3.1 Normen en standaarden

Er zijn een aantal internationale normen en standaarden met betrekking tot informatiebeveiliging. Ze kunnen als basis dienen om de beveiligingsstrategie van de organisatie op elkaar af te stemmen en de invoering van een ISMS te ondersteunen. Net als bij technische maatregelen is het continu veranderen van organisatorische maatregelen een taak van lange adem, zodat het verwijzen naar normen en standaarden ook mogelijk is in verband met de State-of-the-art. De ISO/IEC 27000-serie wordt gebruikt als referentiepunt voor andere normen en standaarden. In sommige gevallen zijn er overlappingen, maar deze kunnen meestal als synergie worden gebruikt, zodat er een positieve invloed is op het gebied van informatiebeveiliging.

De wereld van de ISO/IEC 27000-normen

De ISO/IEC 27000-serie (soms kortweg ISO27k genoemd) is een reeks normen voor informatiebeveiliging. Deze normen worden uitgegeven door de International Organization for Standardization (ISO) en de International Electrotechnical Commission (IEC).

ISO/IEC 27001 is de bekendste norm in de ISO/IEC 27000-serie en formuleert de eisen waaraan een ISMS moet voldoen. Daarnaast zijn er andere normen en richtlijnen voor de concrete uitvoering.

De ISO/IEC 27000-serie bevat onder andere de volgende essentiële inhoud, die elk als een onafhankelijke norm worden beheerd en worden samengevat als een reeks normen.

ISO/IEC Norm	Tevreden
ISO/IEC 27000	ISO/IEC 27000-serie normen overzichtsdocument en terminologie
ISO/IEC 27001	Vereisten voor een ISMS
ISO/IEC 27002	Gids voor het bepalen en implementeren van de vereisten van ISO/IEC 27001
ISO/IEC 27003	Gids voor de algemene vereisten van een ISMS volgens ISO/IEC 27001
ISO/IEC 27004	Gids voor het monitoren en meten van de effectiviteit van het ISMS
ISO/IEC 27005	Gids voor risicobeheer
ISO/IEC TR 27019	Sectorspecifieke gids als uitbreiding op de maatregelen van een ISMS voor procesbesturingssystemen in de energievoorzieningsindustrie
ISO/IEC 27031	Gids voor gereedheid voor informatie- en communicatietechnologie voor bedrijfscontinuïteit
ISO/IEC 27034	Handleiding voor applicatiebeveiliging
ISO/IEC 27035	Gids voor het beheer van informatiebeveiligingsincidenten

Tabel 1: Overzicht ISO/IEC 27000-serie

Andere normen en standaarden

Informatiebeveiligingsnormen en -criteria kunnen worden op basis van hun aandachtsniveau geclassificeerd als bedrijfs-, systeem- en productnormen. Volgens hun formulering kunnen deze worden onderverdeeld in technische, minder technische en niet-technische normen.
Op basis van een eerdere presentatie van het D21-initiatief zouden de bovengenoemde structuurniveaus als volgt kunnen worden gepresenteerd:

	technisch	minder technisch	niet technisch
Bedrijfsstandaard		BSI-Standard 200/ BSI IT-Grundschutz	ISO/IEC 9000 ISO/IEC 20000 ISO/IEC 27000 ISO/IEC 22301 COBIT ISF SOGP
Systemstandaard		ULD Datenschutz-Gütesiegel, Euro-PriSe-Privacy Seal, TÜViT Trusted Process / Site / Product	
Productstandaard	ITSEC ISO/IEC 15408 (CC) ISO/IEC 19790 (FIPS 140) BSI C5		

Afbeelding 5: Structuurniveaus van normen en standaarden op het gebied van informatiebeveiliging

Als norm voor bedrijven en openbare instellingen (organisaties) die in een niet-technische taal is geformuleerd, is er een bijzondere behoefte om ISO/IEC 27001 te onderscheiden van ISO/IEC 9001, ISO/IEC 20000-1, ISO/IEC 22301, CoBIT en ISF SOGP.

ISO/IEC 27000 e.v.
De ISO/IEC 27000ff normenreeks omvat verschillende normen op het gebied van ISMS. De kern van deze reeks normen is ISO/IEC 27001, die in de context van een organisatie de eisen beschrijft voor een Information Security Management System (zie 3.3.1.1).

ISO/IEC 27001 gebaseerd op IT-Grundschutz

Dit omvat de implementatie van ISO/IEC 27001 met behulp van de IT-basisbeschermingsmethodologie van het Duitse federale bureau voor informatiebeveiliging (gedocumenteerd in BSI-standard 200-2) en het IT-Grundschutz Kompendium.

De BSI-norm 200-1 definieert algemene vereisten voor een ISMS en is over het algemeen compatibel met de ISO/IEC 27001 en houdt ook rekening met de aanbevelingen van de andere normen van de ISO/IEC 27000-normenreeks, zoals ISO/IEC 27002. Het biedt geïnteresseerde partijen een gemakkelijk te begrijpen en systematische introductie en begeleiding, ongeacht de methode die ze willen gebruiken om de vereisten te implementeren.

BSI-norm 200-2 biedt, met de procedure volgens IT-Grundschutz, het volgende:

- Concrete en methodologische hulp voor de geleidelijke invoering van een beheersysteem voor informatiebeveiliging
- Rekening houden met de afzonderlijke fasen van het informatiebeveiligingsproces
- Oplossingen uit de praktijk, "best practice" benaderingen
- Mogelijkheid tot certificering

Het onderscheid tussen de "native" ISO/IEC 27001-implementatie en de basisbeschermingbenadering van de BSI is te vinden in de onderstaande tabel:

Categorie	**ISO27001**	**BSI IT-Grundschutz**
Toepassingsgebied van de regelgeving	Relevante normen < 100 pagina's	Kompendium voor basisbescherming > 4.000 pagina's
Eisen	Abstracte en generieke randvoorwaarden	Concrete handvatten voor praktische maatregelen
Risicoanalyse	Volledige analyse van elk doelobject	Vereenvoudigde analyse in geval van verhoogde beschermingseisen

Maatregelen	ca. 100 conceptuele vereisten	> 1.100, concrete acties
Certificering	Certificering	Auditor attesten + Certificering
Geldigheid	3 jaar jaarlijkse toezichtsaudits	3 jaar jaarlijkse toezichtsaudits

Tabel 2: Differentiatie ISO/IEC 27001 vs. BSI Grundschutz

ISO/IEC 20000-1

Deze norm specificeert eisen voor interne en externe organisaties met betrekking tot het leveren van procesgerichte diensten. Sommige van de gevraagde processen (in het bijzonder Information Security Management, Incident & Event Management en Service Continuity Management) overlappen met ISO/IEC 27001. Traditioneel wordt ISO/IEC 20000-1 toegepast op IT-providers, terwijl de reikwijdte van ISO/IEC 27001 alle soorten organisaties kan bestrijken.

ISO/IEC 22301

Deze norm is gericht op het waarborgen van business continuity management (BCM) en specificeert eisen voor BCM-systemen in organisaties. Volgens ISO/IEC 22301 hebben BCM-systemen ook (maar niet alleen) een IT-referentie. Het onderwerp BCM wordt ook behandeld in een onderwerpgebied van ISO/IEC 27001, maar alleen vanuit het perspectief van informatiebeveiliging (d.w.z. de mate waarin de bedrijfscontinuïteit in gevaar kan komen door informatiebeveiligingsincidenten).

BSI 200-4

De BSI-norm 200-4 biedt een methodologie voor de introductie van een BCM-systeem die de stapsgewijze introductie van een Business Continuity Management System (BCMS) beschrijft met het opzetten van een organisatiestructuur met een volwassenheidsmodel. De fasen: reactief BCMS, geavanceerd BCMS en standaard BCMS worden gedefinieerd en een stapsgewijze aanpak wordt aanbevolen.

ISO/IEC 9001

Deze norm specificeert eisen voor kwaliteit managementsystemen, maar bevat ook veel aspecten van informatiebeveiliging, zoals met betrekking tot de verplichtingen om:

- Zorgen voor de beschikbaarheid van middelen en informatie om de processen uit te voeren en te bewaken
- Identificatie, bewaring, bescherming en opvraging van gegevens
- Identificeren, implementeren en onderhouden van infrastructuur zoals gebouwen, werkterrein en bijbehorende nutsvoorzieningen, procesapparatuur (inclusief hardware en software) en ondersteunende diensten (inclusief communicatie- en informatiesystemen)
- Bescherming van eigendommen van klanten, zoals intellectueel eigendom, persoonsgegevens, enz.

COBIT

COBIT is een methode om risico's te beheersen die voortvloeien uit het gebruik van IT ter ondersteuning van bedrijfsrelevante processen. Het is een "gereedschapskist" voor het management dat gericht is op auditing en controlling en dat resultaat- en prestatiemetingen voor alle IT-processen definieert. COBIT beschrijft verschillende procesgebieden, elk met gedefinieerde controledoelen, volwassenheidsmodel en gemeten variabelen. COBIT verwijst naar alle IT-processen, terwijl ISO/IEC 27001 zich richt op de beheersing van het informatiebeveiligingsproces.

Standard of Good Practice (SOGP)

De standaard voor goede praktijken voor informatie van het Information Security Forum (ISF) is een good-practice benadering voor de beveiliging van bedrijfsinformatie en die ook "security benchmarking" mogelijk maakt. Het SOGP behandelt verschillende onderwerpen van informatiebeveiliging (zoals IT-beveiligingbeheer, bedrijfskritische applicaties, informatieverwerking, communicatie / netwerken, systeemontwikkeling) vanuit een bedrijfsperspectief en biedt een alternatieve, deels complementaire en complementaire visie op ISO/IEC 27001.

3.3.2 Beveiligingsorganisatie

De beveiligingsorganisatie richt zich op het beschermen van mensen, informatie en activa tegen mogelijke bedreigingen. Om een uniform beveiligingsniveau te bereiken en beveiliging als integraal onderdeel van de organisatie te verankeren is een goed gestructureerde en functionerende beveiligingsorganisatie is cruciaal.

De taken van de beveiligingsorganisatie omvatten met name:

- Identificatie en evaluatie van veiligheidsrisico's (risicoanalyse)
- Ontwikkeling en implementatie van risicobeperkende maatregelen (strategie)
- Voortdurende herziening en aanpassing van beveiligingsmaatregelen (monitoring)

De essentiële rollen en verantwoordelijkheden binnen een beveiligingsorganisatie zijn:

Rol in de organisatie[21]	Verantwoordelijkheden
Algemeen Directeur (CEO), Raad van Bestuur (CxO)	• Strategische verantwoordelijkheid (dedicated), maar uiteindelijk ook eindverantwoordelijkheid voor informatiebeveiliging • Verantwoordelijkheid voor alle risicobeslissingen
Hoofd informatiebeveiliging (CISO), IT-beveiligingsfunctionaris	• Tactische en (deels) operationele beheersing van informatiebeveiliging • Ondersteuning van het management bij de uitvoering van haar IS-taken • Personeelseenheid met rechten en plichten om rechtstreeks te rapporteren aan het topmanagement
Functionaris Informatiebeveiliging (ISO)	• Operationele beheersing van informatiebeveiliging, indien nodig tactische taken voor individuele business units • Organisatorisch direct toegewezen aan de CISO
IS Management Team, Stuurgroep Veiligheid	• Permanent orgaan voor het coördineren van de planning en uitvoering van informatiebeveiligingsmaatregelen • Bestaande uit CISO, ISO('s), applicatievertegenwoordigers, bedrijfseigenaren, functionarissen voor gegevensbescherming, vertegenwoordigers van het topmanagement • Advies- en controlefunctie voor de CISO
Functionaris voor gegevensbescherming (FG of DPO)	• Niet per se te worden beschouwd als onderdeel van het IS-management, maar idealiter regelmatig betrokken bij het IS-managementproces als een belangrijke stakeholder op het gebied van compliance
Auditfunctionaris, Auditmanager	• Centraal aanspreekpunt voor interne en externe audits • Coördineert en controleert de planning en uitvoering van audits • Assisteren van de CISO namens hen.

Tabel 3: Rollen en verantwoordelijkheden binnen een beveiligingsorganisatie

[21] De rolaanduidingen kunnen per organisatire verschillen

Ongeacht de verantwoordelijkheden die in de tabel worden vermeld, blijft de algehele verantwoordelijkheid bij het managementniveau (management, bestuur). Dit wordt bevestigd in de huidige wetgeving met een focus op informatiebeveiliging en gegevensbescherming naast de reeds geldende vereisten (zoals de AktG[22]).

Voor de maatregelen moeten minimaal de ISO/IEC 27000 tot ISO/IEC 27005 normen in acht worden genomen. Als andere toepasselijke eisen, normen en resultaten van risicoanalyses dit vereisen, kunnen ook verdere organisatorische maatregelen nodig zijn.

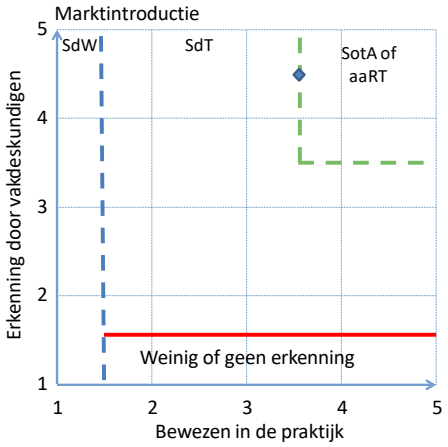
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.3.3 Information Security Management System (ISMS)

Een ISMS is bedoeld om de beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van informatie binnen het toepassingsgebied ervan te waarborgen door binnen een organisatie procedures en regels vast te stellen en daarmee samenhangende beveiligingsmaatregelen te implementeren. Dit betekent dat informatiebeveiliging permanent wordt gepland, beheerd en gecontroleerd om het vereiste beveiligingsniveau te bereiken, te behouden en continu te verbeteren.

[22] https://www.gesetze-im-internet.de/aktg/

Eisen

De basis voor het ISMS is de definitie van de reikwijdte en de context waarin het ISMS moet worden opgezet en geëxploiteerd. Voor de scopebepaling moet rekening worden gehouden met interne en externe vereisten, verwachtingen ten aanzien van de ISMS-doelstelling, betrokken partijen en wet- en regelgeving.

Een ISMS vereist een continu verbeteringsproces (CIP), dat wordt geïmplementeerd in de vorm van de PDCA-cyclus (Plan, Do, Check, Act) om het behoud van de informatiebeveiliging in de organisatie te waarborgen. Voor het realiseren van een effectief ISMS moeten de volgende eisen worden geïmplementeerd.

De steun van het hoogste managementniveau (management, raad van bestuur, enz.) voor de inrichting en verdere ontwikkeling van een ISMS moet worden gewaarborgd, aangezien beslissingen over de doelstellingen, reikwijdte en implementatie van het ISMS moeten worden genomen vanuit het hoogste managementniveau en daarvoor middelen moeten worden vrijgemaakt. De ondersteuning van het hoogste managementniveau voor het ISMS wordt geboden door de goedkeuring (ondertekening) van de Richtlijn Informatiebeveiliging. Deze richtlijn definieert de informatiebeveiligingsdoelstellingen van de organisatie binnen het toepassingsgebied van het ISMS, afgestemd op de bedrijfsdoelen en -strategieën en stelt de toewijding van het hoogste managementniveau vast om het ISMS voortdurend te verbeteren. Dit is essentieel omdat de algehele verantwoordelijkheid voor informatiebeveiliging altijd bij het hoogste managementniveau blijft. De richtlijn moet worden bekendgemaakt aan alle medewerkers in het toepassingsgebied.

Om een ISMS op te zetten en technische en organisatorische beveiligingsmaatregelen te implementeren, moet, op het gebied dat van toepassing is, een passende, overkoepelende organisatiestructuur voor informatiebeveiliging aanwezig zijn. De rollen en verantwoordelijkheden van alle betrokken personen en partijen moeten duidelijk worden gedefinieerd. In een opleidings- en bewustmakingsprogramma moet, afhankelijk van hun taken, rollen en verantwoordelijkheden, voldoende rekening worden gehouden met alle personen in het toepassingsgebied.

Voor de succesvolle werking van het ISMS en ter ondersteuning van het informatiebeveiligingsproces moeten ook interne/externe communicatievereisten en een proces voor het documenteren van het ISMS (gedocumenteerde informatie en records) worden gedefinieerd.

Een van de speerpunten van het ISMS is risicomanagement, om (IT-)risico's voor de organisatie in kaart te brengen, te analyseren en door middel van passende maatregelen zo beheersbaar mogelijk te maken en terug te brengen tot een acceptabel niveau. Daartoe moet het risicobeheer worden aangepast aan de organisatie en worden geïntegreerd in het informatiebeveiligingsproces.

Aanbevelingen/implementatie

De volgende normen worden aanbevolen voor de implementatie van een ISMS:

- ISO/IEC 27001:2022
  Deze norm stelt eisen aan een certificeerbaar ISMS en beschrijft de processen die nodig zijn voor implementatie, controle, controle en continue verbetering. Als certificering van het ISMS wordt aangevraagd, moeten de aanvullende eisen van de in bijlage A vermelde controles worden geïmplementeerd.

- BSI-standaard 200-1
  Deze beschrijft de algemene vereisten voor een ISMS, waarbij de IT-basisbeschermingsmethodologie wordt gecombineerd met de vereisten van ISO/IEC 27001 om ermee compatibel te zijn, waardoor ISO/IEC 27001-certificering op basis van IT-Grundschutz mogelijk is.

- VdS-richtlijnen 10000 (VdS 10000)
  VdS Schadenverhütung GmbH, een dochteronderneming van de Duitse Vereniging van Verzekeraars, biedt, speciaal voor kleine en middelgrote ondernemingen, een praktische, compacte catalogus met maatregelen voor de ontwikkeling van een ISMS. Certificering door de VdS is ook mogelijk. De richtlijnen zijn gebaseerd op de ISO/IEC 27001-normen en de BSI-Grundschutz.

- Information Security Management Systeem in 12 stappen (CISIS12)
  Het "Netz für Informationssicherheit im Mittelstand", met leden als het Beierse IT Security Cluster e.V. en de Universiteit van Regensburg, biedt een wetenschappelijk onderbouwd model voor de praktische invoering van een ISMS in 12 stappen voor kleine en middelgrote instellingen op basis van de ISO/IEC 27001-normen en de BSI-Grundschutz. Certificering is mogelijk.

- Oostenrijks handboek voor informatiebeveiliging
  Het Oostenrijkse handboek voor informatiebeveiliging beschrijft en ondersteunt de procedure voor het opzetten van een uitgebreid ISMS en biedt door de gekozen structuur een implementatiehulpmiddel voor implementatie in overeenstemming met ISO/IEC 27001. De handleiding heeft op belangrijke punten overlap met de BSI IT-Grundschutz.

Kwaliteitsbewaking

Voor de implementatie van de PDCA-cyclus in het kader van het ISMS moeten periodiek (ten minste jaarlijks) audits worden uitgevoerd om na te gaan of technische en organisatorische maatregelen effectief zijn en in overeenstemming met de richtlijn informatiebeveiliging worden geïmplementeerd en toegepast. Daartoe moet een verordening worden opgesteld voor het herzien en verbeteren van het informatiebeveiligingsproces, evenals een regelmatig auditplan van ten minste drie jaar om interne en externe audits uit te voeren. Audits moeten, in overeenstemming met het auditplan, periodiek en op ad-hocbasis worden uitgevoerd en door professioneel gekwalificeerde personen. Redenen voor audits zijn bijvoorbeeld proceswijzigingen, wijzigingen in de scope, wijzigingen in de infrastructuur en het identificeren van nieuwe, kritieke risico's.

Het hoogste managementniveau moet regelmatig worden geïnformeerd over de status van informatiebeveiliging, bijvoorbeeld afgeleid van interne/externe audits en moet het ISMS in de vorm van managementbeoordelingen evalueren om de geschiktheid, geschiktheid, effectiviteit en voortdurende verbetering van het ISMS te waarborgen.

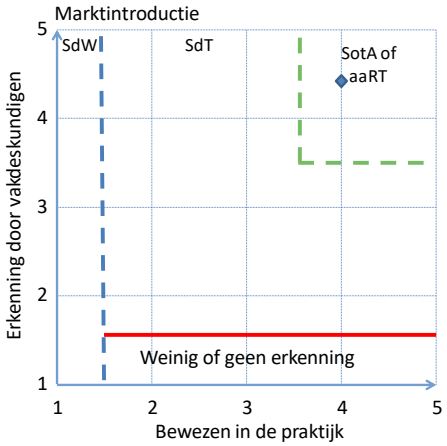
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.3.4 Secure software Development (SSD)

Tijdens het hele softwareontwikkelingsproces moet rekening worden gehouden met de beveiliging van een applicatie. Ongeacht de gebruikte ontwikkelingsmethode moet rekening worden gehouden met

maatregelen voor een veilige ontwikkeling van applicaties. Procesmodellen en best-practices voor veilige softwareontwikkeling zijn beschreven in BSIMM, OWASP SAMM, OWASP ASVS, de BSI-richtlijn "Guidelines for the Development of Secure Web Applications" of ISO/IEC 27034 en onderwezen in de TeleTrusT Professional for Secure Software Engineering T.P.S.S.E. De essentiële beschermingsmaatregelen binnen het softwareontwikkelingsproces staan vermeld in de afzonderlijke hoofdstukken.

Analyse van de vereisten

Veilige applicatieontwikkeling begint met een analyse van de vereisten. De basis van een eisenanalyse is een dreigingsanalyse. De te beschermen (bedrijfs-)activa moeten worden gedefinieerd en de bedreigingen die voor deze activa bestaan moeten worden beschreven. Er moet rekening worden gehouden met de architectuur van de applicatie, met name de gegevensopslag en gegevensstromen, en met de vertrouwensgrenzen. De risico's van deze geïdentificeerde dreigingen moeten vervolgens worden beoordeeld en hieruit moeten tegenmaatregelen en beveiligingseisen voor de applicatie worden afgeleid. Een nuttige methode om specifieke bedreigingen te identificeren is een definitie van zogenaamde misbruikgevallen. Deze beschrijven specifieke aanvallen en het gewenste gedrag van de applicatie in het geval van een aanval. Verdere beveiligingseisen aan de applicatie komen bijvoorbeeld van wettelijke bepalingen en contractuele verplichtingen. Deze beveiligingseisen worden, net als de functionele eisen, meegenomen in de daaropvolgende ontwerpfase van het softwareontwikkelingsproces en ook in de specificatie van de testcases voor de latere tests van de applicatie.

Het Volere-sjabloon[23], dat vaak wordt gezien als de standaard van de algemene vereistenspecificatie, definieert al een aantal beveiligingsvereisten waarmee rekening moet worden gehouden:

- 15a. Toegangvereisten
- 15b. Integriteitseisen
- 15c. Privacyeisen
- 15d. Auditeisen
- 15e. Immuniteitseisen

Software ontwerp

Een veilig ontwerp moet, om de geïdentificeerde bedreigingen tegen te gaan, rekening houden met alle beveiligingsvereisten. Het resultaat van het ontwerpproces is onder andere de beveiligingsarchitectuur inclusief een strategie voor het verwerken van gegevens. Een veilig ontwerp houdt rekening met aspecten zoals veilige authenticatie, cryptografische vereisten, foutafhandeling, systeemconfiguratie, vertrouwensrelatie tussen applicatiecomponenten en de bedrijfslogica van de applicatie. Onvoldoende aandacht voor beveiliging in het ontwerp van een applicatie is vaak de oorzaak van zwakke punten in de applicatie, zoals ontbrekende of onjuiste authenticatie en autorisatie en kan pas achteraf met veel moeite worden verholpen. Andere oorzaken zijn onder meer sleutels en wachtwoorden die in de code zijn ingebouwd, onjuiste behandeling van gevoelige gegevens en onveilige foutafhandeling die de aanvaller nuttige informatie biedt. Het naleven van Secure Design Principles helpt een architect om tot een robuust ontwerp van zijn applicatie te komen. Voorbeelden van dergelijke bewezen ontwerpprincipes zijn Least Privilege, Defense-in-Depth en Secure-by-Default. Ontwerpprincipes zoals Privacy-by-Default worden steeds belangrijker, vooral met betrekking tot de General Data Protection Regulation van de EU. Daarnaast kan een architect gebruik maken van zogenaamde ontwerppatronen en security best-practices, die in tegenstelling tot ontwerpprincipes een meer concrete, maar taalonafhankelijke aanpak bieden voor het oplossen van terugkerende problemen. Het ontwerp, of in ieder geval de ontwerpaspecten die relevant zijn vanuit beveiligingsoogpunt, moeten een ontwerpbeoordeling ondergaan voordat de implementatie van de applicatie begint.

Implementatie

Typische implementatiefouten, zoals de ongecontroleerde verwerking van input, inclusief de output van deze gegevens, en het mengen van code en data, kunnen leiden tot beveiligingslekken zoals: injecties, cross-site scripting en buffer overflows. Speciale programmeerrichtlijnen helpen ontwikkelaars om tijdens de implementatie specifieke aandacht te besteden aan beveiliging, deze moeten individueel worden afgestemd op de gebruikte programmeertalen, bibliotheken en frameworks. Bij het gebruik van frameworks moeten deze correct worden gebruikt om hun beveiligingskenmerken niet te ondermijnen.

[23] https://www.volere.org/templates/volere-requirements-specification-template/

Bijvoorbeeld kan gespecificeerd worden dat alleen bepaalde functies en objecten mogen worden gebruikt en dat softwaremodules alleen mogen worden toegepast na succesvolle tests met een code-analyse tool. Met behulp van statische codecontroles moet de broncode geautomatiseerd worden onderzocht op typische implementatiefouten. De broncode, of in ieder geval de delen van de broncode die relevant zijn vanuit veiligheidsoogpunt (volgens de resultaten van de dreigingsanalyse), moet ook worden onderworpen aan een handmatige code review.

Zwakke punten in de applicatie kunnen echter ook het gevolg zijn van het gebruik van onveilige componenten van andere fabrikanten. Daarom moeten dergelijke componenten zorgvuldig worden geselecteerd en moet de publicatie van beveiligingsbulletins van deze leveranciers, evenals de CVE-database met bekende kwetsbaarheden, voortdurend worden herzien. Een dergelijke controle van componenten van derden moet met behulp van een tool voor afhankelijkheidscontrole geautomatiseerd plaatsvinden. Wanneer u programma's, zoals containeroplossingen, gebruikt om de applicatie te implementeren, moeten deze ook worden gecontroleerd op bekende beveiligingslekken.

Testen van softwarebeveiliging

Met behulp van blackbox / greybox / whitebox tests en statische en dynamische beveiligingsscans wordt gezocht naar kwetsbaarheden in de applicatie. Waar van toepassing verdient, om de hoogst mogelijke efficiëntie te bereiken, een combinatie van black box/grey box en white box testen, evenals statische en dynamische beveiligingsscans met gespecialiseerde tools, de voorkeur. De gebruikte versleutelingsalgoritmen kunnen bijvoorbeeld gemakkelijk door statische analyse van de broncode worden gedetecteerd en geëvalueerd, terwijl beveiligingslacunes die ontstaan door integratie van verschillende componenten of alleen tijdens runtime (zoals in communicatie met een authenticatiedienst) gemakkelijk door dynamische analyse van het systeem kunnen worden gedetecteerd. In tegenstelling tot handmatige beveiligingstests, kunnen beveiligingsscans geautomatiseerd worden uitgevoerd als onderdeel van het softwareontwikkelingsproces om een beveiligingsaudit van elke softwareversie te garanderen, bovendien moeten de vereiste beveiligingsmaatregelen van de applicatie, , d.w.z. de mate waarin de applicatie is beschermd tegen de aanvallen die in de dreigingsanalyse zijn geïdentificeerd, in de testfase worden gecontroleerd. Een goede bron voor het maken van testcases zijn de gedefinieerde misbruikgevallen.
Deze beveiligingstests geven echter geen absolute uitspraak over de beveiliging van de applicatie. Veiligheid kan niet, zoals bij functionaliteitstests, worden bewezen door het feit dat het verwachte gedrag overeenkomt met het waargenomen gedrag. Veiligheid is een negatief criterium, het bestaat meestal uit het voorkomen van ongewenst gedrag. Hier is de creativiteit van een aanvaller bijna eindeloos. Er kunnen dus altijd meer dreigingen zijn en dus ook andere testcases waar nog niet aan is gedacht. Daarom worden penetratietests vanuit het oogpunt van de aanvaller en Breach-and-Attack Simulations (BAS) door goed opgeleid personeel en met de juiste gespecialiseerde toepassingen aanbevolen.

Bescherming van broncode en bronnen

Om de integriteit van code en bronnen te behouden en zo de applicatie te beschermen tegen manipulaties zoals backdoors, Trojaanse paarden en wijzigingen in de stroomlogica, moeten broncodecontrolesystemen worden gebruikt en indien nodig moeten individuele codedelen alleen aan bepaalde ontwikkelaars worden toegewezen. Gevoelige informatie mag niet worden opgeslagen in broncodecontrolesystemen om te voorkomen dat deze onbedoeld naar het publiek wordt gelekt. Daarnaast moet een veilige ontwikkelomgeving worden gewaarborgd door onder andere toegangsrechten te beperken en systemen te versterken, ontwikkelaars alleen gepersonaliseerde gebruikersaccounts te laten gebruiken, niet met beheerrechten te werken en getraind te worden in beveiliging.

Software certificering

Voordat de software wordt geleverd, is het zinvol om deze vooraf te controleren en te certificeren door een neutrale instantie. Hoewel de functionaliteit van de software door middel van testen is gewaarborgd, zorgt certificering ervoor dat de architectuur, het vereistenbeheer, het configuratiebeheer en het risicobeheer geschikt zijn voor een veilig ontwikkelings- en, belangrijker nog, probleemoplossingsproces.

Om kwetsbaarheden later te kunnen verhelpen, moeten architectuur en ontwerp zo worden ontworpen dat niet alleen bugs kunnen worden verholpen, maar ook defecte componenten in geval van noodsituaties kunnen worden vervangen.

Voor complexere software is Requirement Management essentieel. De eisen moeten voor levering (opnieuw) worden gecontroleerd om er zeker van te zijn dat ze duidelijk zijn gedefinieerd volgens International Requirements Engineering Board (IREB). De implementatie van requirements moet herleidbaar zijn tot de broncode. In het eenvoudigste geval kan dit worden gedaan door identifiers toe te wijzen die vervolgens ook worden gebruikt in codeopmerkingen. Dit maakt het mogelijk om snel te reageren op kwetsbaarheden die bekend worden.

Nauw verweven met requirements management is Configuration Management. Hier moet worden nagegaan of een softwareversie met broncode en alle bijbehorende documenten eenduidig kan worden toegewezen aan een versie (en later aan een softwarerelease). Bij het wijzigen van de eisen moet duidelijk zijn welke documenten al up-to-date zijn en rekening houden met de eisen en welke niet. Omdat documenten individueel worden ontwikkeld, hebben de documenten meestal verschillende versies in versiebeheer, daarom moet naast het loutere versiebeheer van de documenten ook een zogenaamde baseline worden gedefinieerd die bepaalt welke documenten in welk versienummer bij elkaar horen en dus overeenkomen met een release. Hierdoor is het mogelijk om te zien welke softwareversie, fouten en kwetsbaarheden al zijn verholpen.

In de eerste stap dient risicomanagement om zich bewust te worden van mogelijke risico's en bedreigingen die zich kunnen voordoen als gevolg van onder andere kwetsbaarheden. Risicobeheer is met name van essentieel belang wanneer mensenlevens in gevaar kunnen worden gebracht. In het geval van softwarecertificering moet voor levering worden gecontroleerd of er een risicobeheersysteem is dat

- Risico's identificeert,
- Risico's classificeert op basis van waarschijnlijkheid en ernst,
- Maatregelen definieert om risico's te verminderen,
- Risico's herclassificeert nadat de maatregelen zijn geïmplementeerd,
- Met regelmatige tussenpozen en in geval van wijzigingen wordt voortgezet.

Als de software in een systeemverband draait, moet ook dit systeemverband worden gecertificeerd.

Oplevering van de software

Een kwetsbaarheid in de oplevering en inrichting van de software kan het resultaat van alle eerdere beveiligingsmaatregelen in het softwareontwikkelingsproces teniet doen. Daarom moet, om te voorkomen dat de productieapplicatieomgeving- in gevaar komt, een veilig leverings- en installatieproces de integriteit van de uitgerolde software waarborgen. Het gebruik van code-signatures is een goede manier om dit te doen, maar aanvallen op de uitgerolde applicatie kunnen ook mogelijk zijn door een onveilige configuratie van de applicatie zelf, daarom moet in de productieomgeving worden gezorgd voor een veilige configuratie van de software en moeten ongeoorloofde wijzigingen in de configuratie worden voorkomen. Als beveiligingsmaatregel worden geschikte standaardinstellingen (Secure by Default), het vierogen-principe en training voor beheerders aanbevolen. Om de potentiële schade van een aanval tot een minimum te beperken, moet de applicatie zo min mogelijk bevoegdheden hebben. Vooral in containeromgevingen worden applicaties vaak onnodig als root-gebruikers uitgevoerd, wat ten koste van alles moet worden vermeden. Ook is het essentieel voor de beveiliging van de applicatie dat deze altijd up-to-date wordt gehouden met betrekking tot beveiligingsupdates.

Security Response

Aangezien kwetsbaarheden nooit volledig kunnen worden uitgesloten, moet elke fabrikant voorbereid zijn op meldingen en snel kunnen reageren. Het security response proces van een fabrikant beschrijft zijn aanpak van het omgaan met beveiligingsproblemen die bij hem bekend zijn geworden. Beveiligingspatches zijn tijdkritisch en moeten daarom snel worden geleverd. Dit omvat zowel in-house ontwikkelde componenten als bekende kwetsbaarheden in standaardsoftware zoals bibliotheken en frameworks. Om beveiligingsonderzoekers te motiveren kwetsbaarheid te melden, zijn Responsible Vulnerability Disclosure of Bug-Bounty programma's een goede optie. Het is essentieel dat gemelde kwetsbaarheden op zo'n manier terugvloeien in het softwareontwikkelingsproces dat ze worden opgelost.

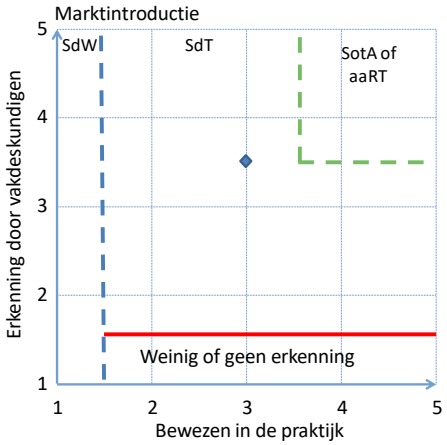
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.3.5 Proces certificering

Om informatiebeveiliging en gegevensbescherming met succes te implementeren in de organisatie, moeten relevante processen worden geïdentificeerd en passende maatregelen worden geïmplementeerd. De uitvoering van dergelijke maatregelen is echter alleen doeltreffend als de doeltreffendheid ervan regelmatig wordt geëvalueerd. Deze verificatie kan worden gedaan door interne en externe bronnen. Een bijzondere externe impact, maar niet verplicht voor alle bedrijven, wordt bereikt door certificering volgens de huidige normen. In dit hoofdstuk worden de mogelijkheden van procescertificering beschreven.

Context Informatiebeveiliging

In het kader van informatiebeveiliging kan een ISMS worden gecertificeerd volgens ISO/IEC 27001 of (in ieder geval in Duitsland) op basis van BSI IT-Grundschutz.

De ISMS-certificeringaudits hebben de volgende doelstellingen:

- Beoordeling van de voortgang van de implementatie van een ISMS
- Bepaling van de naleving van het ISMS van de organisatie met de normen
- Bepaling van het vermogen van het ISMS om te voldoen aan wettelijke, regelgevende en contractuele vereisten
- Testen van de toepassing en effectiviteit van het ISMS
- Signaleren van zwakke punten / verbeterpotentieel van het ISMS

Binnen een toepassingsgebied van het ISMS moeten Interne audits (first-party audits) in het algemeen ten minste eenmaal per jaar door of namens de organisatie worden uitgevoerd. Deze audits zijn verplicht voor ISMS-certificering. Elke organisatie-eenheid (of een onderdeel van de scope, zoals locatie, gebouw, enz.) moet regelmatig intern worden gecontroleerd. In het geval van een interne audit is het essentieel om ervoor te zorgen dat de afdelingen niet zelf auditen, maar dat de audits altijd door een onafhankelijk persoon worden uitgevoerd.

De Second-Party Audits zijn externe ISMS-audits die worden uitgevoerd door stakeholders die geïnteresseerd zijn in de organisatie (bijvoorbeeld eigen klanten). Als externe audits worden uitgevoerd door onafhankelijke auditorganisaties, worden ze "audits door derden" genoemd. In het geval van een uitbestedingscontract kunnen passende leveranciersaudits nodig zijn.

De leverancier (of uitbestedende aannemer) kan echter ook aantonen dat aan de informatiebeveiligingeisen wordt voldaan door middel van een passend certificaat (zoals ISO/IEC 27001 en ISO/IEC 27001 op basis van BSI IT-Grundschutz).

Als een ISMS moet worden gecertificeerd, moet de auditprocedure worden uitgevoerd door een geaccrediteerde certificatie-instelling. Certificatie-instellingen voor ISO/IEC 27001 zijn geaccrediteerd volgens ISO/IEC 17021 en ISO/IEC 27006. Een overzicht van in Duitsland geaccrediteerde instanties voor ISMS-certificering is te vinden op de website van de Duitse accreditatie-instantie (DAkkS). Voor de BSI IT-Grundschutz is het Bundesamt für Informationssicherheit (BSI) de verantwoordelijke certificeringsinstantie.

Bij de certificeringsaudit controleert het auditteam de naleving van de eisen van ISO/IEC 27001 en BSI IT-Grundschutz. Bij de audits moet rekening worden gehouden met de ISO/IEC 27002- en ISO/IEC 27005-normen (en eventuele andere branchespecifieke toevoegingen aan de 27000-normenreeks). Auditoren van ISO/IEC 27001-certificeringsinstanties zijn verplicht om als onderdeel van het auditproces de ISO/IEC 19011- en ISO/IEC 27007-normen in overweging te nemen. In het geval van audits in overeenstemming met BSI IT-Grundschutz moet het respectieve certificeringsschema van de BSI in acht worden genomen.

Certificeringen volgens ISO/IEC 27001 en ISO/IEC 27001 op basis van BSI IT-Grundschutz hebben een geldigheidsduur van 3 jaar en worden ten minste jaarlijks gecontroleerd in het kader van toezichtsaudits. Als het certificaat na 3 jaar moet worden verlengd, moet de organisatie vóór het verstrijken van de periode van drie jaar met succes een hercertificeringsaudit hebben doorstaan.

Afhankelijk van de branche moet mogelijk ook aan branchespecifieke eisen worden voldaan. Nagegaan moet worden of de relevante sectorspecifieke eisen een bewijs van een gecertificeerd ISMS vereisen. Bovendien kunnen verdere eisen worden gedefinieerd die in overeenstemming met de specificatie moeten worden geïmplementeerd en aangetoond. Een overzicht van de gepubliceerde sectorspecifieke normen is te vinden op de website van BSI.

Daarnaast zijn er andere, deels branchespecifieke normen, standaarden en richtlijnen die ook betrekking hebben op afzonderlijke aspecten van informatiebeveiliging (zoals VdS 10000, CISIS12, IDW EPS 980 nF, HIPAA, EuroCloud StarAudit, CSA CCM, ITIL, SOC, PCI DSS, Fedramp).

Andere voordelen die in het voordeel van ISMS-certificering spreken zijn:

- Bewijs van passende risicobeoordeling en behandeling
- Bevestiging van de functionaliteit van het ISMS door onafhankelijke derden
- Bewijs van continue verbetering van het ISMS
- Vermindering van de aansprakelijkheid in geval van incidenten, omdat naleving van een in de EU geharmoniseerde norm aanleiding geeft tot een vermoeden van conformiteit met de erkende regels van de technologie (normen) en de stand van de techniek
- Externe presentatie in het kader van corporate marketing voor reputatie ten opzichte van anderen

Context gegevensbescherming

De implementatie van een Data Protection Management System (DSMS) is ook een goede manier om de effectiviteit van maatregelen in verband met de vereisten van de General Data Protection Regulation (GDPR) te controleren. Hoewel de GDPR een dergelijk systeem niet uitdrukkelijk voorschrijft, toont het toch op veel plaatsen de noodzaak van een dergelijk systeem aan. GDPR Art. 32 lid 1d[24]) vereist bijvoorbeeld een "procedure voor het regelmatig evalueren, beoordelen en evalueren van de effectiviteit van de technische en organisatorische maatregelen om de beveiliging van de verwerking te waarborgen."

Aangezien een dergelijke procedure een geplande en gestructureerde procedure binnen de organisatie vereist, d.w.z. een implementatie van het klassieke PDCA-model vereist, is het opzetten van een DSMS ideaal voor dit doel. Als dit is afgestemd op de elementen van de ISO high-level structure, kan het ook worden geïntegreerd in een bestaand ISMS op basis van ISO/IEC 27001.

[24] Zie ook GDPR Art. 5 lid 2 "De verwerkingsverantwoordelijke (...) moet (...) naleving bewijzen" en GDPR Art. 24 lid1 "(...) en om aan te tonen (...) dat de verwerking in overeenstemming met deze verordening is uitgevoerd".

Net als bij een ISMS kan ook het DSMS worden geauditeerd en zo kan het volwassenheidsniveau van zo'n systeem worden bepaald. Op basis van de ISO/IEC 19011 richtlijn kunnen audits worden uitgevoerd op basis van een auditprogramma en een auditplan. Een audit kan in principe worden uitgevoerd door de functionaris voor gegevensbescherming. Voor grotere organisaties kunnen de audits ook worden uitgevoerd door vakkundig opgeleide medewerkers van de organisatie of adviesbureaus die gespecialiseerd zijn in gegevensbescherming.

Als onderdeel van de zogenoemde leveranciersaudits kunnen ook eventuele verwerkers van de organisatie worden gecontroleerd.

Ongeacht het bovenstaande bestaat in het kader van de gegevensbescherming ook de mogelijkheid van certificering om het bewijs van naleving van de bepalingen van de GDPR te verkrijgen (zie GDPR Art. 42 lid 1). In overeenstemming met GDPR Art. 42 lid 5 moeten in dit verband echter eerst "specifieke certificeringsprocedures voor gegevensbescherming, en ook gegevensbeschermingszegels en keurmerken" worden goedgekeurd door geaccrediteerde certificeringinstellingen in overeenstemming met GDPR Art. 43 (in Duitsland bijvoorbeeld de DAkks) of de bevoegde toezichthoudende autoriteit. Dit is nog niet gebeurd.

Zoals uit de formulering van GDPR Overweging 100 kan worden afgeleid, hebben dergelijke "specifieke certificeringsprocedures voor gegevensbescherming en gegevensbeschermingszegels en keurmerken" echter alleen betrekking op product-, proces- en dienstcertificeringen (conform ISO/IEC 17065). In dit verband vermeldt de GDPR zelf bijvoorbeeld:

- Bewijs van naleving van de verplichtingen van een verwerkingsverantwoordelijke (conform GDPR Art. 24 lid 3);
- Bewijs van naleving van de technische vormgeving en gegevensbeschermingvriendelijke standaardinstellingen (conform GDPR Art. 25 lid 3);
- Bewijs van voldoende garanties van een verwerker (conform GDPR Art. 28 paragrafen 5 en 6);
- Bewijs van de beveiliging van de verwerking (conform GDPR Art. 32 lid 3);
- Bewijs van passende waarborgen in verband met de gegevensverwerking in een derde land (conform GDPR Art. 46 lid 2 onder f)).

Een DSMS kan niet worden gecertificeerd door middel van gegevensbeschermingspecifieke certificeringsprocedures en gegevensbeschermingszegels en keurmerken" in de zin van de GDPR. Deze zijn echter complementair aan een DSMS en kunnen in principe in aanmerking worden genomen als bewijs van naleving van de vereisten van de GDPR bij het auditen van een DSMS.

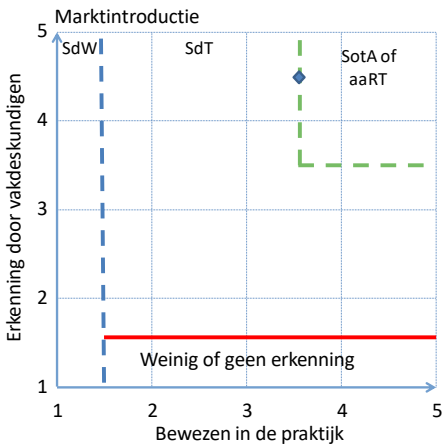
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.3.6 Beheer van kwetsbaarheden en patches

Het doel van kwetsbaarheids- en patchbeheer is het identificeren en oplossen van zwakke punten in de beveiliging en functionaliteit van software en firmware. Patches[25] zijn bedoeld om geïdentificeerde kwetsbaarheden te verhelpen om misbruik ervan te voorkomen. Het proces voor kwetsbaarheids- en patchbeheer omvat het beoordelen, identificeren, evalueren en implementeren ervan in alle producten en systemen van een organisatie. Voor het kwetsbaarheids- en patchbeheerproces moeten de verantwoordelijkheden voor de implementatie en voor het testen van de effectiviteit in de organisatie worden gedefinieerd.

- Beoordeling

Om patches en kwetsbaarheden efficiënt te beheren, moet eerst het IT-landschap van de organisatie worden geïnventariseerd. Aangezien dit in de loop van de tijd kan veranderen, moet een dergelijk onderzoek regelmatig worden uitgevoerd en up-to-date worden gehouden. Componenten die zich niet in het interne netwerk of de cloudomgeving van de organisatie bevinden (zoals smartphones en notebooks van serviceproviders) moeten via speciale richtlijnen worden beheerd. Deze richtlijnen zijn bedoeld om de eigenaren van deze componenten aan te moedigen ervoor te zorgen dat de softwareversie op hun apparaten onafhankelijk wordt bijgewerkt en om ze regelmatig te verbinden met het bedrijfsnetwerk.

- Identificatie en evaluatie

Om kwetsbaarheden, softwarefixes en bedreigingen te identificeren, moeten relevante informatiebronnen (websites van leveranciers, CERT's, CVSS-databases, mailinglijsten van software- en hardwareleveranciers, nieuwsgroepen van derden, enz.) worden gecontroleerd, maar ook moet rekening worden gehouden met professionele tools voor kwetsbaarheids- en patchbeheer van ondernemingen. Iedereen die verantwoordelijk is voor IT-systemen, applicaties, netwerkcomponenten, enz. moet periodiek een overzicht/samenvatting van de huidige patchstatus verstrekken. Hieruit moet een rapport worden gemaakt voor de beoordeling van de huidige kwetsbaarheden en patchsituatie en worden gebruikt om het huidige risico (zoals CVSS-score) te beoordelen. De volgende oplossingen zijn beschikbaar als behandelingsopties:

- Overdracht naar patchbeheer om geïdentificeerde kwetsbaarheden te dichten met een geschikte patch (update),
- Definieer tijdelijke oplossingen (configuratieaanpassing, code-analyse, enz.) om de kwetsbaarheid aan te pakken,
- Het getroffen systeem afsluiten of isoleren.

Als patches om de kwetsbaarheid te verhelpen handmatig worden gedownload, moet hun authenticiteit worden gecontroleerd met behulp van gestandaardiseerde methoden (cryptografische checksums, signatures en digitale certificaten), vooral voor downloads van internet. Patches moeten in de eerste plaats rechtstreeks bij de bronnen van de fabrikanten worden verkregen. Alleen in uitzonderlijke gevallen (bijvoorbeeld in het geval van geïntegreerde producten van derden, zoals runtime-bibliotheken) zijn patches van een andere geverifieerde vertrouwde bron toegestaan.

- Vaststelling

Nadat de authenticiteit van de patches is gegarandeerd, moeten ze worden gecontroleerd in testsystemen. Indien mogelijk moeten de testsystemen op dezelfde of vergelijkbare manier worden uitgerust en geconfigureerd als het productiesysteem.

Vóór de definitieve implementatie in de productieomgeving van de patches moet een back-up van de getroffen systemen worden gemaakt, zodat de patches in geval van een fout opnieuw kunnen worden geïnstalleerd. In het geval van ongewenste prestaties of beperkte functionaliteit moeten maatregelen voor probleemoplossing worden geïdentificeerd en geïmplementeerd.

[25] De drie belangrijkste gebieden zijn:
- Bugfix: Bugfix is het corrigeren van fouten die worden gevonden in de broncode van het programma.
- Hotfix: Hotfix verwijst naar het onmiddellijk oplossen van fouten in het applicatieprogramma.
- Update: Een update is de klassieke vorm van updaten. Het bevat functionele verbeteringen en in sommige gevallen ook het corrigeren van fouten

Om het implementatieproces goed te laten verlopen, moeten de nodige voorbereidingen worden getroffen. Dit omvat bijvoorbeeld het informeren van alle systeemeigenaren en het definiëren van het tijdsbestek voor het verspreiden van patches. De installatie moet ook worden aangekondigd aan gebruikers, zodat ze hun operationele processen op tijd voor de aangekondigde installatieperiode kunnen voltooien.

Normaal gesproken moet de distributie van patches geautomatiseerd plaatsvinden (bijvoorbeeld met een patchbeheertool). Toch kan het voorkomen dat beheerders individuele patches lokaal moeten installeren. In dit geval moet de communicatie veilig worden bewaard en moet de uitwisseling van bestanden plaatsvinden met een authenticatiecontrole.

Zodra patches zijn uitgerold, moet de voortgang worden bewaakt en gecommuniceerd, om bijvoorbeeld mislukte implementatiepogingen op tijd te detecteren. Hiertoe moeten onmiddellijk passende corrigerende maatregelen worden genomen.

- Afhandeling van uitzonderingen

Voor systemen en toepassingen waarvoor

- geen updates van de fabrikant meer beschikbaar zijn (legacy-systemen),
- door de fabrikant nog geen updates van het besturingssysteem zijn uitgebracht,
- niet op korte termijn, om operationele redenen zoals automatisering in de procestechnologie, een onderhoudsvenster beschikbaar kan worden gesteld,
- in geval van een update een hercertificering van het hele systeem noodzakelijk is,

moeten andere technische maatregelen worden geïdentificeerd en uitgevoerd. Omdat een shutdown of eenvoudige herconfiguratie meestal niet compatibel is met operationele vereisten, moeten

- maatregelen aan de netwerkzijde, zoals scheiding, zonering, inkapseling en toepassing van brandwerende wanden, evenals
- netwerkbewaking met behulp van een inbraakdetectiesysteem

bescherming bieden tegen bestaande kwetsbaarheden en deze op kunnen sporen.

Goedkeuringen van de fabrikant

Als, voor de installatie van patches (zoals releases voor patches van databases en besturingssystemen) de het vrijgeven van de fabrikant nodig is, kunnen beschikbare patches meestal, omdat verlies van functionaliteit mogelijk zou zijn en geen garantie zou worden aanvaard door de fabrikant, niet worden geïnstalleerd. Om deze reden moeten perioden voor de release en implementatie van patches en updates en alternatieve workarounds voor kwetsbaarheden contractueel worden vastgelegd met de fabrikant.

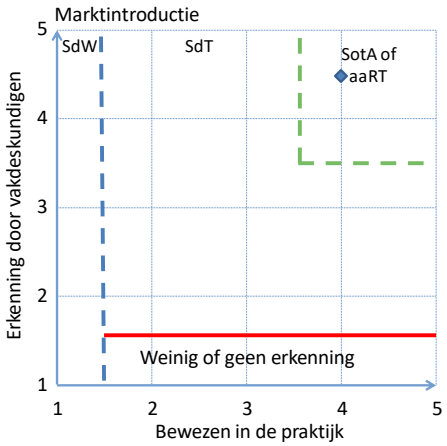
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.3.7 Risicobeheer

Risicobeheer is een essentieel instrument voor het beheersen van bedrijfsrisico's en dus de voorwaarde voor het selecteren van passende risicobeperkende beveiligingsmaatregelen. In de bedrijfsvoering wordt het gebruik van beveiligingsmaatregelen bepaald door een afweging van de kosten en baten. Om de voordelen te bepalen, moeten beveiligingsrisico's worden geïdentificeerd en geëvalueerd. Een goed en gestructureerd beheer van informatiebeveiligingsrisico's (ISRM) zorgt voor de nodige transparantie die het management in staat stelt om in dit kader de juiste beslissingen te nemen. Daarnaast is het beheer van informatiebeveiligingsrisico's[26] een kernelement bij de implementatie en herhaalde actualisering van informatiebeveiligingbeheersystemen en gegevensbeschermingbeheersystemen.

Normen

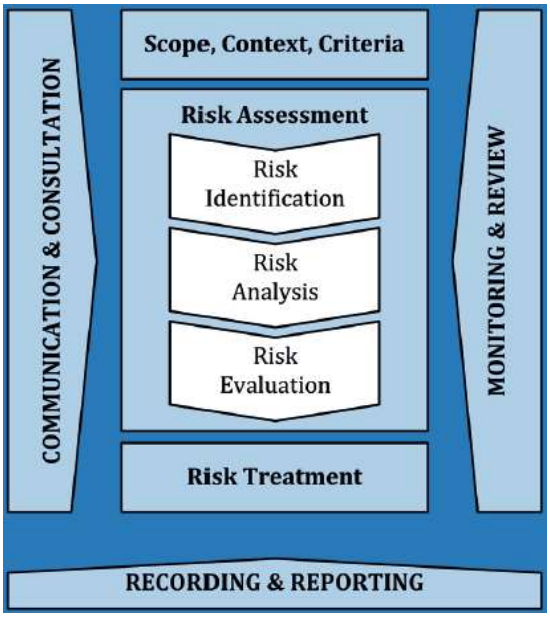
De belangrijkste internationale norm voor risicobeheer in het algemeen is ISO/IEC 31000. De norm die specifiek van toepassing is op informatiebeveiligingsrisico's is ISO/IEC 27005[27]. Deze laatste is qua proces zeer nauw gebaseerd op ISO/IEC 31000, maar bevat aanvullende (niet-normatieve) informatie over de identificatie en evaluatie van assets, voorbeelden van bedreigingen en kwetsbaarheden en methoden van risicobeoordeling in de context van informatiebeveiliging. In Duitsland is de BSI-Grundschutz ook relevant, met name BSI 200-3 (kortweg BSI-GS). Voor industriële automatiseringssystemen is ook de IEC 62443 Part 3-2-norm voor "Safety Risk Assessment and System Design" beschikbaar.

Afhankelijk van de regelgeving moeten organisaties mogelijk voldoen aan andere vereisten, zoals de Europese Richtlijn Netwerk- en Informatiebeveiliging 2 (NIS2) met de Duitse NIS2 Implementation and Cybersicherheitsstärkungsgesetz, de General Data Protection Regulation (GDPR) en de IT-Sicherheitskatalog van het Bundesnetzagentur (IT-SiKat), die alle aanvullende vereisten voor risicobeheer bevatten. Industriespecifieke beveiligingsnormen, de zogenaamde B3S, zijn ook gedefinieerd voor individuele industrieën met betrekking tot de IT-Sicherheitsgesetz en geven aanbevelingen voor de implementatie van risicobeheer voor providers van kritieke infrastructuur.

Proces

Risicomanagement is een cyclisch proces (volgens PDCA = Plan, Do, Check, Act). Naarmate omstandigheden zoals de dreigingsituatie, kwetsbaarheden van het systeem en de technologische omgeving veranderen, moet de risicobeoordeling up-to-date worden gehouden en moet de effectiviteit ervan worden bewaakt. Afbeelding 1 toont het risicoproces volgens ISO/IEC 31000.

[26] In deze tekst verwijzen "IT-risico's" en "IT-beveiliging" naar risico's en beveiliging voor alle soorten informatie, niet alleen voor elektronisch verwerkte gegevens.
[27] De ISO/IEC 27005-norm wordt momenteel herzien.



Afbeelding 6: Risicoproces volgens ISO/IEC 31000

In de eerste stap (**het vaststellen van de context**) worden de basisvoorwaarden voor ISRM gecreëerd. Ten eerste wordt bepaald op welke onderdelen van de organisatie ISRM überhaupt van toepassing is; als het ISRM wordt geïntroduceerd in het kader van een ISMS, vloeit dit meestal voort uit de reikwijdte van het ISMS. De bedrijfsprocessen die in het ISRM moeten worden opgenomen, moeten worden geselecteerd. Van de bedrijfsprocessen uitgaand, wordt rekening gehouden met de bijbehorende organisatieonderdelen, IT- en OT-systemen en -applicaties, faciliteiten voor data- en spraakcommunicatie, serviceproviders en ook eigendommen en gebouwen. Een ISRM-organisatie wordt ingericht met de juiste taakverdeling (bijvoorbeeld voorgezeten door een risicomanager), als dit nog niet is gedaan binnen een ISMS en DSMS. Het is ook raadzaam om, indien beschikbaar, interfaces te definiëren tussen het ISRM en het centrale risicobeheer van de onderneming.

Tijdens de **risico-identificatie** worden bedreigingen geïdentificeerd. Bedreigingen werken tegen waarden (activa). In een ISRM zijn de waarden in de eerste plaats informatie en in de tweede plaats systemen en componenten voor het verwerken en beschermen ervan. Tijdens de risico-identificatie worden de bedreigingen voor de activa bepaald. Volgens de definitie van het BSI zijn bedreigingen de interactie van bedreigingen (zoals natuurrampen, pandemieën, inbraken, hackers, insiders) en kwetsbaarheden (zoals softwarefouten, organisatorische tekortkomingen, technische defecten). De uitdaging is om zoveel mogelijk van deze bedreigingen in kaart te brengen. Gestandaardiseerde risicocatalogi zoals die in ISO/IEC 27005 Annex D en het risico-overzicht uit het BSI Grundschutz Kompendium bieden hierbij ondersteuning. Deze catalogi moeten echter, afhankelijk van de gekozen context en de bestaande waarden, worden aangepast. In dit proces is de samenwerking van informatiebeveiligers en experts, bijvoorbeeld in een werkgroep, belangrijk.

Risicoanalyse betekent het beoordelen van de dreiging in termen van waarschijnlijkheid van optreden en potentieel voor schade. Zoals hierboven al aangehaald, is het zelden mogelijk om terug te vallen op solide cijfers voor IT-risico's. Ook hier zijn de beoordelingen van experts, bij voorkeur uit meerdere disciplines, doorslaggevend. Schade kan van verschillende aard zijn (zoals financiële schade, gevaar voor lijf en leden, aantasting van de aanvoer of productie/productie, reputatie, etc.). Aangezien waarschijnlijkheidsinformatie onderhevig is aan een hoge mate van onzekerheid en schade niet altijd duidelijk kan worden gekwantificeerd, kunnen IT-risico's meestal niet worden uitgedrukt als een concreet getal (kardinaal), maar eerder binnen een ordinale schaal, bijvoorbeeld "hoog", "gemiddeld", "laag". ISO/IEC 27005 Bijlage E biedt nuttige richtlijnen voor dit type classificatie. Een dreiging dat op deze manier wordt geclassificeerd, wordt een "risico" genoemd.

Risico's moeten worden **geëvalueerd** en op de juiste manier worden aangepakt; daarvoor zijn verschillende opties. Je kunt ze bijvoorbeeld bewust dragen (accepteren), je ertegen verzekeren of tegenmaatregelen nemen (zie ISO/IEC 31000 Hoofdstuk 6.4.4), maar je mag ze niet negeren. Op deze manier wordt een bewuste keuze gemaakt. Deze beslissing moet worden genomen door een persoon die de passende verantwoordelijkheid op zich neemt, hetzij voor de kosten van de actie of voor schade

als een risico zich voordoet. Deze persoon wordt gewoonlijk een 'risico-eigenaar'[28] genoemd. Om het risico te verkleinen, stellen deskundigen tegenmaatregelen voor, waarvan de kosten en de vermindering van het risico de basis vormen voor de beslissing om de maatregelen al dan niet uit te voeren. De "risico-eigenaar" neemt vervolgens de beslissing over de uitvoering ervan en de acceptatie van het restrisico dat overblijft nadat de maatregelen zijn geïmplementeerd. Vanwege wettelijke vereisten voor providers van kritieke infrastructuur of in het kader van de GDPR is de "risico-eigenaar" niet volledig vrij om risico's zonder verdere behandeling te aanvaarden of over te dragen.

Communicatie, **melding** (met name in de richting van het management) en **monitoring** zijn ondersteunende processen. Binnen een ISMS en DSMS zijn ze al aanwezig en moeten dienovereenkomstig worden toegepast op ISRM. In de aanwezigheid van een centraal risicobeheersysteem is het belangrijk dat er efficiënte communicatie en complementariteit is tussen dit systeem en het ISRM en dat criteria worden gedefinieerd voor het escaleren van informatiebeveiligingsrisico's naar het centrale risicobeheersysteem van de organisatie die voor beide partijen begrijpelijk en aanvaardbaar zijn.

Praktische tips

De volledige invoering van een ISRM is voor organisaties vaak een veelomvattende taak (in termen van tijd en kosten). Net als andere processen is ISRM onderhevig aan een continu verbeteringsproces, wat tegelijkertijd betekent dat je niet kunt verwachten dat je bij de eerste poging een perfect proces neerzet. Integendeel, een te zware aanpak kan een last voor de toekomst blijken te zijn: het risico bestaat dan dat het proces op de lange termijn "in slaap valt" of alleen wordt geïmplementeerd als een formeel noodzakelijk relikwie zonder enig herkenbaar voordeel. Hierbij is het aan te raden om in het begin te kiezen voor een pragmatische aanpak, waarbij minder aandacht wordt besteed aan volledigheid dan aan kwaliteit. Het is belangrijk dat de risico's met hoge prioriteit worden geïdentificeerd, geanalyseerd en op de juiste manier worden aangepakt en dat er een zo breed mogelijke consensus bestaat tussen de betrokken partijen.

In het begin zijn de identificatie van bedreigingen en de juiste categorisering ervan bijzonder uitdagend. U kunt zich houden aan standaard dreigingscatalogi, zoals die in ISO/IEC 27005. Toch is er zelden een eenduidig antwoord op bijvoorbeeld de vraag of de dreiging van "bliksem" onder "overmacht" moet worden geclassificeerd en als een groot algemeen risico moet worden behandeld en of risico's onafhankelijk van elkaar kunnen worden behandeld, d.w.z. of bijvoorbeeld "bliksem" niet samen met het risico van "stroomuitval" moet worden behandeld. De relaties kunnen willekeurig complex worden, zodat je bepaalde onnauwkeurigheden moet accepteren. Onnauwkeurigheden spelen sowieso een rol via schattingen van de waarschijnlijkheid van optreden. Het is belangrijk om het doel niet uit het oog te verliezen, namelijk dat de resultaten van de risicoanalyse kunnen worden gebruikt om een begrijpelijke beslissing te nemen of er al dan niet actie moet worden ondernomen.

Nauwelijks minder moeilijk is de beoordeling van de waarschijnlijkheid van voorkomen. Het is aan te raden om zoveel mogelijk externe en interne informatiebronnen te gebruiken. De eerste omvatten CVE[29]-lijsten, informatie over fabrikanten, CERT-diensten (zoals van de BSI), de laatste de evaluatie van informatiebeveiligingsincidenten, penetratietests, audits en bewustmakingsmaatregelen. De waarden moeten regelmatig, bijvoorbeeld ten minste eenmaal per jaar, worden aangepast aan de huidige situatie.

Welke beschermingsdoelen worden door de maatregel afgedekt?

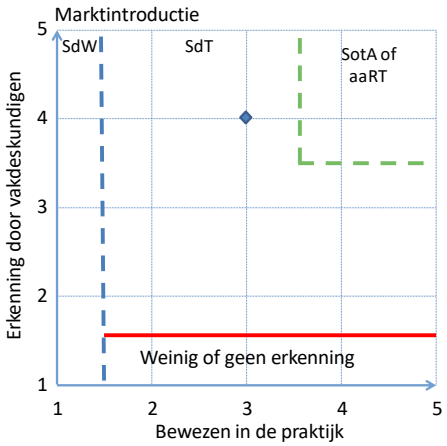
☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

[28] De term "risico-eigenaar" uit ISO 27001 wordt ook wel vertaald als "risico-eigenaar" of "risico-eigenaar", afhankelijk van de verantwoordelijkheden van de betrokkene.
[29] De Common Vulnerabilities and Exposures (CVE) is een gestandaardiseerde lijst van kwetsbaarheden en beveiligingsrisico's van computersystemen.

Kwalificatie van de maatregel



3.3.8 Persoonlijke certificering

De organisatorische maatregelen omvatten onder andere de inzet van gekwalificeerd gespecialiseerd personeel. Dit geldt met name in bedrijfskritische gebieden en kritieke infrastructuren (KRITIS). Dit is de enige manier om de activa van de organisatie te beschermen en te voldoen aan de vele wettelijk vastgelegde eisen met betrekking tot de kwaliteitscontrole van het personeel in dienst.

Vooral vanwege de toenemende verscheidenheid aan technische oplossingen is het absoluut noodzakelijk om alle medewerkers die in de IT-sector werken continu bij te scholen, ook wat betreft innovaties. Medewerkers moeten worden opgeleid en gecertificeerd op basis van de respectieve activiteit en de daaruit voortvloeiende behoeften, zowel met betrekking tot de te vervullen rol (zoals beheerder, ontwikkelaar, IT-architect, auditor, informatiebeveiligingsfunctionaris, functionaris voor gegevensbescherming) als met betrekking tot de branchespecifieke (zoals telecommunicatie, transport) en oplossingsspecifieke (zoals on-premises, cloud) kenmerken.

Met de persoonlijke certificering wordt de beroepskwalificatie aangetoond. Dat komt omdat een persoonlijk certificaat meestal pas wordt afgegeven na een specialistische opleiding en het met succes afgelegde daarop gebaseerde examen.

Afhankelijk van het doel en het toepassingsgebied zijn er verschillende certificeringsprogramma's op de markt. Hieronder staan een paar voorbeelden:

- **Administrators**
  - Er zijn verschillende fabrikantafhankelijke certificeringsprogramma's die gericht zijn op het gebruik, de configuratie en het beheer van het betreffende product. Het gaat hier met name om certificaten van Microsoft, Oracle, Cisco, IBM, maar ook om certificeringsprogramma's van cloudserviceproviders zoals Microsoft, AWS en Google.

  - ITIL-beoefenaars en -managers zijn fabrikantonafhankelijk en naar de processen voor waardecreatie van de informatietechnologie ingedeeld.

- **Software ontwikkelaar**
  - TeleTrusT Professional voor Secure Software Engineering (T.P.S.S.E.) van TeleTrusT De focus van de T.P.S.S.E.-certificering ligt op expertise in hoe en waar beveiligingsaspecten worden geïntegreerd in softwareontwikkeling (www.teletrust.de/tpsse/).
  - Gecertificeerde Secure Software Lifecycle Professional (CSSLP) van ISC² Dit is een leveranciersneutrale certificering die de expertise aantoont van een persoon om, binnen de levenscyclus van een softwareontwikkeling, beveiliging te implementeren (www.isc2.org/Certifications/CSSLP).

- **Software tester**
  - Gecertificeerde testers van verschillende niveaus in verschillende testgebieden van de International Software Testing Qualifications Board (ISTQB) (www.istqb.org/certifications/certification-list/).

- **IT-architecten**
  - Gecertificeerde professional voor software-architectuur (CPSA) door iSAQB
    De International Software Architecture Qualification Board (iSAQB) is een vereniging van software-architectuurexperts uit de industrie, advies- en trainingsbedrijven, de academische wereld en andere organisaties (www.isaqb.org/certifications/).

  - TOGAF, The Open Group Architecture Framework (TOGAF) biedt een benadering voor het ontwerpen, plannen, implementeren en onderhouden van bedrijfsarchitecturen. Als operationeel raamwerk van de Government and Agency Frameworks groep en Instantie biedt de TOGAF de Architecture Development Method (ADM), een procesmodel voor de ontwikkeling van technische architecturen.

- **IT-security auditors**
  - Certified Information Systems Auditor (CISA) door ISACA
    CISA is een wereldwijd erkende certificering op het gebied van auditing, controle en beveiliging van informatiesystemen (www.isaca.de/de/zert-start/international/cisa).

  - ISO/IEC 27001 Leadauditor
    De focus ligt op de voorbereiding en uitvoering van een audit van het Information Security Management System (ISMS). De certificering wordt aangeboden door verschillende aanbieders.

  - IT-Grundschutz-Auditor
    Certificering voor het uitvoeren van audits in overeenstemming met de BSI-normen en het IT-Grundschutz Kompendium.

- **IT-beveiligingsexperts**
  - TeleTrusT Information Security Professional (T.I.S.P.) door TeleTrusT
    De inhoud die voor het T.I.S.P.-certificaat wordt onderwezen, omvat de belangrijkste aspecten van informatiebeveiliging, technische en organisatorische maatregelen en Duitse en Europese wetgeving (www.teletrust.de/tisp/).

  - Gecertificeerde Information Systems Security Professional (CISSP) door ISC²
    Om het certificaat te behalen moet specialistische kennis van veiligheidsrelevante aspecten uit verschillende gebieden van de Common Body of Knowledge (CBK) worden aangetoond (www.isc2.org/Certifications/CISSP).

  - Comptia Security+ van de Computing Technology Industry Association (COMPTIA)
    Dit certificaat richt zich op basiskennis van beveiligingsconcepten en technische en organisatorische maatregelen (www.comptia.org/de/zertifizierungen/security).

  - Certified Information Security Manager (CISM) van ISACA
    De focus ligt op de planning, implementatie, controle en monitoring van IT-beveiligingsconcepten voor specialisten en managers (www.isaca.de/de/zert-start/international/cism1).

Speciaal voor de Duitse markt heeft het Federaal Bureau voor Informatiebeveiliging (BSI) ook een trainingsreeks[30] voor IT-beveiligingsexperts opgezet met een focus op het BSI IT Baseline Protection Kompendium. Het gaat met name om:

  - BSI IT-Grundschutz Praktiker

  - BSI IT-Grundschutz Adviseur

  - BSI IS Penetratietester

[30] www.bsi.bund.de/

- **Functionaris Gegevensbescherming / Coördinator Gegevensbescherming / Adviseur Gegevensbescherming**
  - Tot op heden is geen van de adviserende, vormgevende en controlerende beroepen op het gebied van gegevensbescherming in overeenstemming met ISO/IEC 17024 gecertificeerd volgens een erkende onafhankelijke certificeringsprocedure en door een onafhankelijke certificeerder. Adequate expertise op het gebied van gegevensbescherming is afhankelijk van verschillende factoren en kan niet in één cursus worden gegeven[31]. Daartoe wordt een uitgebreidere opleiding op het gebied van gegevensbescherming aanbevolen. Bijvoorbeeld:

    - Certified Information Privacy Professional (CIPP)
      Deze IAPP-training richt zich op wetten, beleid en normen inzake gegevensbescherming in belangrijke internationale rechtsgebieden, de vaardigheden die nodig zijn om gegevensbeschermingsactiviteiten te beheren en hoe u zich kunt voorbereiden op het certificeringsexamen (iapp.org/train/).

- **Branchespecifieke certificaten**

  - Telecommunicatie
    - Zero-Outage
      De inhoud van de Zero-Outage certificeringen omvat best practices en normen voor het leveren van veilige, betrouwbare en maximaal beschikbare end-to-end IT-diensten en -oplossingen in de telecommunicatiesector (zero-outage.com/).

  - Vervoer
    - Certificaten voor operationele ICT in het spoorwegbedrijf
      De inhoud van de certificeringen voor bedrijfsgerelateerde ICT in het spoorwegbedrijf omvat best practices, normen en standaarden waarmee rekening moet worden gehouden in IT-projecten en IT-toepassingen in het spoorwegbedrijf (www.hmocs.de/).

    - RCS Academie (SBB)
      De inhoud van de RCS Academy certificeringen omvat de best practices, normen en standaarden waarmee rekening moet worden gehouden bij IT-projecten en IT-toepassingen op het gebied van dispatching van spoorwegexploitatie, met name in Zwitserland.

  - Auto-industrie
    - TISAX-auditor
      De Trusted Information Security Assessment Exchange (TISAX) heeft tot doel de informatiebeveiliging in de toeleveringsketen van de auto-industrie te beschermen. Het is sterk gebaseerd op ISO/IEC 27001, maar is specifiek afgestemd op de eisen van de auto-industrie.

In sommige gevallen hebben andere Europese landen hun eigen, individuele certificeringsprogramma's die nog niet aan uniforme regelgeving zijn onderworpen. Een overzicht van de certificeringsprogramma's van de Europese landen is samengesteld door de Europese Cyber Security Organisatie (ECSO) [32].

Welke beschermingsdoelen worden door de maatregel afgedekt?

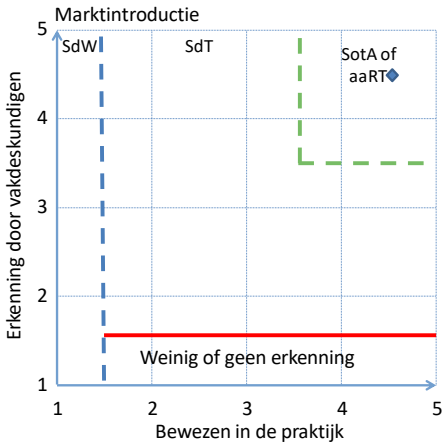
☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

[31] BvD, BvD, Professionele taakomschrijving van de Functionaris Gegevensbescherming, www.bvdnet.de/wp-content/uploads/2018/04/BvD-Berufsbild_Auflage-4_dt_en.pdf
[32] www.ecs-org.eu/documents/publications/5fad54a94cfac.pdf

Kwalificatie van de maatregel



3.3.9 Beveiligen van gebruikersaccounts met speciale rechten

Om systemen te beheren zijn gebruikersaccounts met uitgebreide bevoegdheden vereist. Door mogelijk ongeoorloofd of oneigenlijk gebruik vormen deze accounts en bijbehorende rechten een risico met een kans op grote schade. Daarom moeten passende voorschriften worden opgesteld om een goed IT-systeembeheer te handhaven, in het bijzonder met betrekking tot de toekenning, het gebruik en de intrekking van beheerrechten.

Naast interactieve gebruikersaccounts met beheerrechten worden voor toepassingen en toepassingsservices meestal serviceaccounts gebruikt die geen directe interactie van de kant van een gebruiker met beheerrechten vereisen. Dit omvat ook de serviceaccounts (zoals voor Cron-taken). De onjuiste (meestal te genereuze) van rechten aan serviceaccounts is een grote kwetsbaarheid in de meeste bedrijven toewijzing, die in het bijzonder ook doelwit zijn van aanvallers.

Vereisten voor beheerdersaccount en toegangsrechten

Er moeten richtlijnen en voorschriften worden opgesteld voor het gebruik en de afhandeling van beheeraccounts en machtigingen. Voordat aan een beheerder een beheerdersaccount wordt toegekend, moet de gebruiker eerst akkoord gaan met en ermee instemmen zich aan dit beleid en deze voorschriften te houden. Een overtreding van de gedefinieerde richtlijnen en voorschriften moet worden opgehelderd en gevolgen hebben.

Er moet een restrictieve machtigingsstrategie worden gevolgd, volgens welke, als het niet expliciet is toegestaan of vrijgegeven, de toegang tot hulpbronnen in het algemeen verboden is als. Daartoe moet een gedefinieerd model of een gedefinieerde procedure voor de toekenning van rechten worden toegepast. Een mogelijkheid hiervoor is het Role Based Access Control (RBAC) model. RBAC is een functiegebaseerde toegangscontrole, waarbij autorisaties worden toegekend op basis van gedefinieerde rollen. Gebruikers krijgen een of meer rollen toegewezen en krijgen zo de toegangsrechten van deze rollen. Bij RBAC worden de respectievelijke rollen gedefinieerd op basis van functieprofielen.
Voor de toekenning van beheerrechten moeten de need-to-know en least-privilege principes in acht worden genomen. In het need-to-know-principe ontvangt elke persoon alleen de kennis, autorisatie en/of het bezit van vertrouwelijke informatie die nodig is om zijn of haar eigen taken uit te voeren. Met het least-privilege principe krijgt elke gebruiker precies die rechten die absoluut noodzakelijk zijn voor de vervulling van zijn of haar taken.

De toewijzing van beheerrechten moet worden uitgevoerd in een gedefinieerd en gecontroleerd proces waarin elke aanvraag wordt goedgekeurd en gedocumenteerd. Beheerrechten kunnen pas worden verleend nadat dit proces is voltooid.

Voor beheerrechten moet u toegewezen beheerdersaccounts maken en die verschillen van reguliere gebruikersaccounts, zonder beheerwerk. Activiteiten die ook zonder beheerrechten kunnen worden uitgevoerd, mogen niet door accounts met beheerrechten worden uitgevoerd.

"Superbeheerders" met autorisaties voor alle systemen moeten worden vermeden. Bestaande standaard beheeraccounts moeten afhankelijk van de mogelijkheid worden gedeactiveerd, hernoemd en niet of in beperkte mate worden gebruikt.

Elk account met beheerrechten moet op unieke wijze aan een persoon kunnen worden toegewezen. Als dit vanwege de systeemeigenschappen niet mogelijk is, moet het gebruik van een geanonimiseerd beheeraccount worden beveiligd door bijbehorende organisatorische en/of technische maatregelen en moet de afhandeling hiervan worden vastgelegd. Vereiste groepsaccounts voor beheer activiteiten moeten nauwkeurig worden gespecificeerd (met name de toegestane groep personen) en de afhandeling ervan moet ook worden gedocumenteerd en is alleen in uitzonderlijke gevallen toegestaan. Het gebruik van groepsaccounts moet consequent worden geregistreerd.

Voor alle beheer taken moeten vervangingsregels worden vastgesteld. Daarnaast moeten noodaccounts met beheerrechten worden aangemaakt, waarvan de toegangsgegevens veilig moeten worden opgeslagen. Het gebruik van deze accounts mag slechts in beperkte mate en op een gecontroleerde manier (zoals het vierogen principe) mogelijk zijn en moet worden gedocumenteerd. Voor noodaccounts met multi-factor authenticatie (MFA) is het belangrijk op te merken dat alle factoren voor authenticatie aanwezig en operationeel of toegankelijk moeten zijn, zelfs in noodgevallen.

Als tijdelijke beheerrechten worden verleend, moeten deze een tijds-/logische beperking hebben en moeten ze worden ingetrokken wanneer de noodzaak ophoudt te bestaan.

Beheerdersaccounts met speciale (uitgebreide) bevoegdheden moeten worden beveiligd met een sterke authenticatieprocedure (koppeling van verschillende authenticatie-kenmerken, challenge-response of op certificaten gebaseerde procedures) waarin de identiteit van de gebruiker duidelijk kan worden vastgesteld. Gebruikersaccounts met uitgebreide autorisaties moeten worden beveiligd met authenticatie-kenmerken van verschillende typen (zoals kennis en bezit). Als een authenticatieprocedure die geschikt is voor het risico niet mogelijk is, moet worden nagegaan of aanvullende technische of organisatorische maatregelen nodig zijn om het risico te beschermen. Het gebruik van dezelfde wachtwoorden voor meerdere beheerdersaccounts is niet toegestaan.

Documentatie van alle beheeraccounts en hun respectievelijke autorisaties moet een volledig en up-to-date worden beheerd. Dit geldt zowel voor gebruikte systemen, zoals besturingssystemen of apparaat-firmware, als voor gespecialiseerde toepassingen, zoals centrale toepassingen.

Voor veiligheidskritische activiteiten moet, overeenstemming met het beginsel van functiescheiding, een taakverdeling of een scheiding van taken worden doorgevoerd in. Deze indeling of scheiding moet zo zijn vormgegeven dat het uitvoeren van veiligheidskritische activiteiten wordt gekoppeld aan de aanwezigheid van meerdere gebruikers (bijvoorbeeld door het vierogen principe) of dat een activiteit wordt verdeeld over meerdere personen die elkaar niet mogen vertegenwoordigen. In ieder geval moeten beheerrollen worden gescheiden van controlerende rollen, zoals interne audits.

Alle logins en activiteiten die door beheerdersaccounts worden uitgevoerd moeten worden gelogd, zodat kan worden getraceerd welke activiteiten door welke accounts zijn uitgevoerd. Om de traceerbaarheid van activiteiten, die door beheerdersaccounts worden uitgevoerd, te garanderen, mogen beheerders niet in staat zijn om zelf logfile- en auditlogfiles van hun eigen activiteiten te wijzigen of te verwijderen. Deze logfiles en auditlogfiles moeten regelmatig worden herzien om te controleren of de activiteiten van de administraties aan de voorschriften voldoen.

Serviceaccounts in het gebied Machine-2-Machine (M2M)

De beheerdersaccounts zijn vaak goed beveiligd, terwijl de bescherming van serviceaccounts vaak wordt verwaarloosd. Door gebruik te maken van deze omstandigheid slagen aanvallers er vaak in om de "laterale beweging" te maken, d.w.z. het verplaatsen van het ene gecompromitteerde systeem naar het volgende (vaak meer kritieke) systemen.

Serviceaccounts zijn vaak bijzonder kwetsbaar omdat:

- Deze accounts maken geen gebruik van multi-factor authenticatie (MFA)
- Opgeslagen wachtwoorden van deze accounts zijn zeer eenvoudig te lezen (beheerrechten vereist)

- Aangezien de wachtwoorden van deze accounts vaak niet worden gewijzigd en niet onderhevig zijn aan een nieuw wachtwoordbeleid, zijn ze vanwege hun leeftijd vaak nog steeds erg gemakkelijk te compromitteren
- De wachtwoorden van deze accounts zijn vaak bij veel mensen bekend en het is niet gedocumenteerd welke groep mensen er toegang toe heeft
- Deze accounts hebben vaak te uitgebreide rechten en volgen daarom niet het principe van least-privilege
- Deze accounts worden vaak voor te veel doeleinden gebruikt en tellen dus onnodig veel rechten op

Alle serviceaccounts moeten worden aangemaakt en gedocumenteerd volgens een gedefinieerde procedure. Voor deze accounts moeten sterke, willekeurig gegenereerde wachtwoorden worden gebruikt en deze mogen alleen toegankelijk worden gemaakt voor een klein, afgebakend deel van de mensen. Als mensen de organisatie verlaten met kennis van de toegangsgegevens van deze accounts of van functie veranderen, moeten de wachtwoorden worden gewijzigd na een passende risicobeoordeling.

Voor de bescherming van serviceaccounts mag interactieve toegang niet worden toegestaan voor deze accounts en elke poging om interactief in te loggen met een dergelijk account moet onmiddellijk worden onderzocht. Voor elke taak en service moeten afzonderlijke, specifieke accounts worden aangemaakt (en niet bijvoorbeeld slechts één account per systeem) en het principe van de minste bevoegdheden moet strikt worden nageleefd. Om niet per ongeluk extra rechten van andere accounts over te nemen, mogen serviceaccounts niet van andere accounts worden gekopieerd.

Aanbevelingen / Implementatie

Voor het beheer van beheerdersaccounts en hun toegangsrechten, evenals voor de implementatie van regelgeving, wordt het gebruik van een Privileged Access Management (PAM)-oplossing aanbevolen. Relevante normen zijn:

- ISO/IEC 27002:2022
  De norm bevat aanbevelingen voor de implementatie van de maatregelen die vereist zijn door ISO/IEC 27001 Annex A voor de toewijzing, het beheer en de audit/control van beheeraccounts. Als certificering in overeenstemming met ISO/IEC 27001 wordt nagestreefd, moeten deze maatregelen worden geïmplementeerd in het kader van het ISMS. Implementatie-instructies voor deze maatregelen zijn voornamelijk te vinden in de paragrafen 8.2 "Geprivilegieerde toegangsrechten", "8.15 Logging" en "8.18 Gebruik van hulpprogramma's met geprivilegieerde rechten".
- BSI IT-Grundschutz Kompendium (februari 2022)
  Het BSI IT-Grundschutz Kompendium beschrijft in de OPS.1.1.2-module bedreigingen in verband met beheerdersaccounts en afgeleide vereisten voor het omgaan met deze accounts.
- Oostenrijks handboek voor informatiebeveiliging
  Het Oostenrijkse handboek voor informatiebeveiliging bevat aanbevelingen voor het beheer van gebruikers, inclusief beheeraccounts. Aanbevelingen zijn te vinden over de toewijzing, het beheer en de documentatie van toegangsrechten, evenals over de regulering van toegangsopties in geval van vertegenwoordiging en noodsituaties.
- BDEW White Paper: Eisen voor veilige controle- en telecommunicatiesystemen 2.0
  Naast de eis om te voldoen aan het need-to-know-principe in de algemene vereisten, beveelt de BDEW-whitepaper ook aan dat applicaties en gespecialiseerde applicaties ook gebruikersconcepten moeten implementeren waarin beheerdersrollen in kaart kunnen worden gebracht en in kaart kunnen worden gebracht met gedetailleerde toegangscontrole.

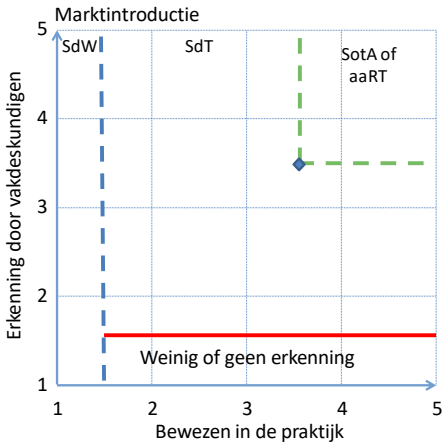
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.3.10 Dark-web Monitoring

Verlies van bedrijfskritische informatie kan ernstige gevolgen hebben. Een ieder die op de hoogte is van het verlies kan reageren. Net als in de echte wereld, waar gestolen goederen op de zwarte markt worden verhandeld, wordt via het internet gestolen bedrijfsinformatie (zoals informatie over kwetsbaarheden, bevindingen van gebruikte cookies, gestolen inloggegevens, informatie over betalingstransacties) op het dark-web[33] verhandeld. Dark-web verwijst naar een groot aantal afzonderlijke netwerken (darknets) binnen het internet.

Het dark-web wordt door aanvallers gebruikt om informatie met elkaar uit te wisselen en om gestolen bedrijfsinformatie weer te geven en/of te verkopen. Dit gebeurt meestal direct na de aanval. Technische compromittering van bedrijven, systemen en netwerken vinden vaak ongemerkt plaats. Ze leiden tot een datalek of kunnen worden gebruikt als voorbereiding voor een gerichte aanval. Het monitoren van het dark-web kan daarom helpen om bewijs van een aanval op een bedrijf die heeft plaatsgevonden of op handen is, te identificeren en te documenteren en om op basis van de beschikbare informatie passende corrigerende maatregelen te nemen.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

Regelmatig gericht monitoren van het dark-web[34] in opdracht door gespecialiseerde dienstverleners of applicaties kan helpen om geplande of verwachte toekomstige aanvallen door andere aanvallers (zoals door een ransomware aanval, illegale gegevensdiefstal of vervolgaanvallen) te voorkomen. De maatregel draagt zo bij aan het minimaliseren van de risico's. Het kan ook supply-chain aanvallen (ook bekend als aanvallen op de waardeketen) aan het licht brengen om te voorkomen dat een aanval op de eigen omgeving indirect wordt uitgevoerd via externe leveranciers of leveranciers of via de toeleveringsketen.

Dark-web monitoring biedt zelf geen bescherming tegen de dreiging van compromittering (indringing door daders). De inzichten die voortvloeien uit dark-web monitoring kunnen echter de risico's voor de getroffen organisatie minimaliseren door passende responsmaatregelen te nemen om verdere schade te voorkomen of op zijn minst te beperken.

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Handmatige analyses van de openbaar beschikbare informatie over een organisatie en de huidige dreigingsituatie voor de betreffende branche worden uitgevoerd, om vervolgens geautomatiseerde, individueel aan de organisatie aangepaste, regels en voorschriften op te stellen.

Deze zorgen voor een regelmatige monitoring (minimaal dagelijks) van bijvoorbeeld:

- Marktplaatsen en forums op het dark-web (o.a. mogelijk via speciale aanbieders)

[33] Ook wel Darknet of Deep Web genoemd
[34] Als een speciale vorm van informatie over cyberdreigingen (zie hoofdstuk 3.2.27)

- Gepubliceerde datalekken (zoals Identity Leak Checker van het Hasso Plattner Instituut[35])
- Openbare en niet-openbare communicatie op het World Wide Web en op sociale mediaplatforms, met inbegrip van relevante gesloten gebruikersgroepen
- Waarschuwingen van relevante autoriteiten (zoals BSI of US-Cert)
- Verslaggeving

De handmatige analyses van de informatie en de dreigingsituatie worden indien nodig, om een continue optimalisatie van de regelgeving te garanderen, herhaald.

Een hoge mate van automatisering en professionalisering kan op basis van de grote hoeveelheid data die te verwachten is, meestal alleen worden bereikt door middel van een managed service. Daarnaast moeten gespecialiseerde data-analisten met een onderzoekende tactische achtergrond bij de taken worden betrokken.

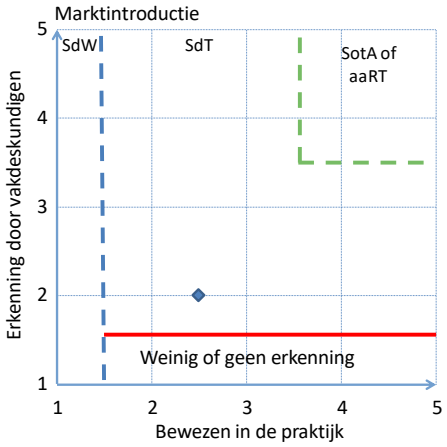
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.3.11 Omgaan met dienstverleners

Het uitbesteden van diensten kan voordelig zijn als dienstverleners gerichter en innovatiever zijn en de opdracht beter of goedkoper kunnen leveren dan de klant of een speciale technologie in gebruik hebben.

Het inschakelen van dienstverleners gaat soms echter gepaard met aanzienlijke risico's (zoals afhankelijkheid, verlies van controle en controlemogelijkheden, risico's voor informatiebeveiliging). In het ergste geval kunnen deze risico's het bestaan van de organisatie in gevaar brengen. Hoe vertrouwelijker, gevoeliger de gegevens of gegevens die onderworpen zijn aan beperkingen (zoals vertrouwelijkheid, gegevensbescherming), hoe groter het risico. Tegen deze achtergrond zijn de selectie, controle, monitoring en verificatie van dienstverleners als organisatorische maatregel van cruciaal belang.

Het uitbesteden van diensten (zoals netwerkbeheer) gaat gepaard met verschillende bedreigingen voor de IT-beveiliging (inclusief informatiebeveiliging), zoals:

- Inbreuk op de beveiliging die leidt tot vernietiging, verlies, wijziging of ongeoorloofde openbaarmaking van of toegang tot gegevens

[35] sec.hpi.de/ilc/search

- Onjuiste of ongepaste omgang door derden van de verstrekte gegevens met het oog op de uitvoering van het contract
- Misbruik van door de dienstverlener verkregen toegangsrechten en de daaruit voortvloeiende diefstal, verlies of ongeoorloofde openbaarmaking van de verstrekte gegevens
- Menselijke en organisatorische fouten of wangedrag als gevolg van het niet naleven van overeengekomen technische en organisatorische maatregelen
- Juridische risico's (zoals schade als gevolg van handelen of nalaten van dienstverleners, boetes of gevangenisstraffen, officiële bevelen)
- Financiële risico's (zoals falen van de dienstverlener door insolventie).

Om deze bedreigingen tegen te gaan, worden de volgende maatregelen aanbevolen:

1. **Maatregelen voor de selectie van dienstverleners:**
    - Ontwerp of aanpassing van het aankoopproces met als doel de nadruk te leggen op gegevensbescherming en informatiebeveiliging, bijvoorbeeld door de juiste instanties bij het selectieproces in een vroeg stadium te betrekken en minimumnormen (basisnormen) vast te stellen op basis van individuele of algemeen aanvaarde normen (zoals Trusted Computer System Evaluation Criteria (TCSEC))
    - Uitvoering in gestructureerde vorm van verzoeken om informatie (RFI) met vragen over informatiebeveiliging, of over gegevensbescherming met het verzoek om een bindende verklaring van de dienstverlener
    - Request for Proposal (RFP) van verschillende dienstverleners op basis van een gedetailleerde specificatie of specificatie en individuele eisen op het gebied van gegevensbescherming en informatiebeveiliging
    - Due diligence, d.w.z. zorgvuldig onderzoek met evaluatie van alle relevante aan een juridische transactie verbonden juridische risico's

2. **Maatregelen voor het beheer en de beoordeling van dienstverleners:**
    - In ieder geval is het raadzaam om, met betrekking tot het toezicht op dienstverleners, intern verantwoordelijkheden te definiëren en te delegeren
    - Het type en de reikwijdte van de maatregelen zijn afhankelijk van verschillende factoren, zoals de grootte van de organisatie, de complexiteit van de service level agreement (SLA), de organisatiestructuur en bestaande processen in de organisatie
    - Vaststellen en toepassen van de, in overeenstemming met de vastgestelde en contractueel overeengekomen vereisten, criteria voor de continue monitoring van de bekwaamheid van de dienstverleners (in overeenstemming met ISO/IEC 9001 subparagraaf 8.4)
    - Idealiter worden de maatregelen geïntegreerd in een IT-risicobeheersysteem dat is ingebed in de bestaande bedrijfsprocessen (zoals IT-beveiligingsbeheer, compliancebeheer, gegevensbeschermingsbeheer).

3. **Maatregelen voor het toezicht op dienstverleners:**
    - Prioritering van taken en bepaling van inspectie-intervallen
    - Bepaling van het type en de reikwijdte van de auditmaatregelen (zoals auditmaatregelen ter plaatse, gebruik van vragenlijsten en commerciële databases voor het risicobeheer van de dienstverlener, enz.) door het individuele risico dat gepaard gaat met de ingebruikname van de betreffende dienstverlener te beoordelen op basis van de mate van waarschijnlijkheid dat bepaalde risico's zich voordoen, de mate waarin het risico kan worden beïnvloed en de inspanning die nodig is om dit te doen
    - Audits van dienstverleners / leveranciers (IT-beveiligingsaudits, gegevensbeschermingsaudits, fysieke beveiligingsaudits) tijdens de uitvoering van het contract
    - Beheer van contracten, certificaten en andere documentatie.

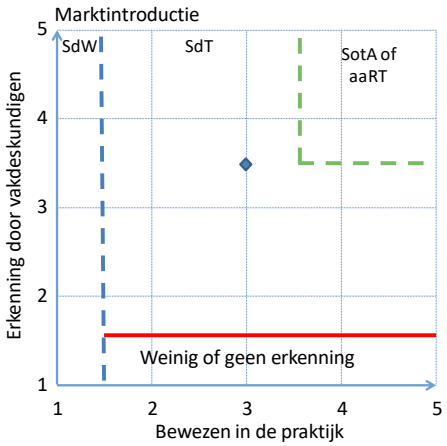
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.3.12 Software stuklijst (SBOM)

Een software bill of materials (verder geduid als software stuklijst) is een lijst van componenten en hun afhankelijkheden die een IT-applicatie of -service nodig heeft. Deze lijst is machineleesbaar en zorgt voor transparantie over de gebruikte componenten van derden. Dit kan worden gebruikt om kwetsbaarheden die door onderliggende componenten worden veroorzaakt te bepalen.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

De maatregel is bedoeld om bij supply-chain aanvallen, die worden uitgevoerd door gebruik te maken van beveiligingslekken in de gebruikte componenten (zoals softwarebibliotheken), het potentiële aanvalsoppervlak te kunnen identificeren. Zonder SBOM is er geen informatie over welke componenten in een gebruikte IT-applicatie of -dienst worden gebruikt en dit maakt het veel moeilijker, zo niet onmogelijk, om potentiële kwetsbaarheden te identificeren.

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

SBOM levert een volledige BOM van alle componenten die in een IT-applicatie of -dienst worden gebruikt. Aan de hand van deze informatie kun een lijst met beveiligingslekken, die mogelijk aanwezig zijn in een bepaald onderdeel, worden gecontroleerd en zo informatie verstrekken over de vraag of de IT-toepassing of -service die gebruikt wordt ook door dit beveiligingslek kan worden getroffen.

Voor SBOM zijn verschillende dataformaten ontwikkeld. ISO-standaarden zijn er voor de SPDX[1]- en SWID[2]-formats en OWASP heeft de CycloneDX[3]-standaard overgenomen. SWID en SPDX worden voornamelijk gebruikt voor de unieke identificatie van software voor verschillende doeleinden (niet alleen beveiliging). CycloneDX daarentegen richt zich op de beveiliging van applicaties en de analyse van supply-chain componenten, zelfs buiten software, waaronder bijvoorbeeld hardwarecomponenten en clouddiensten.

SBOM is een centrale maatregel voor de verdediging tegen aanvallen op de toeleveringsketen. De Amerikaanse regering heeft de verstrekking en het gebruik van SBOM door leveranciers verplicht gesteld aan de Amerikaanse overheid door middel van een uitvoerend bevel in mei 2021[4], gespecificeerd door het Amerikaanse ministerie van Handel (juli 2021)[5] en NIST (februari 2022)[6].

De Europese Commissie heeft het aanbieden van een SBOM geformuleerd[36] als een van de centrale beveiligingsvereisten als onderdeel van de Cyber Resilience Act. Daarnaast heeft BSI met de TR03183 de technische specificaties voor een software stuklijst (SBOM) gedefinieerd[37].

[36] EU CRA, digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
[37] BSI, SBOM-vereisten: TR-03183-2: TR-03183-2, www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/TR-03183-2-SBOM-Anforderungen.html

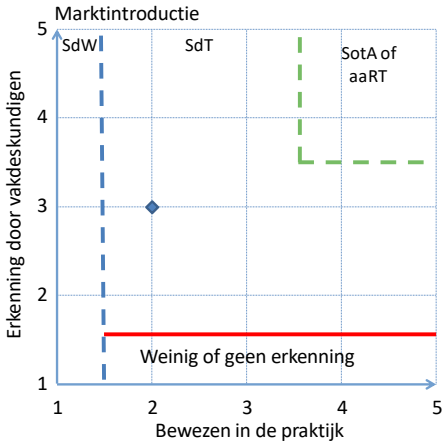
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.3.13 Geo-redundanties

Het efficiënte gebruik van de ingezette systemen en applicaties hangt onder andere af van de constante beschikbaarheid daarvan. Een uitval van de IT-infrastructuur (zoals netwerken, applicaties, opslag, databases en rekencapaciteit) heeft een directe negatieve impact op de bedrijfsvoering. Als een hoge beschikbaarheid vereist is, moet de IT-infrastructuur redundant worden opgezet en in geval van een noodsituatie op korte termijn beschikbaar worden gesteld. De redundantie moet zo zijn ontworpen dat een uitval van een enkel onderdeel niet leidt tot het uitvallen van de gehele IT-infrastructuur. Afhankelijk van een risicoanalyse kan geo-redundantie een bijzondere rol spelen.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

De lijst van elementaire bedreigingen[38] van het Duitse Federale Bureau voor Informatiebeveiliging (BSI), ook bekend als de G0-catalogus, is vastgesteld als een standaard en biedt een gestructureerd overzicht van 47 potentiële bedreigingen en kwetsbaarheden in informatiesystemen. Door de toepassing van deze catalogus, inclusief hun beoordeling en prioritering, in de beoordeling van beschermingsbehoeften en risicoanalyse te standaardiseren, kunnen organisaties een uniform begrip van risico's ontwikkelen en efficiënter werken. Bovendien bevordert standaardisatie de vergelijkbaarheid van beveiligingsmaatregelen en verbetert het de communicatie tussen verschillende actoren op het gebied van informatiebeveiliging.

Uittreksel van elementaire bedreigingen met een focus op bedreigingen voor de beschikbaarheid:

- Brand (G.01), water (G.03), natuurrampen (G.05)
- Stroomuitval (G.08)
- Systeem-, netwerk- (G.09) en servicestoring (G.011)
- Lichamelijke schade, inbraak (G.044), vandalisme (G.044), diefstal (G.044) etc.

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

[38] BSI - Elementaire bedreigingen vanaf 07.12.2020, www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Elementare-Gefaehrdungen/elementare-gefaehrdungen_node.html

Om een hoge beschikbaarheid te garanderen moet de gebruikte IT-infrastructuur redundant zijn. Hier betekent "redundantie" dat in dezelfde constellatie en configuratie een component meerdere keren (minstens twee keer) beschikbaar is. Welk onderdeel van de IT-infrastructuur redundant, of zelfs geo-redundant, moet worden ingericht, wordt bepaald door de risicoanalyse.

Een IT-infrastructuur is redundant als zijn technische tweeling

- gelijkwaardige middelen in stand houdt,
- structureel gescheiden is,
- volledig onafhankelijk is op het gebied van stroomvoorziening, airconditioning en netaansluiting
- en zonder terugwerking van elkaar is opgezet.

In het geval van een storing, bijvoorbeeld als gevolg van storm, aardbevingen, sabotage, stroomuitval of componentfouten, neemt de redundant opgezette IT-infrastructuur een deel of het geheel van de verwerking over om zo de werking van het hele systeem te behouden.

De configuratie van redundantie is afhankelijk van de risicobeoordeling en de mogelijke potentiële hoeveelheid schade. Hoe korter de downtime die vanuit operationeel oogpunt kan worden getolereerd, hoe meer de IT-infrastructuur van redundante componenten moeten worden voorzien. Dit leidt op zijn beurt tot hogere kosten voor de voorbereiding ervan en voor een voortdurend bijgewerkte voorraad.

Geo-redundantie houdt als geografisch criterium ook rekening met locatie. De keuze van de locatie moet individueel worden overwogen, aangezien deze gebaseerd is op de individuele risicoanalyse van de organisatie. Aanbevelingen over relevante criteria zijn bijvoorbeeld te vinden bij het BSI[39]. Daar zijn met name de ruimtelijke afstanden van redundante datacenters te zien en die als ruwe richtlijn kunnen worden gebruikt.

In de context van het toenemende gebruik van clouddiensten moet, in het kader van een uit te voeren risicobeoordeling, worden gevalideerd of redundantie van de gebruikte operationele componenten moet worden vastgesteld. Meestal worden deze niet automatisch aangemaakt door de cloudserviceprovider (CSP), maar moeten ze afzonderlijk worden geconfigureerd. Ook hier is het zinvol om vooraf een redundantieconcept op te stellen dat past bij de risicobeoordeling en paraatheid van de organisatie.

Cloudaanbiedingen hebben vaak heel vaal vrij te kiezen opties voor geo-redundantie, die tegen de juiste kosten kunnen worden aangeschaft. Een afweging moet worden gemaakt tussen eisen en kosten, waarbij rekening moet worden gehouden met de vooraf relevant geachte risicofactoren.

Bij het ontwerp en de uitvoering van geo-redundantie moet ook rekening worden gehouden met juridische aspecten. Dit is met name relevant bij het gebruik van niet-Europese dienstverleners en datacenters, aangezien deze onder verschillende jurisdicties kunnen vallen en dus mogelijk voor verschillende interpretaties kunnen leiden (zoals vergelijking van de CLOUD Act versus de GDPR).

Op het hoogste beveiligingsniveau moet ook worden nagedacht over een onafhankelijke doorontwikkeling van de clouddienst. Dit vereist onder meer escrow-procedures, een werking onafhankelijk van de fabrikant en de ontwikkeling van technische expertise.

Welke beschermingsdoelen worden door de maatregel afgedekt?

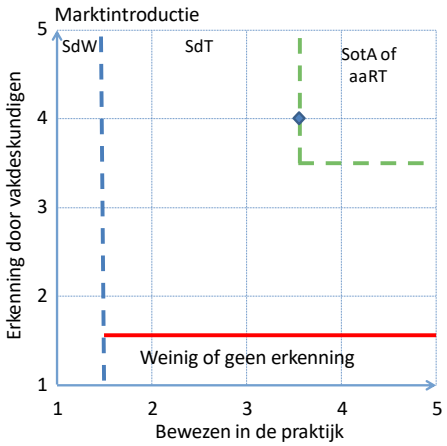
☒ Beschikbaarheid

☐ Integriteit

☐ Vertrouwelijkheid

[39] BSI - Locatiecriteria voor datacenters (bund.de), www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Hochverfuegbarkeit/Standort-Kriterien_HV-RZ/Standort-Kriterien_HV-RZ_node.html

Kwalificatie van de maatregel



3.3.14 Bewustzijn van de gebruiker

Van medewerkers wordt verwacht dat ze zich in hun dagelijkse werkzaamheden houden aan alle wet- en regelgeving op het gebied van informatiebeveiliging. Als workflows (bijvoorbeeld het openen van een e-mailbijlage) eenmaal een gewoonte zijn geworden, zijn ze moeilijk te veranderen. Daarom zijn er nieuwe "veilige" routines nodig. Deze kunnen niet op alleen uitgevaardigd worden, maar moeten ook worden geoefend. Daarnaast moet er een basisbegrip en motivatie ontstaan bij de medewerkers, zodat zij de maatregelen op lange termijn en duurzaam uitvoeren.

Tegen welke dreiging(en) van IT-beveiliging wordt de maatregel ingezet?

- Het bevorderen van aanvallen (zoals social engineering en ransomware) en mogelijk schadelijke acties vanwege onvoldoende bewustzijn van informatiebeveiliging
- Compromittering van accounts voor aanvallen of uitbuiting door fraudeurs
- Verlies of openbaarmaking van vertrouwelijke gegevens door onzorgvuldig handelen
- Het niet detecteren van beveiligingsincidenten en ontoereikende actie na een beveiligingsincident

Welke actie (procedures, faciliteiten en werkingswijzen) wordt in dit hoofdstuk beschreven?

Organisaties moeten ervoor zorgen dat medewerkers[40] hun activiteiten uitvoeren in overeenstemming met de regels voor informatiebeveiliging. Bewustwording en kennis alleen hiervoor zijn niet voldoende. Er is nieuw veilig gedrag nodig, deze moeten worden geoefend en verankerd als een nieuwe routine in het dagelijkse werk. Daarnaast moet het management het goede voorbeeld geven en een voorbeeld zijn van deze routines.

De benadering van de organisatie van het onderwerp bewustzijn moet gestructureerd zijn. De volgende stappen moeten worden gevolgd:

1. Selectie van onderwerpen en thema's
2. Bepaling van de doelstellingen van de bewustwordingscampagne(s)
3. Uitvoering en verificatie van de doeltreffendheid

Bij de **keuze van onderwerpen en thema's** moet in de eerste plaats rekening worden gehouden met de resultaten van het eigen risicobeheer en de eigen doelstellingen op het gebied van informatiebeveiliging. Andere aspecten zoals informatiebeveiligingsincidenten in de eigen of vergelijkbare organisaties, het in overweging nemen van de eigen informatiewaarden ("kroonjuwelen"), de eigen bedrijfscultuur, eisen van belangrijke stakeholders, de analyse en evaluatie van de eigen informatiebeveiligingskengetallen en de resultaten van audits moeten ook bij de selectie worden betrokken.

[40] Alle personen die onder toezicht van de organisatie werkzaamheden verrichten. Wanneer in dit hoofdstuk over medewerkers wordt gesproken, wordt dit altijd in deze bredere zin bedoeld.

De **doelen van de bewustwordingscampagne(s)** moeten worden geformuleerd als concrete, operationele doelen. Meetbaarheid vereist criteria die kunnen worden gebruikt om te bepalen in hoeverre het doel is bereikt (doelbereikcriteria). De doelen moeten voor aanvang worden gedefinieerd en gedocumenteerd, bovendien moet een aankondiging aan de werknemers worden overwogen als dit het bereiken van doelen verbetert.

De **implementatie** gebeurt in negen stappen, waarvan de meeste op elkaar zijn afgestemd[41]:

1. **Veiligheidshygiëne**: Allereerst moeten de eigen voorschriften worden gecontroleerd op feitelijke en praktische haalbaarheid. Van niemand kan worden verwacht dat hij zich aan regels houdt die in het kader van zijn eigen werk niet of slechts met aanzienlijke moeite kunnen worden toegepast. Als dit het geval is, moet worden nagegaan of de regels zodanig kunnen worden aangepast dat ze het gewenste doel bevorderen en kunnen worden geïmplementeerd. Beveiliging kan het meest effectief worden verbeterd wanneer het eenvoudig te implementeren is en naadloos kan worden geïntegreerd in bestaande processen.
2. **Informatie**: Medewerkers hebben informatie nodig over de bestaande regelgeving, d.w.z. dat deze bekend en beschikbaar moet worden gesteld.
3. **Sensibilisering**: Medewerkers moeten worden bewust gemaakt worden. Daarbij mogen geen bedreigingsmodellen worden gebruikt en mag geen angst worden gecreëerd, maar motivatie. Dit kan bereikt worden door professionele en persoonlijke meerwaarde aan te tonen.
4. **Kennis en begrip**: Medewerkers moeten weten en fundamenteel begrijpen hoe hun "onveilige" gedrag door de dreigingen kan worden uitgebuit.
5. **Toestemming**: Werknemers moeten actief en, indien mogelijk, vrijwillig instemmen om hun steentje bij te dragen, d.w.z. om hun eigen gedrag te veranderen.
6. **Verwachte zelfredzaamheid**: Medewerkers moeten ervan overtuigd zijn dat ze het gewenste gedrag ook daadwerkelijk kunnen bereiken en hiermee een belangrijke bijdrage leveren.
7. **Vaardigheden implementeren**: Hiermee worden de nieuwe vaardigheden geïmplementeerd. Het gewenste nieuwe gedrag wordt geoefend en medewerkers worden eraan herinnerd dat ze hebben ingestemd met het nieuwe gedrag, hoe het oude gedrag eruit zag en waarom het niet langer wordt toegepast.
8. **Verankering**: Het nieuwe gedrag moet verankerd worden en terugval in oude gewoontes moet worden voorkomen. Verankering kan door herhaling, methoden van moedwillig vergeten en nudging[42] geregeld en geïmplementeerd worden.
9. **Veilig gedrag**: In de laatste stap is het nieuwe veilige gedrag routine geworden. Om dit nieuwe gedrag te ondersteunen, kan een beloningssysteem worden geïntroduceerd.

Voor elke stap moeten geschikte hulpmiddelen en ondersteuningsmethoden worden gekozen. Bij de selectie van externe diensten en dienstverleners moet ervoor worden gezorgd dat de hierboven beschreven substappen van het implementatieproces worden afgedekt. Indien nodig moeten deze worden aangevuld met verdere maatregelen.

Alle maatregelen moeten geselecteerd en op een manier die geschikt is voor de doelgroep geïmplementeerd worden op basis van de behoeften van de verschillende geadresseerden (softwareontwikkelaars, IT, HR-afdeling, marketing, verkoop, enz.).

Om ervoor te zorgen dat aan de voorwaarden voor de uitvoering van de volgende processtap wordt voldaan en om ervoor te zorgen dat de gestelde doelen worden bereikt, moet na elke processtap een doeltreffendheidstest worden uitgevoerd. Indien nodig moet de stap worden herhaald of versterkt.

Welke beschermingsdoelen worden door de maatregel afgedekt?

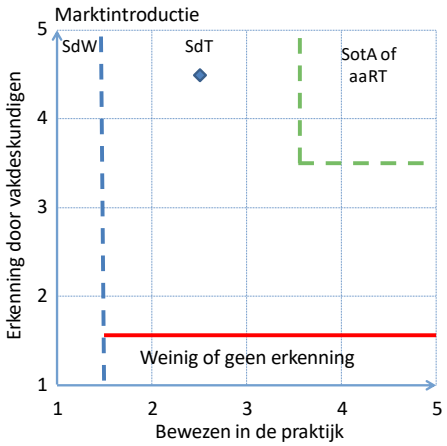
☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

[41] Human-Centred Security am Horst-Görtz-Institut für IT-Sicherheit, Ruhr Universität Bochum (hgi.rub.de/)
[42] Stups of Chubs, in de zin van stof tot nadenken. Het creëren van randvoorwaarden die mensen aanmoedigen om een (ook door henzelf gewenst) gedrag te vertonen, bijvoorbeeld het in het zicht en binnen handbereik positioneren van gezonde voeding in een kantine.

Kwalificatie van de maatregel



3.3.15 Asset Management

Een "asset" is elk type (financiele-, informatie-) waarde van een organisatie. Asset Management gaat over het beleid en de processen die helpen om gedurende zijn levenscyclus rekening te houden met elk asset. Vanuit het oogpunt van IT (IT asset management) gaat het om het beheer van IT-middelen - hardware, software en ook data en clouddiensten die door de organisatie worden gebruikt.

Vanuit het oogpunt van informatiebeveiliging vormt de lijst van activa en eigenaren de basis voor een analyse van de beschermingsbehoeften en helpt het bij het prioriteren van risicobehandeling en de keuze van beschermingsmaatregelen. Het is van essentieel belang dat het asset-register geen uitputtende lijst is, maar analoog aan de CMDB in ITIL moet worden verstaan en grofweg kan worden onderverdeeld in immateriële en materiële activa.

Vanuit het oogpunt van IT-security biedt IT asset management de basis voor een compleet beeld van het IT-landschap van de organisatie en daarmee voor alle IT-beveiligingsmaatregelen met betrekking tot IT-assets; inclusief risicobeoordeling, patchbeheer, beveiligingsmonitoring en zero trust.

Zonder gestructureerde asset management kunnen organisaties kwetsbaar zijn voor ongeoorloofde toegang, verlies en vernietiging van kritieke informatie. Immers, als de waarden van de organisatie onbekend zijn, is het niet mogelijk om hun behoefte aan bescherming vast te stellen en ook niet om passende beschermingsmaatregelen te nemen.

Asset management maakt het mogelijk om te voldoen aan wet- en regelgeving en bevordert de operationele efficiëntie door een duidelijke toewijzing van verantwoordelijkheden en middelen. Bovendien voorkomt volledig asset management het ontstaan van "schaduw-IT", die aanvallers kan voorzien van veelbelovende aanvalsvectoren die niet door de organisatie worden gecontroleerd. Daarom moet asset management worden geïntegreerd in de essentiële inkoopprocessen.

De belangrijkste taken in asset management zijn:

- **Inventarisatie en registratie**: Alle bedrijfswaarden moeten systematisch worden geïnventariseerd, geclassificeerd en geregistreerd.
- **Verantwoordelijkheden toewijzen**: Voor elk bedrijfsmiddel moet een duidelijke verantwoordelijkheid worden gedefinieerd, inclusief de verantwoordelijkheid om deze te beschermen.
- **Classificatie**: Bedrijfsactiva moeten worden geclassificeerd op basis van hun belang en om ervoor te zorgen dat ze adequaat worden beschermd.
- **Beleid en procedures**: Implementeer duidelijke beleidsregels en procedures voor de behandeling en bescherming van media om ongeoorloofde distributie, wijziging en vernietiging te voorkomen.
- **Periodieke beoordeling**: Evalueer en actualiseer het asset managementplan regelmatig om ervoor te zorgen dat het voldoet aan de huidige bedreigingen en bedrijfsdoelstellingen.

In tal van normen en voorschriften worden de bewezen praktijken en aanbevelingen beschreven, waaronder:

- BSI-norm 200-2: Deze definieert een gestructureerde aanpak voor het bepalen van de assets en het classificeren van de beschermingsvereisten van normaal tot zeer hoog
- ISO/IEC 27001: Deze internationale norm voor informatiebeveiligingbeheersystemen (ISMS) benadrukt het belang van asset management.
- NIST SP 800-53: Het raamwerk van het National Institute of Standards and Technology (NIST) biedt richtlijnen voor het beheer van informatiesysteembronnen.
- ISO/IEC 19770-1: Specificeert in de context van de organisatie de eisen voor een IT asset management systeem
- COBIT: ISACA's Control Objectives for Information and Related Technologies (COBIT) framework omvat principes en praktijken voor IT-beheer, inclusief asset management.

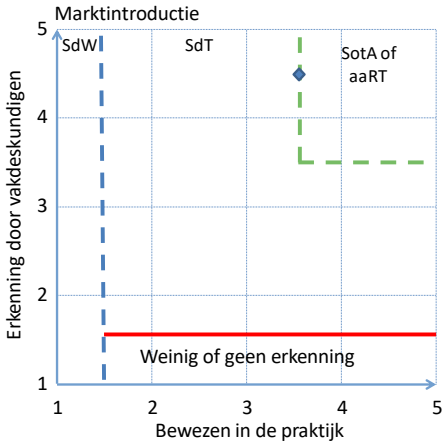
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☒ Integriteit

☒ Vertrouwelijkheid

Kwalificatie van de maatregel



3.3.16 Incident Management

Security incident management combineert als reactie op gedetecteerde en potentiële beveiligingsincidenten technische en organisatorische maatregelen. Naast het registreren, analyseren en beheren van problemen, kwetsbaarheden en gerichte aanvallen, beschrijft en plant het ook hoe om te gaan met dergelijke incidenten, inclusief juridische kwesties.

Het doel van security incident management is het aansturen van planning, het identificeren en implementeren van randvoorwaarden om effectieve en efficiënte maatregelen te kunnen nemen om de organisatie in geval van een incident onverwijld te beschermen.

De belangrijkste activiteiten van incident management zijn:

- Registratie: Melding en identificatie van het incident
- Classificatie: Beoordeling en classificatie als beveiligingsincident
- Analyse: Onderzoek naar en bepaling van de omvang van het incident
- Reactie: Implementatie van mitigerende en herstelmaatregelen
- Herstel: Terugkeer naar de normale bedrijfsvoering en waarborg van de integriteit
- Follow-up: Documentatie en analyse om toekomstige incidenten te voorkomen

Aangezien incidenten vaak gepaard gaan met een schending van de beveiligingsdoelstelling beschikbaarheid, moet in eerste instantie een gekwalificeerde "eerste analyse" en classificatie van een incident worden uitgevoerd. Afhankelijk van het resultaat wordt vervolgens op basis hiervan de verwerking overgenomen door het betreffende specialistische team. Het is zinvol om een onderscheid te maken tussen functionele en beveiligingsincidenten (of deze op zijn minst afzonderlijk te labelen), aangezien beide verschillende benaderingen, vaardigheden en maatregelen vereisen. Functionele incidenten hebben invloed op de algemene bedrijfsvoering en IT-diensten, terwijl beveiligingsincidenten specifiek gericht zijn op de dreiging en inbreuk van de informatiebeveiliging. Deze laatste vereisen vaak meer dringende en gespecialiseerde maatregelen om de schade te minimaliseren en de integriteit van de systemen te waarborgen.

Van de behandelaars van beveiligingsincidenten zijn bijvoorbeeld kennis van IT-beveiliging en de netwerkarchitectuur van het betreffende bedrijf, en operationele ervaring in het forensisch onderzoek van beveiligingsincidenten vereist.

Om deze vereisten voortdurend te waarborgen, is het gebruik van Security Operations Center (SOC) en Computer Security Incident Response Team (CSIRT) teams zinvol. Het SOC maakt continue monitoring van de IT-infrastructuur, snelle identificatie van bedreigingen en gecoördineerde responsacties mogelijk. Een CSIRT richt zich op enkelvoudige, ernstige en complexe incidenten. Dit verhoogt de efficiëntie en effectiviteit van incidentmanagement aanzienlijk.

Het samenbrengen van gegevensbronnen in SIEM-systemen (Security Information and Event Management) of andere platforms voor de identificatie en beoordeling van beveiligingsincidenten is een belangrijke voorwaarde voor vroegtijdige detectie en analyse van bedreigingen. Voor snelle responstijden worden (gedeeltelijk) geautomatiseerde processen aanbevolen, eventueel met behulp van Security Orchestration, Automation and Response (SOAR) oplossingen.

Naast het definiëren en documenteren van een gestandaardiseerde procedure voor het beheer van beveiligingsincidenten, moet ook worden gezorgd voor training van werknemers om het beveiligingsbewustzijn van het personeel en de praktijk van het omgaan met beveiligingsincidenten te versterken.

Het opzetten van een beveiligingsincident-team kan worden gedaan met behulp van de ISO/IEC 27035, NIST SP 800-61 of CIS Controls-frameworks.

De transitie van een ernstige onderbreking van de dienstverleningsonderbreking kan van incident naar groot incident en verder naar het bijeenroepen van het noodsituatiehulpteam leiden.

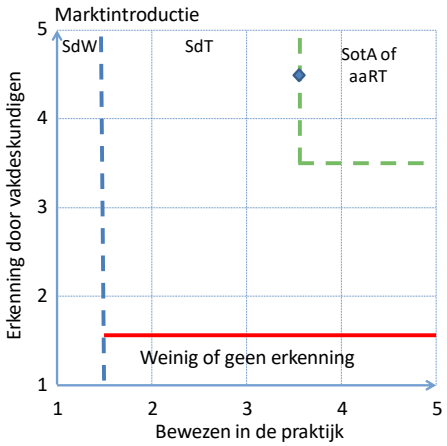
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☐ Integriteit

☐ Vertrouwelijkheid

Kwalificatie van de maatregel



3.3.17 Business Continuity Management (BCM)

Business continuity management (BCM) is een systematische aanpak die ervoor zorgt dat bedrijven ook in crisissituaties in staat blijven om te handelen. BCM omvat strategieën en maatregelen om tijdkritische bedrijfsprocessen te beveiligen en downtime te minimaliseren.

De introductie van een BCM vereist de ondersteuning, afstemming en beschikkingstelling van middelen door het topmanagement, dit wordt vastgelegd in de BCM-richtlijn en daarmee wordt de BCM in werking gesteld.

BCM is essentieel om de weerbaarheid van een organisatie tegen verschillende bedreigingen te waarborgen. Zonder een robuust BCM-systeem kunnen bedrijven, in het geval van verstoringen en crises, aanzienlijke financiële verliezen, reputatieschade en operationele storingen lijden. De behoefte aan BCM komt voort uit het brede scala aan potentiële bedreigingen waarmee organisaties worden geconfronteerd:

- **Natuurrampen**: Gebeurtenissen zoals aardbevingen, overstromingen en stormen kunnen de fysieke infrastructuur van een bedrijf ernstig beschadigen en de bedrijfsvoering verstoren.
- **Cyberaanvallen**: Aanvallen op de IT-infrastructuur (zoals malware, DDoS, ransomware) kunnen leiden tot aanzienlijk gegevensverlies en bedrijfsonderbrekingen.
- **Technische storingen**: Stroomuitval, hardwaredefecten en softwarefouten kunnen de werking van kritieke systemen beïnvloeden.
- **Pandemieën en epidemieën**: Gezondheidscrises (zoals COVID-19-pandemie) kunnen de beschikbaarheid van personeel en middelen ernstig beperken.
- **Falen in de toeleveringsketen**: De toenemende afhankelijkheid van informatietechnologie (IT), functionerende toeleveringsketens en externe dienstverleners (zoals service-, toeleverings- en nutsbedrijven) maakt bedrijven kwetsbaar voor verstoringen. Deze verstoringen belemmeren de beschikbaarheid van bedrijfsprocessen en vormen dus een aanzienlijk risico voor het Business Continuity Management System (BCMS). Een robuust BCMS moet daarom expliciet maatregelen bevatten om dergelijke verstoringen van de toeleveringsketen te identificeren, te beoordelen en te beheren.

BCM wordt gebruikt om te kijken naar de algehele situatie en de veerkracht van de onderneming. Het gaat vooral om het onderhouden van tijdkritische bedrijfsprocessen en de benodigde technische en organisatorische componenten en maatregelen.

Een effectief BCMS bestaat uit verschillende kerncomponenten:

1. **Risicobeoordeling en dreigingsanalyse**: Identificatie en beoordeling van potentiële risico's en bedreigingen voor de organisatie. Deze vormen de basis voor alle verdere BCM-activiteiten.
2. **Business Impact Analysis (BIA)**: Dit omvat het identificeren van kritieke bedrijfsprocessen, het kijken naar de impact van verstoringen op de bedrijfsvoering en het stellen van prioriteiten voor herstel.

3. **Strategieontwikkeling**: Dit maakt het mogelijk om strategieën en maatregelen te ontwikkelen om bedrijfsprocessen in stand te houden en snel te herstellen. Naast de maatregelen is het essentieel dat de rollen en verantwoordelijkheden binnen de organisatie bindend zijn vastgelegd. Er moet voor worden gezorgd dat alle betrokken partijen hun taken kennen en effectief kunnen optreden in geval van een crisis.
4. **Implementatie en testen**: Ten slotte worden de ontwikkelde strategieën en calamiteitenplannen geïmplementeerd. Hun effectiviteit moet regelmatig worden getest en indien nodig worden aangepast. De BCM-plannen moeten, op basis van de resultaten van tests en incidenten uit de echte wereld, regelmatig worden herzien en bijgewerkt.

De implementatie van een BCM-systeem kan in wezen langs de volgende kaders worden gedaan:

- **ISO 22301**: Deze internationale norm vertegenwoordigt de erkende norm voor het opzetten en exploiteren van een BCMS. Het structureert de vereisten voor de planning, implementatie en monitoring van een BCMS volgens de ISO-vereisten voor managementsysteemnormen en vormt de basis voor de mogelijkheid van certificering van een BCM-systeem.
- **BSI-Standard 200-4**: Deze norm biedt uitgebreide praktische richtlijnen voor het opzetten van een BCM-organisatie en het implementeren van een BCMS, met name in verband met de IT-Grundschutz op basis van ISO 27001. De Standard 200-4 wordt met uitgebreide tools gratis ter beschikking gesteld door het BSiG.

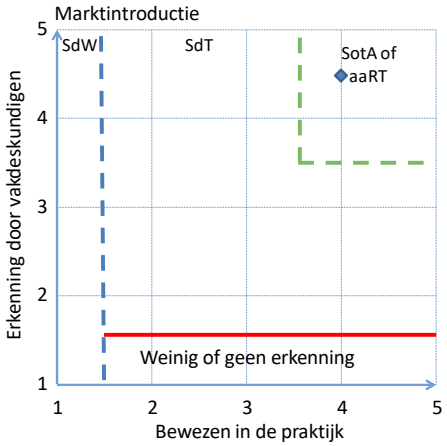
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☐ Integriteit

☐ Vertrouwelijkheid

Kwalificatie van de maatregel



3.3.18 Crisis- en calamiteitenbeheer

Calamiteitenbeheer verwijst naar de planning en implementatie van maatregelen om snel en effectief te reageren op IT-noodsituaties, zoals systeemstoringen en cyberaanvallen. Het doel hiervan is om de impact van dergelijke incidenten te minimaliseren en de bedrijfsvoering zo snel mogelijk te herstellen.

Crisismanagement daarentegen houdt in dat wordt gereageerd op ernstigere en vaak onvoorspelbare gebeurtenissen die een flexibele en alomvattende aanpak vereisen. Daarbij gaat het om het nemen van strategische beslissingen om de stabiliteit en veiligheid van de organisatie op de lange termijn te waarborgen.

Een noodsituatie kan tot een crisis leiden of als zodanig worden uitgeroepen, dat vereist een gestandaardiseerde procedure en gecoördineerde criteria volgens welke het overeenkomstige kritikaliteitsniveau en het daarvoor bestemde procesprotocol worden geactiveerd.

Een (cyclisch) crisismanagementproces bestaat uit:

1. Situatiebeoordeling / controle
2. Beoordeling van de situatie
3. Planning en selectie van maatregelen
4. Delegatie en uitvoering van maatregelen

Hoewel BCM en nood- en crisismanagement erg op elkaar lijken, verschillen ze in hun aanpak:

	BCM	**Crisisbeheersing in noodsituaties**
Focus	Zekerheid van bedrijfscontinuïteit op lange termijn	Korte termijn respons en beheer van acute dreigingen
Doel	Voldoen aan de beschikbaarheidseisen van kritieke bedrijfsprocessen	Bescherming van mensen en activa, minimalisering van schade
Activiteiten	Opstellen en testen van bedrijfscontinuïteitplannen (GFP) voor kritieke bedrijfsprocessen en services	Onmiddellijke reactie, operationele en strategische beslissingen tijdens een crisis
Scenario 's	Aanwezigheid en bekendheid van noodplannen voor storingsscenario's en processen.	Onbekende en bijzonder ernstige scenario's waarvoor geen noodplannen zijn opgesteld.

Tabel 4: Differentiatie tussen BCM vs. nood- en crisismanagement

Er moet een structuur worden afgesproken en gedocumenteerd voor de eerste uren en dagen van een crisis. Met name de alarmering en escalatie, de samenstelling en het vermogen om te werken van het crisisteam en maatregelen voor het snelle herstel van bedrijfsprocessen moeten worden vastgelegd.

Met behulp van de parameters die in een BIA worden verzameld, kan het schadepotentieel van een storing worden beoordeeld. Gestandaardiseerde beoordelingen in combinatie met de inachtneming van de tijdshorizon helpen om het zogenaamde niet-duurzaamheidniveau te definiëren en daaruit passende maatregelen af te leiden.

Opmerking: Belangrijke parameters en termen van BCM en noodbeheer zijn gedefinieerd in de woordenlijst van BSI-norm 200-4:
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_BCM_Glossar.pdf?__blob=publicationFile&v=3

Crisisdefinitie en activatie van crisisorganisatie
Het moet duidelijk worden geregeld wie de huidige situatie tot crisis mag verklaren, rekening houdend met alle informatie die op dat moment beschikbaar is en zo de gedefinieerde processen en middelen mag activeren. Deze beslissing kan worden genomen op basis van vooraf gedefinieerde criteria met betrekking tot de impact en omvang van het incident. In wezen geldt dat wanneer de behandeling van het incident de mogelijkheden van de gevestigde structuren te boven gaat en de effecten niet kunnen worden voorzien, noch in termen van tijd, noch in termen van effecten. Wanneer de crisis wordt uitgeroepen, neemt het crisisteam, onder leiding van de crisismanager, de verantwoordelijkheid op zich voor het beheersen van de situatie.

Crisisteam en verantwoordelijkheden
De samenstelling van het crisisteam kan, afhankelijk van de aard van de crisis, variëren. Om het crisisteam grotendeels in staat te stellen beslissingen te nemen zonder dat andere commissies hoeven te worden geraadpleegd, is het raadzaam om, naast de crisismanager ten minste één lid van de directie ter beschikking te stellen. Het is zinvol om een crisis-kernteam te vormen met de nodige rollen in elke crisis. Dit kernteam wordt, afhankelijk van de situatie, aangevuld met andere rollen. Afhankelijk van de behoeften kan het volgende worden overwogen:

Kernteam	Situative Ergänzung
• Beheer • Communicatie • Recht • Protocol (situatierapport)	• Vertegenwoordigers van kritieke afdelingen • IT • Communicatie • Staf • Financiën • Rechts • Privacy • externe crisisadviseurs • Ondernemingsraad • Secretaresse

Tabel 5: Samenstelling van het crisisteam

Om ervoor te zorgen dat ook bij afwezigheid van individuele leden kan worden gehandeld , moet voor elke functie in het crisisteam moet een duidelijke plaatsvervangende regeling en toegankelijkheid worden gedefinieerd.

Situationele verlengingen zijn op elk moment mogelijk met als doel alle noodzakelijke competenties te betrekken die nodig zijn voor een snelle beslissing over hoe verder te gaan.

Communicatie en informatie-uitwisseling
In geval van een crisis moeten alle interne en externe belanghebbenden die buiten het crisisteam relevant zijn, via vooraf gedefinieerde communicatiekanalen worden geïnformeerd, worden geïntegreerd in het werk van de crisisorganisatie en worden geïnformeerd over de huidige situatie. Een crisiscommunicatieplan moet de volgende aspecten omvatten:

- Interne communicatie: regelmatige updates naar medewerkers
- Externe communicatie: mediamanagement, klantinformatie, communicatie met autoriteiten
- Vooraf gebouwde communicatiesjablonen voor verschillende crisisscenario's
- Definiëren van sprekersrollen en communicatiekanalen

Rapportagevereisten en wettelijke vereisten
Er zijn verschillende meldingsverplichtingen die in acht genomen moeten worden:

- Providers van kritieke infrastructuren (KRITIS, NIS2) moeten, in overeenstemming met de specificaties en meldingskanalen, incidenten melden aan het Federaal Bureau voor Informatiebeveiliging (BSI).
- Afhankelijk van de branche, zoals telecommunicatiebedrijven (Bundesnetzagentur) en financiële instellingen (BaFin), kunnen ook rapportageverplichtingen relevant zijn.
- Als toegang tot persoonsgegevens niet kan worden uitgesloten, moet overeenstemming met de GDPR binnen 72 uur een melding worden gedaan bij de bevoegde gegevensbeschermingsautoriteit in.

Naast deze wettelijke en reglementaire meldingsverplichtingen moeten ook interne meldingsverplichtingen worden opgesteld en dienovereenkomstig in acht worden genomen (cyberverzekering, aangifte bij de politie, enz.). Het is belangrijk om deze rapportageverplichtingen regelmatig, ten minste jaarlijks, te controleren om ervoor te zorgen dat ze up-to-date zijn en zo nodig aan te passen. Voor elke meldingsverplichting moeten specifieke contactpersonen en organen worden genoemd en moeten hun contactgegevens altijd worden bijgewerkt.

Regelmatige herziening en bijsturing
Crisisbeheersingsplannen moeten beschikbaar zijn, regelmatig worden herzien en bijgewerkt om te reageren op nieuwe uitdagingen en veranderingen in de bedrijfsstructuur en juridische omgeving.

Deze herziening kan worden uitgevoerd in regelmatige (ten minste jaarlijkse) oefeningen (bijv. table-top oefeningen, planvergaderingen, stafoefeningen,...) om de effectiviteit van de crisisprocessen te waarborgen. Evenzo moet na het einde van een crisis follow-up worden uitgevoerd om de bestaande

plannen, basis van de opgedane kennis over effectiviteit en potentieel voor verbetering, bij te werken op.

De BSI-noodkaart[43] en de noodhandleiding[44] zijn zeer nuttig gebleken. Ze bieden operationele sjablonen met de belangrijkste gegevens in één oogopslag om voorbereid te zijn op het worstcase scenario.

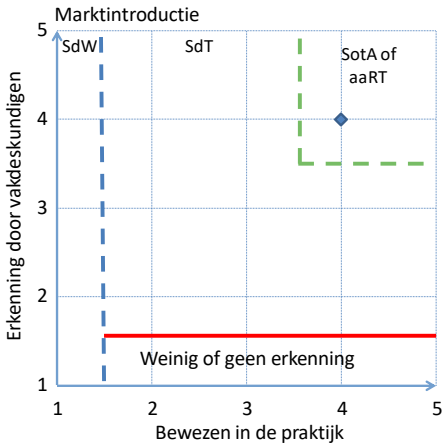
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☐ Integriteit

☐ Vertrouwelijkheid

Kwalificatie van de maatregel



3.3.19 Calamiteitenoefeningen

Wereldwijd blijft het aantal cybersecurity-aanvallen en -dreigingen toenemen. De vraag "of een bedrijf wordt aangevallen" is dan ook achterhaald. In plaats daarvan moeten bedrijven zich voorbereiden op een aanval en de organisatorische maatregelen die daaruit voortvloeien en deze regelmatig testen en oefenen.

Als onderdeel van een calamiteitenoefening kunnen de mogelijke effecten van een succesvolle cybersecurity-aanval worden gesimuleerd. Er zijn verschillende vormen van calamiteitenoefeningen mogelijk, zoals table-top oefeningen, crisisteamoefeningen en volledige oefeningen. Calamiteitenoefeningen kunnen geïsoleerd worden gepland, bijvoorbeeld binnen de afdeling, of geïntegreerd (gezamenlijke calamiteitenoefeningen). De oefening als simulatiespel stelt je in staat om te testen hoe je met een fictieve aanval moet omgaan en om je eigen reactievermogen te testen. Het doel van de oefening is om mogelijke organisatorische zwakheden te identificeren om deze in geval van nood te voorkomen.

De calamiteitenoefening zal de aanpak van de vooraf gedefinieerde veiligheidsdreigingen en in het bijzonder de effectiviteit van bestaande organisatorische maatregelen testen en zwakke punten identificeren. De deelnemers worden geconfronteerd met een onbekende situatie waar ze discursief

[43] BSI Notfallkarte: www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/IT-Notfallkarte/it-notfallkarte_node.html

[44] BSI Notfallhandbuch: www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_Vorlage_Notfallhandbuch.html

mee om moeten gaan (bijvoorbeeld door middel van vragen, taken en acties). Een dergelijke calamiteitenoefening maakt In het bijzonder het volgende mogelijk:

- Het, in een gerichte oefening vóór een noodsituatie, omgaan met concrete dreigingscenario's
- Bespreking en testen van bestaand beleid, calamiteitenplannen en procedures
- Ontwikkelen van organisatorische maatregelen en testen in hoeverre deze maatregelen werken tegen specifieke dreigingen
- Testen van bestaande organisatorische maatregelen
- Bewustzijn creëren van rollen, competenties en verantwoordelijkheden
- Verantwoordelijkheden en communicatielijnen onder de loep nemen en onderwerpen aan een stresstest
- De paraatheid te bevorderen en vertrouwdheid met procedures te oefenen.

De implementatie van veiligheidsoefeningen vereist een individueel incidentscenario dat is ontworpen voor de betreffende organisatie en is gericht op de specifieke kenmerken ervan. Afhankelijk van de behoeften kunnen de individuele omstandigheden van de uit te voeren incidenten tijdens de oefening in complexiteit en omvang worden verhoogd.

Voorafgaand aan de veiligheidsoefening moeten doelen worden gesteld om de effectiviteit van de oefening te valideren. Zo kunnen bijvoorbeeld de volgende doelen worden gedefinieerd:

- Processen van informatie-uitwisseling tussen belanghebbenden moeten worden geoefend
- De effectiviteit van het noodplan moet worden getest
- Maatregelen moeten worden ontwikkeld tegen een specifieke dreiging
- Crisiscommunicatie, intern en/of extern, moet worden getest.

Om de meest relevante dreiging voor het scenario te identificeren, kunnen risicoanalyse en bedreigingsmodellering worden gebruikt. Indien haalbaar en verstandig, kunnen technische hulpmiddelen ook worden gebruikt om het te testen scenario te meten en de effectiviteit ervan te evalueren.

De calamiteitenoefening moet plaatsvinden in een vertrouwde, informele en fouttolerante setting, met voldoende procesoriëntatie. Aangezien de calamiteitenoefening zich richt op het testen van organisatorische maatregelen in het kader van een succesvolle aanval, is geen behoefte aan een virtueel of beveiligd digitaal netwerk met echte tools en technieken.

Organisatorische kennis, expertise op het gebied van informatiebeveiliging, communicatieve vaardigheden en een objectief vermogen om te evalueren, evenals de nodige creativiteit, zijn echter vereist om scenario's te ontwikkelen die realistisch zijn en tegelijkertijd passen bij het doel van de oefening.

Welke beschermingsdoelen worden door de maatregel afgedekt?

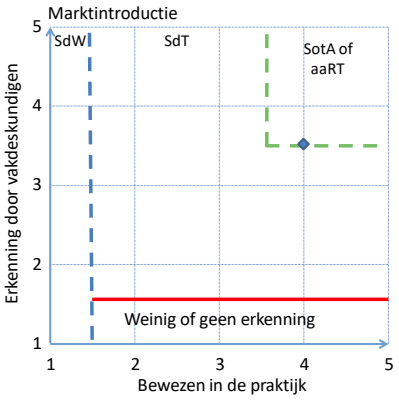
☒ Beschikbaarheid

☐ Integriteit

☐ Vertrouwelijkheid

Kwalificatie van de maatregel

Afb 3



3.3.20 Technische veiligheidsbeoordeling

Op verschillende plaatsen in de hand-out worden audits genoemd, bijvoorbeeld bij de audit van Information Security Management Systems zoals ISO 27001 en BSI baseline protection. Het overgrote deel van de auditformulieren zijn procesaudits en worden verstrekt op basis van bewijsmateriaal in de vorm van documentatie. Het is echter een goed idee om audits aan te vullen met technische veiligheidscontroles. Hoewel audits correcte en zinvolle processen aantonen, leveren technische veiligheidsbeoordelingen die ervan zijn afgeleid bewijs van hun werkelijke effectiviteit. Immers, zelfs met een perfect gedocumenteerde firewall en een gevestigd veranderingsproces kunnen ernstige beveiligingslekken worden verborgen.

De hier gepresenteerde technische veiligheidscontroles zijn eenmalige tests die worden uitgevoerd in het kader van audits. Doorlopende technische maatregelen die als een continu proces in de organisatie kunnen worden vastgesteld, zoals permanente kwetsbaarheidscans, zijn niet het onderwerp van dit artikel.

Afhankelijk van de omgeving zijn er verschillende mogelijke testmethoden. De volgende opties zijn daarom niet uitputtend en moeten worden gekozen door auditors met de juiste technische domeinkennis. De implementatie moet altijd worden uitgevoerd door ervaren experts die dagelijks technische veiligheidscontroles uitvoeren.

Configuratieanalyses

Configuratieanalyses vergelijken idealiter de bestaande beveiligingsconcepten met gevestigd configuratie- en wijzigingsbeheer. In de regel gaat het om steekproefsgewijze inspecties. Als gevolg hiervan moeten verschillen tussen specificaties en technische implementatie aan het licht komen. De volgende voorbeeldvragen kunnen als leidraad dienen:

Bereik	Vraag
Active Directory	Is het wachtwoordbeleid correct geconfigureerd?
Back-up configuratie	Zijn back-uptaken ingesteld volgens de documentatie en worden ze aangepast volgens het wijzigingsbeheer?
Klantenbeheer	Worden alle clients vanuit patchbeheer beheerd en zijn ze up-to-date?
Cloud configuraties	Worden IAM-rollen en –autorisaties, in overeenstemming met de beveiligingsconcepten geïmplementeerd voor clouddiensten (bijv. AWS, IAM en Microsoft Azure RBAC)?
Beheer van databases	Zijn gebruikersaccounts in productie-databases correct gedocumenteerd en op rollen met minimaal noodzakelijke rechten gebaseerd?
Printers en multifunctionele apparaten	Zijn toegangsbeperkingen ingeschakeld en is de toegang tot het netwerk beperkt tot wat nodig is?
E-mail gateways	Zijn filter- en beschermingsmechanismen (zoals SPF, DKIM, DMARC) actief en correct geconfigureerd?

Bereik	Vraag
Firewall-gebruikers	Zijn alle gebruikers gedocumenteerd? De verificatie van de individuele gebruikersaccounts en de veilige bewaring van het "Admin"-wachtwoord wordt afzonderlijk uitgevoerd in het proces Review.
Firewall regels	Zijn de firewall regels duidelijk toe te wijzen aan de documentatie en de wijzigingsverzoeken?
Beheer van mobiele apparaten	Worden mobiele apparaten (zoals smartphones en tablets) geregistreerd, beheerd en versleuteld?
Controlesystemen	Zijn back-uptaken ingesteld volgens de documentatie en worden ze aangepast volgens het wijzigingsbeheer?
Controlesystemen	Zijn alle kritische systemen correct geïntegreerd in de bewaking en worden alarmen geactiveerd volgens gedefinieerde drempels?
Configuratie	Voldoen diensten, protocollen en havens aan de goedgekeurde en gedocumenteerde specificaties?
VPN-toegang	Is overal waar mogelijk twee-factor authenticatie geactiveerd?
Webserver	Voldoen SSL/TLS-configuraties aan gedocumenteerde minimumvereisten. Zijn verouderde protocollen, zoals TLS 1.0, uitgeschakeld?
Wi-Fi-configuratie	Worden zakelijke wifi-netwerken beschermd door WPA2-Enterprise of hoger en zijn gastnetwerken voldoende gesegmenteerd?

Tabel 6: Voorbeeldvragen in configuratieanalyses

Hardening controles[45]

Als onderdeel van hardening controles wordt de implementatie van minimale technische normen voor systemen en applicaties geëvalueerd. Het doel is om na te gaan of vastgestelde hardening specificaties (zoals CIS-benchmarks en eigen interne standaarden) consistent zijn geïmplementeerd. Verschillen tussen de configuratiespecificaties en gangbare werkwijzen worden geïdentificeerd. Voorbeeldvragen zijn:

Bereik	Vraag
Applicatie hardenen	Zijn de standaardwachtwoorden verwijderd en zijn veilige configuratieopties gekozen?
Back-up systemen	Zijn back-up servers en -opslag speciaal gehard, bijvoorbeeld door beperkende netwerktoegang en afzonderlijke authenticatie?
Hardenen van de klant	Is de toegang tot beheerfuncties beperkt voor gebruikers? Zijn de toegestane applicaties (white-listing) beschikbaar en correct geconfigureerd?
Container hardenen	Zijn containerimages afkomstig van betrouwbare bronnen en worden ze regelmatig bijgewerkt? Worden onnodige diensten in de containers uitgeschakeld?
Mobiele apparaten	Is lokale opslagversleuteling actief? Is er beleid voor apparaatbeheer (zoals wissen op afstand)?
Systeem hardenen	Worden onnodige/niet gebruikte services gedeactiveerd en worden er veilige configuraties ingesteld?
Virtualisatie platformen	Is de toegang tot hypervisorbeheersystemen (zoals vCenter) beschermd en beperkt tot geautoriseerde personen?

Tabel 7: Voorbeeldvragen bij hardening controles

Geautomatiseerde scans van kwetsbaarheden

Geautomatiseerde kwetsbaarheidscans registreren systematisch bekende kwetsbaarheden in de technische infrastructuur. Ze moeten op een gerichte manier worden gebruikt om een overzicht te krijgen van de huidige kwetsbaarheidstatus. Voorbeelden:

[45] Zie ook hoofdstuk "Systeem hardening"

- **Back-upinfrastructuren**: Controleer op kwetsbare en verouderde back-upsoftware en op misconfiguraties die ongeoorloofde toegang mogelijk kunnen maken.
- **Cloud-infrastructuren**: Controleer op verkeerd geconfigureerde opslaggebieden (zoals open S3-buckets), verouderde afbeeldingen en onveilige toegangscontroles.
- **Containeromgevingen**: Controleer op kwetsbaarheden in containerimages en verouderde basisimages die het gevolg kunnen zijn van bekende beveiligingslekken.
- **E-mailsystemen**: Controleer op ontbrekende beveiligingen zoals ontbrekende SPF, DKIM en DMARC, evenals bekende kwetsbaarheden in gebruikte mailservers.
- **Netwerkapparaten**: Controleer op verouderde firmware versies en onveilige standaardconfiguraties.
- **Servers en clients:** Controleer op ontbrekende patches, onveilige configuraties en bekende exploits.

Geautomatiseerde kwetsbaarheidscans zijn zeer geschikt voor standaardcomponenten, ze kunnen echter slechts in zeer beperkte mate kwetsbaarheden (in webapplicaties) detecteren, omdat deze vaak individueel (individuele software) zijn ontwikkeld.

Penetratie testen

Een alomvattende penetratietest bestaat niet, omdat penetratietests bedoeld zijn om een echte aanvaller te simuleren. De penetratietesten zijn dan ook individuele testen die met name bruikbaar zijn voor het testen van bedrijfskritische (web)applicaties.

Penetratietests tonen de weerbaarheid van systemen en applicaties tegen gerichte aanvallen. Meer gedetailleerde informatie over penetratietests wordt beschreven in de hand-out "Penetration Tests" van TeleTrusT. De release hiervan is gepland voor 2025.

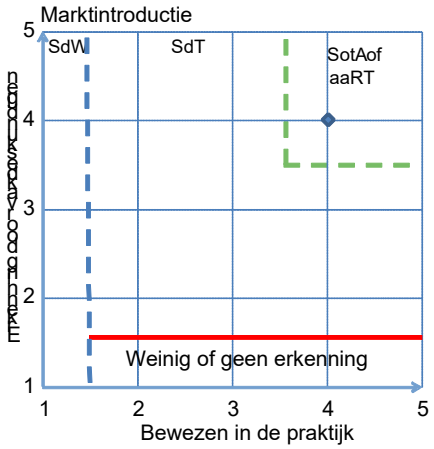
Welke beschermingsdoelen worden door de maatregel afgedekt?

☒ Beschikbaarheid

☐ Integriteit

☐ Vertrouwelijkheid

Kwalificatie van de maatregel



4 Toelichtingen

Hoewel de hierboven beschreven maatregelen zich richten op de wettelijke vereisten in verband met informatiebeveiliging, blijven de meeste ervan slechts een grijze theorie, omdat ze opzettelijk zijn gescheiden van de bedrijfspraktijk om de technologie uit te leggen en op technologieniveau te classificeren volgens de aanvankelijk toegelichte evaluatiecriteria.

In dit hoofdstuk wordt het verband gelegd tussen de hierboven beschreven beveiligingsmaatregelen en de veranderende veiligheidssituatie op de markt. Op deze manier moet de praktische relevantie worden uitgewerkt en moet de toepasbaarheid van de maatregelen dichter bij de lezer worden gebracht,

4.1 Maatregelen tegen ransomware aanvallen

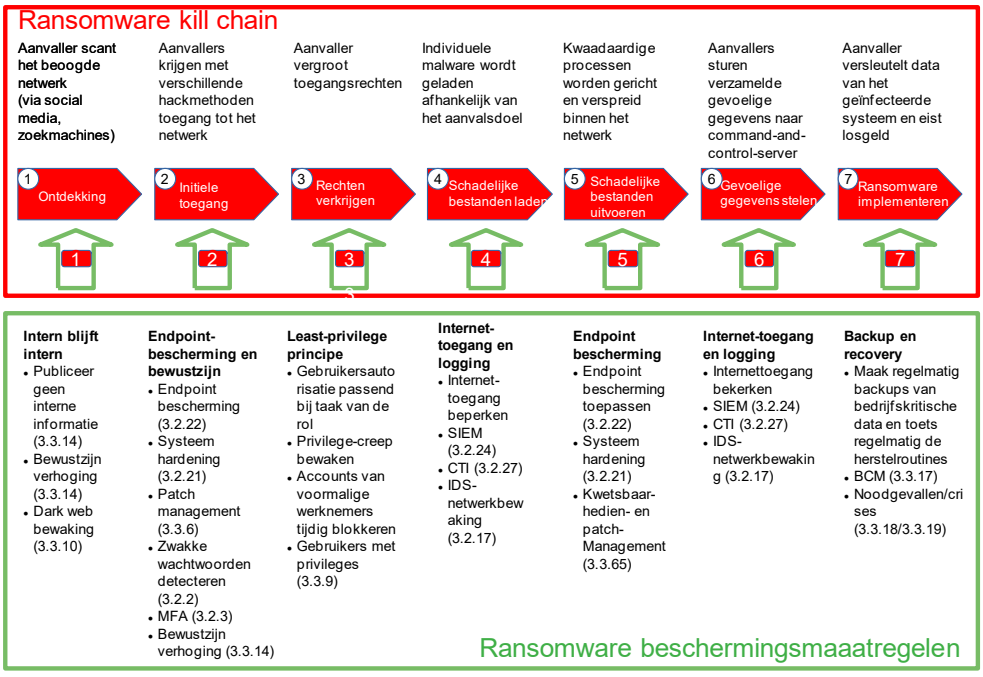
Ransomware beschrijft het een type aanval dat de toegang tot persoonlijke en bedrijfsgegevens blokkeert (meestal door middel van versleuteling) en losgeld eist om die gegevens vrij te geven. In de meeste gevallen is reconstructie van de originele gegevens, zonder het losgeld te betalen, niet mogelijk. Vaak wordt een ransomware aanval geassocieerd met de dreiging om gevoelige en geheime gegevens van het slachtoffer van de aanval te publiceren om de losgeldeis te onderbouwen. Andere brede termen voor ransomware zijn 'afpersing/crypto trojans' en '*afpersingssoftware*'.

De dreiging van ransomware is de afgelopen jaren gestaag toegenomen en is een van de grootste bedreigingen voor zowel particulieren als bedrijven.

In het openbaar wordt vaak gesproken over een ransomware aanval. De procedure van een dergelijke aanval is echter complexer en begint veel eerder dan op het eerste gezicht lijkt. Elke ransomware aanval verschilt in afzonderlijke stappen, maar de algemene aanpak is vergelijkbaar.

Om de complexiteit van een ransomware aanval tegen te gaan, is het gebruik van slechts één maatregel (zoals antivirussoftware en proxyfilters) onvoldoende. Er moeten meerdere maatregelen tegelijk worden uitgevoerd en dus moeten verschillende verdedigingslinies worden opgezet. Voorbeelden van dergelijke activiteiten zijn de detectie van gecompromitteerde accounts en zwakke wachtwoorden, het gebruik van MFA, inbraak detectiesystemen, enz.

In de volgende afbeelding tonen we als voorbeeld de afzonderlijke stappen en de bijbehorende beschermingsmaatregelen die, afhankelijk van de betreffende stap, moeten worden gebruikt,\:



Afbeelding 7: Ransomware kill-chain en beschermende maatregelen (voorbeeld)

De mogelijke stappen en beschermingsmaatregelen worden kort toegelicht in de volgende tabel:

Ransomware kill-chain (voorbeeld)	Ransomware Beveiligingsmaatregelen
1) **Ontdekking** Aanvallers verzamelen zoveel mogelijk informatie over de organisatie dat wordt aangevallen, bijvoorbeeld in openbare zoekmachines (Shodan, Censys) en sociale netwerken.	**1+) Intern blijft intern** Geen informatie te publiceren die alleen bedoeld is voor interne doeleinden (netwerkkaarten, IP-adressen, organogrammen, contactgegevens, enz.). Als mogelijke aanpak kan een classificatie van documenten en gegevens (openbaar, intern, geheim) worden gemaakt. Medewerkers moeten hier ook in getraind worden (3.3.14 HR SdT).
2) **Initiële toegang** Aanvaller krijgt toegang tot het netwerk met behulp van verschillende hacker methoden. Een eerste infectie vindt vaak plaats via phishing e-mailberichtent en kwaadaardige websites. Op dit moment is de daadwerkelijke kwaadaardige code nog niet geladen.	**2+) Endpoint Bescherming & Awareness** Implementeer maatregelen voor eindpuntbeveiliging (3.2.22 HR SdT). Sensibiliseer medewerkers door middel van regelmatige bewustmakingstrainingen (3.3.14 HR SdT). Schakel de uitvoering van macro's uit en beperk deze tot alleen ondertekende macro's. Gebruik maatregelen om gecompromitteerde accounts en zwakke wachtwoorden te detecteren (3.2.2 HR SdT). Gebruik indien mogelijk MFA (3.2.3 HR SdT). Maar ook andere maatregelen, zoals server hardening (3.2.21 HR SdT) en vulnerability en patch management (3.3.6 HR SdT)
3) **Rechten verkrijgen** Aanvaller vergroot de rechten waarmee ze handelen om verdergaande acties te bereiken en dus een hoger schadepotentieel.	**3+) Principe van de minste privileges (PoLP)** Zorg ervoor dat gebruikers alleen de toegangsrechten krijgen die ze nodig hebben om hun taken uit te voeren. Controleer het privilegemodel regelmatig op privilege-creep. Stem maatregelen af op de "gebruikersaccount cyclus" en blokkeer accounts van voormalige werknemers op korte termijn. Bescherm accounts met speciale rechten met MFA (3.2.3 HR SdT / 3.3.9 HR SdT).
4) **Schadelijke** bestanden laden De "dropper" laadt nu de eigenlijke kwaadaardige code ("payload"). Deze payload wordt vaak individueel geprogrammeerd en wordt niet gedetecteerd door antivirussoftware.	**4+) Internettoegang en logfile registratie** Sta internettoegang toe tot gedeelde sites, blokkeer anderen. Afhankelijk van de nood aan bescherming kan het gebruik van ReCoBS (3.2.23HR SdT) nuttig zijn. Verdere technische maatregelen zoals SIEM (3.2.24 HR SdT) en CTI (3.2.27 HR SdT) en netwerkbewaking met behulp van IDS (3.2.17 HR SdT) kunnen logging en monitoring ondersteunen.
5) **Schadelijke bestanden uitvoeren** Verdere kwaadaardige code wordt gedownload, de aanvallers verspreiden zich via het netwerk (lateral movement)	**5+) Bescherming van eindpunten** Pas maatregelen toe voor endpoint bescherming (3.2.22 HR SdT). Implementeer andere maatregelen, zoals systeem hardening (3.2.21 HR SdT) en kwetsbaarheden- en patchbeheer (3.3.6 HR SdT).
6) **Gevoelige gegevens stelen** Gevoelige gegevens, zoals toegangsgegevens, worden naar het commandocentrum van de aanvallers gestuurd (command-and-control server).	**6+) Internettoegang en logfile registratie** Sta internettoegang toe tot gedeelde sites, blokkeer anderen. Afhankelijk van de nood aan bescherming kan het gebruik van ReCoBS (3.2.23 HR SdT) nuttig zijn. Andere technische maatregelen zoals SIEM (3.2.24 HR SdT) en CTI (3.2.27 HR SdT) en netwerkmonitoring met behulp van IDS (3.2.17 HR SdT) kunnen logging en monitoring ondersteunen.
7) **Ransomware implementeren** De daadwerkelijke kwaadaardige code die wordt gebruikt om de gegevens te versleutelen, wordt uitgevoerd.	**7+) Back-up en herstel** In het geval van een succesvolle aanval moeten natuurlijk eerst veel maatregelen worden genomen om de infectievector te vinden en te sluiten en de schade te beperken. Om de systemen opnieuw op te bouwen en de gegevens op een later tijdstip te herstellen, zijn up-to-date, niet-geïnfecteerde back-ups vereist. Verdere aanvullende maatregelen vloeien voort uit de BCM (3.3.17 HR SdT) en de voorbereidingen voor een noodsituatie (3.3.18 en 3.3.19 HR SdT)

Tabel 8: Maatregelen tegen ransomware aanvallen

4.2 Classificatie van maatregelen in ISO/IEC 27001:2022

De ISO/IEC 27001:2022-norm is een internationaal erkend kader voor het Information Security management System (ISMS). Het ondersteunt organisaties van elke omvang en branche bij het systematisch identificeren, beoordelen en aanpakken van hun informatiebeveiligingsrisico's. De standaard is gebaseerd op een risicogebaseerde aanpak en omvat zes belangrijke functies:

1. Context van de organisatie: De organisatie moet interne en externe beïnvloedende factoren identificeren die van invloed zijn op het ISMS. Dit omvat wettelijke vereisten, bedrijfsdoelen en verwachtingen van belanghebbenden.
2. Leiderschap: Het topmanagement is verantwoordelijk voor de informatiebeveiliging. Het moet een duidelijke beveiligingsstrategie definiëren, middelen toewijzen en ervoor zorgen dat beveiligingsdoelen aansluiten bij de bedrijfsstrategie.
3. Planning: Organisaties moeten beveiligingsrisico's beoordelen en passende maatregelen voor risicobeheer definiëren. Dit omvat ook de definitie van veiligheidsdoelstellingen en de voortdurende herziening daarvan.
4. Ondersteuning: Er moet worden gezorgd voor de nodige middelen, competenties en communicatiemaatregelen om het ISMS effectief te laten functioneren en in stand te houden.
5. Werking: Beveiligingsmaatregelen moeten worden geïmplementeerd en beheerd. Dit omvat ook het beheer van incidenten en de continue monitoring van de veiligheidssituatie.
6. Prestatie-evaluatie en -verbetering: Regelmatige evaluaties door middel van interne audits en managementbeoordelingen zijn vereist om de effectiviteit van het ISMS te waarborgen en deze voortdurend te verbeteren.

Naast deze kernaspecten benadrukt ISO/IEC 27001:2022 het belang van een continu verbeterproces. Dit zorgt ervoor dat organisaties kunnen inspelen op veranderende bedreigingen en zakelijke behoeften.

Een essentieel onderdeel van ISO/IEC 27001:2022 is Bijlage A, die een gestructureerde lijst van beveiligingsmaatregelen (controles) bevat. Deze maatregelen hangen nauw samen met de ISO/IEC 27002:2022, die gedetailleerde informatie geeft over de uitvoering van deze controles. De controles zijn onderverdeeld in vier hoofdthema's: organisatorische, persoonlijke, fysieke en technologische maatregelen en hebben betrekking op belangrijke beveiligingsaspecten zoals toegangscontroles, encryptie, incidentbeheer en beveiliging van de toeleveringsketen. Bedrijven gebruiken deze bijlage als referentie om beveiligingsmaatregelen te selecteren en aan te passen aan hun specifieke risico's.

Een belangrijk voordeel van ISO/IEC 27001:2022 is de mogelijkheid tot certificering. Organisaties kunnen hun informatiebeveiligingbeheersysteem laten controleren door een onafhankelijke certificeringsinstantie om aan te tonen dat ze aan de norm voldoen. De certificering dient als een internationaal erkend keurmerk en geeft klanten, partners en regelgevers het signaal dat de organisatie systematische en effectieve maatregelen heeft genomen om informatie te beschermen. Dit kan niet alleen het vertrouwen in IT-beveiliging vergroten, maar ook concurrentievoordeel creëren door bedrijven te helpen voldoen aan wettelijke vereisten en nieuwe zakelijke kansen te ontsluiten.

Hoofdstuk naam	Hoofdstuk #	ISO/IEC 27001:2022 toewijzing				
		4-10	A.5	A.6	A.7	A.8
Authenticatie	3.2.1		A.5.15 A.5.16 A.5.17 A.5.18			
Sterke wachtwoorden beoordelen en afdwingen	3.2.2		A.5.17			
Multi-factor authenticatie	3.2.3		A.5.17			
Cryptografische methoden	3.2.4					A.8.24
Versleuteling van harde schijven	3.2.5					A.8.1 A.8.24
Versleuteling van bestanden en mappen	3.2.6					A.8.24
Versleuteling van e-mailberichtent	3.2.7					A.8.24
Elektronisch verkeer beveiligen met PKI	3.2.8					A.8.24 A.8.27
Gebruik van versleutelde VPN-oplossingen (Layer 3)	3.2.9					A.8.21 A.8.24
Versleuteling (Layer 2)	3.2.10					A.8.21 A.8.24
Veilige cloudgebaseerde gegevensuitwisselingsservices	3.2.11		A.5.23			
Gegevensopslag in de cloud	3.2.12		A.5.23			
Mobiele spraak- en gegevensbescherming	3.2.13					A.8.21 A.8.24
Bescherming van communicatie via instant messenger	3.2.14					A.8.21 A.8.24
Bescherming van mobiele apparaten	3.2.15					A.8.1
Router beveiliging	3.2.16					A.8.8 A.8.9
Netwerkbewaking met behulp van een inbraakdetectiesysteem	3.2.17					A.8.7 A.8.15
Beveiliging van webverkeer	3.2.18					A.8.21 A.8.23
Bescherming van webapplicaties	3.2.19					A.8.23
Bescherming van externe toegang tot netwerken	3.2.20			A.6.7		A.8.20 A.8.22
Systeem hardening	3.2.21					A.8.9
Endpoint Detection & Response Platform	3.2.22		A.5.24 A.5.25 A.5.26			
Webisolatie van internetgebruik	3.2.23					A.8.22
Inbraakdetectie en -evaluatie (SIEM)	3.2.24		A.5.24 A.5.25 A.5.26			
Vertrouwelijke gegevensverwerking	3.2.25		A.5.12 A.5.23			A.8.2 A.8.5
Sandboxing voor analyse van kwaadaardige code	3.2.26		A.5.28			
Informatie over cyberdreigingen	3.2.27		A.5.7			
Beveiligen van IT-beheersystemen	3.2.28					A.8.2
Monitoring van directoryservices en segmentatie op basis van identiteit	3.2.29		A.5.18			A.8.15

Hoofdstuk naam	Hoofdstuk #	ISO/IEC 27001:2022 toewijzing				
Segmentatie en scheiding van netwerken	3.2.30					A.8.22
Platform voor cloudbeveiliging	3.2.31		A.5.23			
Tokenisatie	3.2.32					A.8.11
VOIP-versleuteling met SIPS/SRTP	3.2.33					A.8.21 A.8.24
Versleuteling op Layer 1	3.2.34					A.8.24
Normen en standaarden	3.3.1					
Security organisatie	3.3.2	5.3				
Information Security Management System (ISMS)	3.3.3	4 - 10				
Secure Software Design	3.3.4					A.8.25 A.8.26 A.8.27 A.8.28 A.8.29 A.8.30 A.8.31
Proces Certificering	3.3.5					
Beheer van kwetsbaarheden en patches	3.3.6					A.8.8
Risk Management	3.3.7	6, 8				
Persoonlijke certificering	3.3.8	7.2	A.6.3			
Bevoegde gebruikersaccounts beveiligen	3.3.9					A.8.2
Dark-web bewaking	3.3.10		A.5.7			
Omgaan met dienstverleners	3.3.11		A.5.19 A.5.20 A.5.21 A.5.22			
Software stuklijst (SBOM)	3.3.12		A.5.9 A.5.21			A.8.8
Geo-redundantie	3.3.13					A.8.14
Bewustmaking van de gebruiker	3.3.14	7.3	A.6.3			
IT-Asset Management	3.3.15		A.5.9 A.5.10 A.5.12			
Incident Management	3.3.16		A.5.24 A.5.25 A.5.26			
Business Continuity Management (BCM)	3.3.17		A.5.29 A.5.30			
Nood- en crisisbeheersing	3.3.18		A.5.30			
Noodoefeningen	3.3.19		A.5.29 A.5.30			
Technische systeemaudits	3.3.20					A.8.8

Tabel 9: Classificatie van maatregelen in ISO/IEC 27001:2022

4.3 Classificatie van de maatregelen in het NIST-kader

Het NIST Cybersecurity Framework is in de VS ontwikkeld om organisaties in alle sectoren te helpen om hun informatie- en cyberbeveiligingsrisico's te beheren. Het biedt een flexibele en herhaalbare aanpak op basis van bestaande normen en richtlijnen en omvat vijf basisfuncties:

1. Identificeren:
   Begrijp en definieer de organisatorische context, systemen, activa, gegevens en capaciteiten die moeten worden beschermd.
   Beheer activa die aansluiten bij het belang van de organisatie.
2. Beschermen:
   Stel de juiste beschermende maatregelen vast om ervoor te zorgen dat kritieke services, zelfs in het geval van een incident, worden gehandhaafd.
3. Detecteren:
   Ontwikkel en implementeer de nodige maatregelen voor de vroege opsporing van cyberbeveiligingsincidenten
4. Reageren:
   Definieer acties en plannen om effectief te reageren op gedetecteerde cyberbeveiligingsincidenten.
5. Herstellen:
   Maak een planning voor herstel van een cyberbeveiligingsincident en maatregelen om de normale bedrijfsvoering te herstellen.

Naast de vijf eerder genoemde functies wordt "Governance" beschouwd als een aanvullend onderdeel van het NIST Cybersecurity Framework. De governance-functie speelt een centrale rol in het algehele cyberbeveiligingsproces en wordt weerspiegeld in verschillende aspecten van het framework.

6. Governance (Besturing):
   De strategie, verwachtingen en richtlijnen van de organisatie voor risicobeheer op het gebied van cyberbeveiliging worden bepaald, gecommuniceerd en gecontroleerd.

Veel bedrijven gebruiken het NIST Framework als referentie om hun eigen beveiligingsmaatregelen te verifiëren en te optimaliseren. Het kader bevordert ook de communicatie over cyberveiligheidsrisico's tussen interne en externe belanghebbenden door het gebruik van gemeenschappelijke taal. Het is ontworpen om van toepassing te zijn op organisaties met een lage volwassenheid op het gebied van cyberbeveiliging en op organisaties met geavanceerde programma's.

Deze hand-out neemt een intermediaire rol op zich om de beveiligingsmaatregelen en hun kenmerken op een begrijpelijke manier uit te leggen aan de applicatiebedrijven. Daartoe is het nuttig om de beschreven maatregelen in relatie tot de huidige kaders vast te stellen.

Hoofdstuk naam	**Hoofdstuk**	**NIST toewijzing**					
		Govern	Identify	Protect	Detect	Respond	Recover
Technische maatregelen	3.2						
Authenticatie	3.2.1		X	X			
Beoordelen en afdwingen van sterke wachtwoorden	3.2.2	X		X			
Multi-factor authenticatie	3.2.3			X			
Cryptografische methoden	3.2.4			X			
Versleuteling van harde schijven	3.2.5			X			
Versleuteling van bestanden en mappen	3.2.6			X			
Versleuteling van e-mailberichtent	3.2.7			X			
Met PKI beveiligen van elektronisch dataverkeer	3.2.8			X			
Gebruik van versleutelde VPN-oplossingen (Layer 3)	3.2.9			X			
Versleuteling (Layer 2)	3.2.10			X			
Gegevensuitwisseling in de cloud	3.2.11			X			
Gegevensopslag in de cloud	3.2.12			X			
Mobiele spraak- en gegevensbescherming	3.2.13			X			
Beveiliging van communicatie via Instant Messenger	3.2.14	X		X		X	

Hoofdstuk naam	Hoofdstuk	NIST toewijzing					
		Govern	Identify	Protect	Detect	Respond	Recover
Bescherming van mobiele apparaten	3.2.15	X		X			
Router beveiliging	3.2.16			X			
Netwerkbewaking met behulp van een inbraakdetectiesysteem	3.2.17				X		
Beveiliging van webverkeer	3.2.18			X			
Bescherming van webapplicaties	3.2.19			X			
Bescherming van externe toegang tot netwerken	3.2.20			X			
Systeem hardening	3.2.21			X			
Platform voor detectie en respons van eindpunten	3.2.22				X	X	X
Webisolatie van internetgebruik	3.2.23			X			
Inbraakdetectie en -evaluatie (SIEM)	3.2.24				X	X	X
Vertrouwelijke gegevensverwerking	3.2.25	X		X			
Sandboxing voor analyse van kwaadaardige code	3.2.26				X		
Informatie over cyberdreigingen	3.2.27				X		
Beveiligen van IT-beheersystemen	3.2.28			X			
Monitoring van directoryservices en segmentatie op basis van identiteit	3.2.29		X		X		
Segmentatie en scheiding van netwerken	3.2.30			X			
Platform voor cloudbeveiliging	3.2.31			X			
Tokenisatie	3.2.32			X			
VOIP-versleuteling met SIPS/SRTP	3.2.33			X			
Versleuteling (Layer 1)	3.2.34			X			
Organisatorische maatregelen	**3.3**						
Normen en standaarden	3.3.1	X					
Veiligheidsorganisatie	3.3.2	X					
Information Security Management System (ISMS)	3.3.3			X			
Secure Software Design	3.3.4			X			
Proces Certificering	3.3.5	X		X			
Beheer van kwetsbaarheden en patches	3.3.6		X	X			
Risk Management	3.3.7	X		X			
Persoonlijke certificering	3.3.8	X		X			
Bevoegde gebruikersaccounts beveiligen	3.3.9		X	X			
Dark-web bewaking	3.3.10				X	X	
Omgaan met dienstverleners	3.3.11	X			X		
Software stuklijst (SBOM)	3.3.12		X	X			
Geo-redundantie	3.3.13			X			
Bewustmaking van de gebruiker	3.3.14	X					
IT Asset Management	3.3.15		X				
Incident Management	3.3.16				X	X	X
Business Continuity Management (BCM)	3.3.17					X	X
Nood- en crisisbeheersing	3.3.18				X	X	X
Noodoefeningen	3.3.19				X	X	X
Technische Systeemaudits	3.3.20	X	X	X			

Tabel 10: Classificatie van de maatregelen in het NIST-kader

4.4 Impact van AI op informatiebeveiliging

De term kunstmatige intelligentie omvat verschillende gebieden. Machine learning (ML), Deep Learning (DL) en Generatieve AI (GenAI) zijn van groter belang in de context van IT-beveiliging. Deep learning is een subset van machine learning (met meerlaagse neurale netwerken), terwijl generatieve AI een speciale vorm van deep learning is.

Wat deze drie AI-gebieden gemeen hebben, is dat alle AI-modellen na het trainingsproces zelfstandig data patronen kunnen herkennen binnen grote hoeveelheden. Hoewel de machine learning- en deep learning-modellen de neiging hebben om deze hoeveelheden gegevens te classificeren en te categoriseren, genereren generatieve AI-modellen op basis van de gevonden patronen en statistische aannames nieuwe inhoud.

De toenemende integratie van kunstmatige intelligentie (AI) in bedrijfsprocessen verandert het landschap van informatiebeveiliging en brengt zowel positieve kansen als aanzienlijke beveiligingsrisico's met zich mee. Aan de ene kant kan AI patronen en anomalieën detecteren die wijzen op potentiële bedreigingen. Aan de andere kant kan dezelfde technologie door aanvallers worden gebruikt om informatie over potentiële slachtoffers te vinden, gepersonaliseerde aanvallen uit te voeren en malware te ontwikkelen. Ook zijn aanvallen op AI-toepassingen zelf mogelijk, bijvoorbeeld om actief hun gedrag te beïnvloeden.

AI om informatiebeveiliging te verbeteren

Een van de belangrijkste voordelen van AI is de mogelijkheid om binnen grote hoeveelheden gegevens afwijkingen en ongebruikelijke activiteiten te identificeren. In tegenstelling tot traditionele beveiligingstechnologieën, waarbij detectie meestal gebaseerd is op overeenkomende patronen en signatuur van eerdere aanvallen, is AI in staat om voorheen onbekende bedreigingen te detecteren.

AI maakt het ook mogelijk om binnen een redelijke tijd gegevens uit veel verschillende gegevensbronnen te verwerken en te correleren. AI- en big data-algoritmen leggen verbanden bloot die vaak onopgemerkt zouden zijn gebleven door een menselijke waarnemer.

Een ander voordeel voor organisaties is de toename van efficiëntie die kan worden bereikt door AI te gebruiken in beveiligingstechnologieën. AI-systemen besparen human resources door beveiligingsanalisten in staat te stellen zich te concentreren op relevante activiteiten die als ongebruikelijk zijn gedetecteerd. Bovendien kunnen potentiële bedreigingen meestal sneller worden gedetecteerd, wat de reactietijd op beveiligingsincidenten aanzienlijk kan verkorten.

AI als hulpmiddel voor aanvallers

Aanvallergroepen maken ook gebruik van de mogelijkheden van AI en gebruiken deze specifiek voor hun eigen doeleinden, dat varieert van social-engineering aanvallen tot geautomatiseerde malware-ontwikkeling. Een grote kracht van AI ligt in het efficiënt verwerken en analyseren van openbaar beschikbare informatie. Aanvallers gebruiken deze functionaliteit om gegevens over potentiële slachtoffers te verzamelen en samen te voegen. De verzamelde informatie vormt vervolgens de basis voor ‘aanvallen op maat’. Zo kunnen bijvoorbeeld gepersonaliseerde phishing e-mailberichtent worden gemaakt die zijn afgestemd op de betreffende doelgroep. Terwijl traditionele phishing-berichten vaak schitteren door spelfouten of slechte vertalingen, zijn door AI gegenereerde berichten vaak bijna niet van legitieme te onderscheiden, tegelijkertijd kan het verzenden van phishing-berichten in hoge mate worden geautomatiseerd, wat de slagingspercentages van aanvallers aanzienlijk verhoogt.

Bovendien kan AI de toetredingsdrempel bij het maken van malware voor aanvallers aanzienlijk verlagen. Malware kan worden gegenereerd met behulp van AI-modellen die speciaal voor dit doel zijn getraind.

AI-systemen kunnen zelf ook het doelwit worden van aanvallen, zowel tijdens de trainingsfase als tijdens het gebruik. Bij modelinversie proberen aanvallers met behulp van de output van AI de onderliggende architectuur af te leiden en verdere informatie te extraheren. De diefstal van een getraind AI-model kan ook verstrekkende gevolgen hebben voor een organisatie. De OWASP Foundation houdt een lijst bij van AI-gerelateerde risico's, inclusief risicofactoren en tegenmaatregelen[46].

[46] owasp.org/www-project-machine-learning-security-top-10/

Beschermende maatregelen tegen AI-gerelateerde risico's

Aangezien AI in verschillende vormen zijn weg vindt naar bijna alle organisaties, zijn passende beschermingsmaatregelen nodig om u te beschermen tegen AI-gerelateerde risico's. Vanuit securityperspectief hebben machine learning, deep learning en generatieve AI verschillende effecten. Terwijl de eerste twee hun output rechtstreeks ontlenen aan machineleesbare datasets (inputs), genereert generatieve AI vaak interactief output als reactie op menselijke input. Deze directe gebruikersinteractie in combinatie met een hoge mate van marktdynamiek en enkele AI-eigenaardigheden openen nieuwe aanvalsoppervlakken, vooral op het gebied van generatieve AI. Daarentegen liggen de risico's bij machine learning en deep learning meer op het gebied van AI-modelbeveiliging en het opzetten van een veilige ontwikkel- en testomgeving.

Nog voor het ontwikkelen en implementeren van AI-toepassingen moeten de toepasselijke wettelijke vereisten in kaart worden gebracht. Als producten en diensten worden aangeboden op basis van AI, is de EU AI Act, die regels bevat voor het gebruik van AI, van toepassing. Ook de bepalingen van de GDPR moeten worden nageleefd. Bij het gebruik van AI-toepassingen moet bijvoorbeeld, om te voorkomen dat persoonsgegevens en gevoelige gegevens zonder toestemming worden doorgegeven, worden nagegaan of de ingevoerde gegevens worden doorgegeven aan de fabrikant van de AI-toepassing of aan andere derden.

De onderstaande tabel geeft een overzicht van de momenteel bekende beveiligingsrisico's van AI-modellen en passende preventieve maatregelen. Op beveiliging gerichte organisaties, zoals OWASP, houden deze ruimte voortdurend in de gaten. OWASP biedt niet alleen jaarlijkse lijsten van de tien meest voorkomende aanvalsmethoden[47] tegen generatieve AI-modellen en checklists voor AI-beveiliging[48], ook somt de organisatie concrete maatregelen[49] op om te komen tot een veilig en risicovrij gebruik van AI binnen organisaties. Daarbij wordt een onderscheid gemaakt tussen:

- Algemene veiligheidscontroles
  - Integratie van AI in de eigen beveiligingsprogramma's van de organisatie
  - Maatregelen voor gegevenscontrole en gegevensbeveiliging
  - Maatregelen om ongewenst gedrag van AI te beteugelen

- Maatregelen bij het gebruik van AI
  - Algemene monitoring van het gebruik
  - Maatregelen tegen Evasion aanvallen
  - Maatregelen tegen Prompt injectie
  - Maatregelen tegen het verlies van gevoelige trainingsgegevens
  - Maatregelen tegen diefstal van AI-modellen
  - Maatregelen tegen wangedrag van AI-modellen

- Maatregelen tegen dreigingen tijdens de ontwikkeling
  - Algemene borging van de ontwikkelingsomgeving en toeleveringsketens
  - Maatregelen tegen Model Poisoning
  - Maatregelen tegen datalekken

- Maatregelen tegen bedreigingen tijdens modelruntime
  - Bescherming tegen klassieke veiligheidsrisico's
  - Maatregelen tegen modelmanipulatie tijdens runtime
  - Maatregelen tegen modeldiefstal tijdens runtime
  - Zelfverzekerde omgang met onveilige modeluitgangen
  - Maatregelen tegen de invoer van gevoelige gegevens

Niet alle bedreigingscenario's zijn AI-specifiek. AI-toepassingen zijn vaak ook klassieke SaaS-toepassingen en zijn onderhevig aan de bijbehorende veiligheidsrisico's. Over het algemeen geldt voor alle softwareprojecten dat de ontwikkelomgeving en bijvoorbeeld ook de toepassings-API beveiligd moeten worden. De volgende tabel geeft een overzicht van AI-beveiligingsrisico's, beschermende maatregelen en de verantwoordelijkheden voor de tegenmaatregelen.

[47] genai.owasp.org/llm-top-10/
[48] genai.owasp.org/resource/llm-applications-cybersecurity-and-governance-checklist-english/
[49] owaspai.org/docs/ai_security_overview/

	Veilige levenscyclus van softwareontwikkeling	Code Review	Monitoring van ongunstige inputs	EDR/XDR	Audits van modellen tegen ongunstige input en triggers	Data Loss Preventie	Opschonen van trainingsgegevens	Security Audits	Gebruikerstraining	Gebruikersauthenticatie	Toegangscontrole	Audit-Logs	Contracten	Geen internettoegang voor modellen	Bias-Detektie software	Verklaarbare AI-frameworks	Individuele factchecking	Reinforcement learning met mensen in een lus en finetuning van de modellen	Wettelijke vereisten
Model Poisoning Aanvallers vervalsen gegevens tijdens training	A	A		A	B		A	A			A	A				A			
Aanvallers stelen of repliceren het model	A		N	B		B		B		B	B	B							
Aanvallers stelen of repliceren vertrouwelijke bedrijfsgegevens die in het model zitten	A	A	N	A	B	B	A	B		B	B	B							
Fabrikanten triggeren backdoors op bepaalde onderwerpen / via afhankelijkheden		N		N				N				N		N					
Fabrikanten nemen opzettelijk valse verklaringen op in modellen		N			N				N	N		N			N	N	N		
Model stuurt klantgegevens naar fabrikant		N				N		N	N	N	N	N	N	N		N			N
Inbreuk op het auteursrecht							A		A				B			N		A	A
Leveranciers compromitteren als gevolg van kwetsbaarheden in applicaties	A	B		B		N		B			B	B	B	N					A
Openbaarmaking van de systeemprompt door middel van Prompt injectie			A		A	A		A		A	A	A	A	B					A
Compromitteren door aanvallen op de toeleveringsketen	B	B		B		N		B			B	B	B	N					B
AI-fabrikanten en AI-aanbieders verzamelen legaal of illegaal gebruikersinvoer						N			N	N	N		B	N					A
AI-componenten in lokale software verzamelen klantgegevens		N		N		N		N			N	N	B	N					A
Leveranciers manipuleren de output van het AI-model					N				N				B		N	N	N		B
Modellen hallucineren en confabuleren							A		N							N	N	A	

	Veilige levenscyclus van softwareontwikkeling	Code Review	Monitoring van ongunstige inputs	EDR/XDR	Audits van modellen tegen ongunstige input en triggers	Data Loss Preventie	Opschonen van trainingsgegevens	Security Audits	Gebruikerstraining	Gebruikersauthenticatie	Toegangscontrole	Audit-Logs	Contracten	Geen internettoegang voor modellen	Bias-Detektie software	Verklaarbare AI-frameworks	Individuele factchecking	Reinforcement learning met mensen in een lus en finetuning van de modellen	Wettelijke vereisten
Modellen reproduceren vooroordelen in hun antwoorden															B	B	N	A	A
Aanvallen van derden via gecompromitteerde websites, e-mailberichtent en phishing			N	N		N		N	N		N	N		B		B			
Gebruikers testen Prompt Injections			B		B				N	N	N	B	B					A	A
Genereren van phishing e-mailberichtent			B						N	B		B	B					A	N
Illegale en schadelijke informatie ophalen			B		B					B		B	B		B	A	N	A	A
Fraude en manipulatie met door machines gegenereerde teksten en afbeeldingen			B						N	B		B	B					A	N
Bedrijven en derden ontvangen indirect valse informatie van AI-gebruikers									N				N				N		
Ontvangst van niet-beoordeelde AI-inhoud via sociale media, onderzoeksliteratuur, enz.									N				N				N		
Publicaties met impliciete en ongenoemde AI-ondersteuning									N				N				N		N

Tabel 11: Veiligheidsrisico's van AI-modellen en beschermingsmaatregelen

Legenda:

A = Tegenmaatregelen van de kant van ontwikkelaars en/of verkopers van het model
N = Tegenmaatregelen van de kant van de gebruikers van het model
B = Tegenmaatregelen aan beide zijden

Het EU-agentschap ENISA noemt dat "misbruik van AI voor cyberaanvallen" tegen 2030[50] een van de belangrijkste cyberbeveiligingsdreigingen is. De gebruikte AI-algoritmen en tools evolueren voortdurend. Aanvallers profiteren van deze ontwikkeling en aanvallen worden steeds complexer en moeilijker door detectietools te detecteren. Bedrijven, overheden en organisaties staan dan ook voor de uitdaging om met behulp van AI de detectie van en verdediging tegen aanvallen te optimaliseren en

[50] ec.europa.eu/newsroom/ECCC/items/766303/en

steeds effectiever te maken. De introductie en integratie van AI moet zorgvuldig en snel worden gepland, continu worden gemonitord, regelmatig worden geactualiseerd en verder worden ontwikkeld.

Daarnaast is het ook essentieel om het personeel op te leiden en bewust te maken van de bedreigingen van AI. Nu AI steeds meer wordt geïntegreerd in een breed scala aan bedrijfsprocessen, is een fundamenteel begrip van de technologie, evenals de juiste regelgeving en beveiligingsmaatregelen, noodzakelijk.

4.5 Beveiliging van de toeleveringsketen

De veerkracht van toeleveringsketens wordt voor organisaties steeds meer een centrale, sectoroverschrijdende vereiste. Door geopolitieke spanningen, cyberdreigingen en aanscherping van de regelgeving neemt de druk toe om afhankelijkheden niet alleen economisch maar ook op het gebied van veiligheid te beoordelen. Met de nieuwe NIS2-richtlijn, de bijgewerkte ISO/IEC 27001:2022 en de Duitse wet op de due diligence in de toeleveringsketen (LkSG) worden specifieke eisen van kracht, die zowel van invloed zijn op organisaties als op hun dienstverleners en leveranciers. Daarnaast biedt de ISO 28000 een gespecialiseerd kader voor een gestructureerde beoordeling van veiligheidsrelevante aspecten binnen de gehele toeleveringsketen.

Een belangrijk kenmerk van de NIS2[51] is de uitgebreide focus op upstream serviceproviders en leveranciers. Bedrijven worden verplicht uit te leggen hoe zij de risico's in hun toeleveringsketen identificeren, beoordelen en beheersen. Onderdeel hiervan zijn de mogelijkheid om incidenten te melden en het recht om beveiligingsmaatregelen bij derden te controleren.

ISO/IEC 27001 in de herziene versie van 2022[52] is geschikt voor implementatie. De norm vereist een systematisch beheer van informatiebeveiliging dat niet eindigt bij de grenzen van de organisatie. De nieuwe maatregelen A.5.22 en A.5.23 roepen specifiek op om de veiligheid in de toeleveringsketen te beheren en duidelijke controlemechanismen in te stellen bij ICT-dienstverleners.

Een ander juridisch onderdeel is de Duitse wet voor de Due Diligence van de leveringsketen (LkSG), die sinds 1 januari 2023 bindend is voor bedrijven met meer dan 1.000 werknemers. Het verplicht bedrijven om systematische risicoanalyses uit te voeren in hun wereldwijde toeleveringsketens. Bedrijven moeten niet alleen hun directe zakenpartners evalueren, maar ook verantwoordelijkheid nemen voor de stadia stroomopwaartse van de toeleveringsketen. Naast risico's voor mens en milieu worden ook IT-beveiligingsrisico's steeds belangrijker. Een succesvolle cyberaanval op een kritieke leverancier kan niet alleen operationele schade veroorzaken, maar ook juridische gevolgen hebben, bijvoorbeeld als due diligence-verplichtingen worden geschonden als gevolg van onderbreking van de leveringsrelatie.

De ISO 28000 vult deze aanpak op een zinvolle manier aan, omdat het zich specifiek richt op veiligheidsaspecten in logistieke processen. In tegenstelling tot de ISO 27001, die voornamelijk betrekking heeft op informatiebeveiliging, heeft de ISO 28000 ook betrekking op fysieke risico's, sabotage, productmanipulatie en veiligheidskritische onderbrekingen in transport en opslag. De norm is met name geschikt voor internationale bedrijven en voor organisaties met een verhoogd risico in de fysieke toeleveringsketen. Door hun gestructureerde aanpak kunnen processen worden geïdentificeerd, geëvalueerd en verbeterd om daarmee de hele waardeketen veiliger te maken. Vanuit praktisch oogpunt is het aan te raden om bestaande (informatiebeveiligings)beheersystemen in te zetten en gericht uit te breiden.

Integratie van de eisen van de NIS2, de ISO/IEC 27001, de ISO 28000 en de LkSG is mogelijk en ook nuttig.

Doorslaggevende succesfactoren hiervoor zijn het betrekken van leveranciers bij bestaande beveiligingsprocessen en transparante communicatie over verwachtingen en maatregelen. Op deze manier kan het voldoen aan de toenemende wettelijke eisen als een strategisch voordeel worden gebruikt.

[51] Op het moment van publicatie van deze hand-out was de NIS2 nog niet geïmplementeerd in Duitsland.
[52] De toeleveranciers van de automobielindustrie moeten de specificaties implementeren volgens de TISAX-standaard.

Allereerst moet een overzicht worden gecreëerd van het leverancierslandschap. Hierin moet duidelijk worden hoe en welke leveranciers aan de eigen organisatie zijn gekoppeld. Dit geldt niet alleen voor leveranciers van softwareproducten, maar, voor zover zij via directe of indirecte technische of procedurele interfaces met de organisatie zijn verbonden, voor alle leveranciers van de organisatie.

Daarbij moeten bestaande contracten worden herzien, verantwoordelijkheden opnieuw worden gedefinieerd en risicobeoordelingen regelmatig worden aangepast. In het geval van strategisch kritische leveranciers is het zinvol om regelmatig leveranciersaudits uit te voeren en waarbij ook de veiligheidsaspecten worden meegewogen[53].

Risicoanalyse maakt het mogelijk om kritieke processen te identificeren, afhankelijkheden te bepalen, risico's in verband met de betreffende dreigingsituatie te beoordelen en is daarmee ook de basis voor de identificatie van geschikte beveiligingsmaatregelen. Aan de technische kant worden onder andere de toegang tot bedrijfssystemen, de omvang en gevoeligheid van de verwerkte gegevens, de regionale risicosituatie en de eerdere incidentgeschiedenis beoordeeld.

Voor de geïdentificeerde risico's moeten veiligheidseisen worden vastgesteld. Deze eisen hebben een tweeledig doel: enerzijds dienen ze voor een gestructureerde identificatie van veiligheidsmaatregelen voor de eigen organisatie, anderzijds ondersteunen ze de dialoog met leveranciers en creëren ze een gemeenschappelijk begrip van de noodzakelijke maatregelen. Vanwege de sterke onderlinge afhankelijkheid van de processen moet de beveiliging van de toeleveringsketen sectoroverschrijdend worden overwogen.

Moderne supply-chain management, dat wil voldoen aan de eisen van de NIS2, de ISO 27001 en de LkSG, vraagt om een samenspel van governance, processen en technologie. Vooral op operationeel niveau moeten, om daadwerkelijke effectiviteit te bereiken, gedefinieerde eisen worden omgezet naar concrete veiligheidsmaatregelen.

Op technisch niveau betekent dit bijvoorbeeld dat de toegang voor externe dienstverleners uitsluitend via beveiligde, gesegmenteerde verbindingen verloopt. Deze omvatten jump-hosts met session-recording, tijdelijk delen van toegang, multi-factor authenticatieprocedures en logfile-registratie van alle activiteiten. Daarnaast moeten voor bijzonder gevoelige verbindingen, om realtime verdacht gedrag te detecteren, SIEM-systemen worden gebruikt.

Om de veiligheid van de toeleveringsketen te waarborgen zijn verschillende maatregelen nodig. De eerste stap begint met de aanschaf van de IT-beveiligingscomponenten. Onder het trefwoord Secure-by-Demand heeft het Amerikaanse Cybersecurity & Infrastructure Security Agency (CISA) een richtlijn opgesteld met 12 eisen voor fabrikanten opgesteld waarmee bij de aanschaf rekening moet worden gehouden[54]. Deze handreiking is in de eerste plaats opgesteld voor de aanschaf van veilige OT, maar kan in licht gewijzigde vorm ook worden gebruikt voor IT-componenten. CISA benadrukt dat de weging van de afzonderlijke aanbevelingen moet worden aangepast aan de individuele omstandigheden. Dit geldt met name voor de gebruikte systemen en het beschikbare budget.

Vooral in het geval van softwareleveranciers en software-intensieve IT-producten is het noodzakelijk om de levering van een SBOM[55] door de leverancier te eisen en deze voortdurend up-to-date te houden. De SBOM is bedoeld om het mogelijk te maken om snel kritieke software-inhoud te identificeren en indien nodig te beperken.

Ook vulnerability management speelt een rol. Externe webservices en interfaces moeten regelmatig door middel van geautomatiseerde scans worden gecontroleerd op configuratiefouten, verouderde systemen en onveilige certificaten. Van toonaangevende producten en diensten kan deze informatie te koop zijn. Ze worden direct meegenomen in de risicobeoordeling.

Op gegevensniveau is de consistente toepassing van het beginsel van Least Privileges van essentieel belang. Dienstverleners krijgen alleen toegang tot wat ze absoluut nodig hebben, bovendien moeten alle gegevensstromen worden versleuteld, zowel in transit als in rust. Dit moet duidelijk en op een technisch begrijpelijke manier worden geregeld in contracten.

[53] Zie hoofdstuk "Omgaan met dienstverleners"
[54] www.cisa.gov/resources-tools/resources/secure-demand-guide
[55] Zie hoofdstuk "Software stukslijst“ (SBOM)

Naast de geïmplementeerde technische beveiligingsmaatregelen moet altijd rekening worden gehouden met de continuïteit van de bedrijfsvoering. Ook moeten nood- en herstartplannen[56] worden opgesteld en getest.

Ook zijn robuuste organisatiestructuren nodig: een leveranciersregister met beveiligingsprofielen, auditcycli met op risico's gebaseerde intervallen, gecoördineerde escalatieprocedures in incidentmanagement en training voor alle interne afdelingen die met derden werken. Informatiebeveiliging moet, als een natuurlijk onderdeel van corporate diligence, worden geïntegreerd in het dagelijks leven van de inkoop-, juridische en projectafdelingen.

Het beveiligen van de supply-chain is geen geïsoleerd project, maar onderdeel van een lange termijn veiligheidsstrategie. Bedrijven die in een vroeg stadium beginnen met het implementeren en hun afhankelijkheden op een gestructureerde manier analyseren, creëren niet alleen rechtszekerheid, maar ook operationele veerkracht en dus meer veerkracht in een steeds onstabielere omgeving. Dit dient de belangen van alle stakeholders en verhoogt op de lange termijn de waarde van de onderneming.

[56] Zie hoofdstuk "Calamiteiten en crisisbeheersing"

IT Security Association Germany (TeleTrusT)

Het Bundesverband IT-Sicherheit e.V. (TeleTrusT) is een wijdverspreid competentienetwerk voor IT-beveiliging bestaande uit leden uit de industrie, administratie, consultancy en onderzoek, evenals nationale en internationale partnerorganisaties met vergelijkbare doelstellingen. Met een breed scala aan leden en partnerorganisaties belichaamt TeleTrusT het grootste competentienetwerk voor IT-beveiliging in Duitsland en Europa. TeleTrusT biedt interdisciplinaire fora voor IT-beveiligingsexperts en vergemakkelijkt informatie-uitwisseling tussen leveranciers, gebruikers, researchers en autoriteiten. TeleTrusT becommentarieert technische, politieke en juridische kwesties met betrekking tot IT-beveiliging en is organisator van evenementen en conferenties. TeleTrusT is een vereniging zonder winstoogmerk, met als doel de professionaliteit van informatiebeveiliging te bevorderen, het bewustzijn en de beste praktijken op alle domeinen van informatiebeveiliging te vergroten. TeleTrusT is drager van de "European Bridge CA" (EBCA; PKI-netwerk van vertrouwen), de IT-expert-certificering "TeleTrusT Information Security Professional" (T.I.S.P.) en "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) en biedt het vertrouwenszegels "IT Security made in Germany" en "IT Security made in EU". TeleTrusT is lid van het European Telecommunications Standards Institute (ETSI). Het hoofdkantoor van de vereniging is gevestigd in Berlijn, Duitsland.

Contact:

IT Security Association Germany (TeleTrusT)
Dr. Holger Mühlbauer
Chausseestraße 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.