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

TeleTrusT
Pioneers in IT security.

IT Sicherheitsgesetz en EU General Data Protection Regulation:

Richtlijn "State of the Art"

Technische en organisatorische maatregelen

2020

Nederlandse versie

in co-operatie met

centrum informatiebeveiliging en privacybescherming

Erkentelijkheid

TeleTrusT bedankt de volgende personen voor hun deelname aan de TeleTrusT werkgroep Stand der Techniek en hun actieve bijdrage aan deze richtlijn.

Projectleiding

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

Auteurs en deelnemende experts

Alsbih, Amir - Keyidentity GmbH
Bartels, Karsten U. - HK2 Rechtsanwälte
Barth, Michael - genua GmbH
Barzin, Petra - Secorvo Security Consulting GmbH
Beutlhauser, Harald - Rohde & Schwarz Cybersecurity GmbH
Dehning, Oliver - Hornetsecurity GmbH
Dominkovic, Dennis - SEC Consult Unternehmensberatung GmbH
Dubbel, Sascha - CrowdStrike GmbH
Falkenthal, Oliver - CCVOSSEL GmbH
Fischer, Marco - procilon IT-Solutions GmbH
Gehrmann, Mareike - Taylor Wessing Partnergesellschaft mbB
Gimbut, Leonid - DIGITTRADE GmbH
Gora, Stefan - Secorvo Security Consulting GmbH
Heyde, Steffen - secunet Security Networks AG
Kerbl, Thomas - SEC Consult Unternehmensberatung GmbH
Kippert, Tobias - TÜV Informationstechnik GmbH
Kolmhofer, Robert - FH Oberösterreich Studienbetriebs GmbH
Krebs, Tobias - eperi GmbH
Krosta-Hartl, Pamela - LANCOM Systems GmbH
Lawicki, Tomasz - Schwerhoff Consultants
Liedke, Bernd - TÜV Informationstechnik GmbH
Maier, Janosch - Crashtest Security GmbH
Martin, Karl-Ulrich - Detack GmbH
Menge, Stefan - AchtWerk GmbH & Co. KG
Michaelis, Patrick - The Auditing Company, Sachverständigen-Sozietät Dr. Schwerhoff
Mörl, Ramon - itWatch GmbH
Mühlbauer, Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Müller, Siegfried - MB connect line GmbH
Paulsen, Christian - DFN-CERT Services GmbH
Robin, Markus - SEC Consult Unternehmensberatung GmbH
Rost, Peter - Rohde & Schwarz Cybersecurity GmbH
Wallaschek, Felix - Detack GmbH
Wüpper, Werner - Wüpper Management Consulting GmbH

Colofon

Uitgever:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
IT Security Association Germany (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4306
Fax: +49 30 4005 4311
E-Mail: info@teletrust.de
https://www.teletrust.de

Dutch version: Jan Breeman

V 1.6_2020-02_NL

Inhoud

Afbeeldingenoverzicht

Tabeloverzicht

Principes van de richtlijn

Toen de Duitse IT-Sicherheitsgesetz (ITSiG) in juli 2015 van kracht werd, lanceerde het Bundesverband IT-Sicherheit e.V. (TeleTrusT) de werkgroep Stand der Technik (hierna AK SdT genoemd), om geïnteresseerden richting en aanbevelingen te geven te geven op de State of the Art, ofwel stand van de techniek, voor de technische en organisatorische maatregelen. Om aan deze hoge eisen te voldoen, heeft de AK SdT voor het ontwikkelen, de evaluatie en het bijwerken van de richtlijn de volgende beginselen vastgesteld:

1. ***Basisbegrip van het document***

Deze richtlijn is bedoeld om bedrijven en leveranciers (fabrikanten en dienstverleners) te helpen bij het bepalen van de State of the Artin de zin van de General Data Protection Regulation (GDPR) en de ITSiG. Het document kan dienen als referentie voor contractuele overeenkomsten, aanbestedingsprocedures en voor de classificatie van geïmplementeerde beveiligingsmaatregelen.

2.

Deze richtlijn is een uitgangspunt voor het bepalen van wettelijk voorgeschreven IT-beveiligingsmaatregelen. Deze richtlijn is een uitgangspunt voor het bepalen van juridische IT-beveiligingsmaatregelen; ze vormen geen vervanging voor technisch, organisatorisch of juridisch advies of voor individuele adviezen.

3. ***Verantwoordelijkheid voor de ontwikkeling, evaluatie en actualisering***

De AK SdTen de TeleTrusT werkgroep Recht zijn gericht op het beantwoorden van de vraag, hoe de desbetreffende State of the Art relevant is in de zin van de wet met betrekking tot de technische en organisatorische maatregelen, en hoe wettelijke eisen kunnen worden geïmplementeerd.

4. ***Begrip van de aanpa***

De AK SdT verwerkt haar resultaten op transparante wijze en stelt de aanbevelingen voor actie en oriëntatie, met een reguliere bijwerkprocedure, publiekelijk ter discussie.

5. ***Evaluatieprocedure***

De AK SdT baseert haar evaluatie op een gestandaardiseerde methode, die voor elke afzonderlijke maatregelen is ingevuld en bekend gemaakt. De methode voor het beoordelen van de State of the Art van technische maatregelen wordt beschreven in hoofdstuk 2.2.

6. ***Actualisatie***

Om gelijke tred te houden met de technologische vooruitgang, s het de bedoeling dat deze richtlijn regelmatig wordt bijgewerkt en gepubliceerd. Momenteel is het doel om tweejaarlijks een update van de richtlijnen te publiceren.

Kleine aanpassingen van en toevoegingen aan de richtlijn (zoals nieuwe bijdragen aan technische maatregelen) zullen gedurende het jaar als een zogenaamde herziening van de richtlijn verschijnen.

Leeswijzer

Deze richtlijn is uitgangspunt voor het bepalen van de wettelijke IT-beveiligingsmaatregelen die overeenkomen met de State of the Art. Ze vormt geen vervanging voor technisch, organisatorisch of juridisch advies of specifieke adviezen.

De ITSiG is gericht op het leveren van een bijdrage aan het verbeteren van de beveiliging van informatiesystemen in Duitsland en is van kracht sinds 25/07/2015; het kan één op één ook worden toegepast in Nederland.

1 Introductie

1.1 IT Sicherheitsgesetz (Wet op de IT-beveiliging)

De ITSiG is sinds 25 juli 2015 van kracht en is bedoeld om bij te dragen aan het verbeteren van de beveiliging van informatietechnologiesystemen in Duitsland. De voorschriften die aan de wet ten grondslag liggen, zijn bedoeld om de systemen te beschermen met betrekking tot de huidige en toekomstige dreigingen in termen van beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van beschermde goederen. Volgens de toelichting op de wet heeft de wet als doel de IT-beveiliging van bedrijven te verbeteren, de bescherming van de burgers op internet te vergroten en ook het Bundesamt für Sicherheit in der Informationstechnik (BSI)[1] en het Bundeskriminalamt (BKA)[2] te versterken.

De ITSiG is een zogenaamde omnibus bill, de wet zelf diende alleen om verschillende sectorspecifieke wetten aan te passen. De ITSiG heeft onder andere in de wet op het Bundesamt für die Sicherheit in der Informationstechnik (BSIG) wettelijke regels gestel voor kritische infrastructuren (de KRITIS Verordnung, kortweg KritisV) en heeft juridische wijzigingen aangebracht in het Atomgesetz (AtomG)[3], het Energiewirtschaftsgesetz (EnWG)[4], het Telemediengesetz (TMG)[5] en het Telekommunikationsgesetz (TKG)[6].

De ITSiG en de bijbehorende rechtvaardiging zijn beschikbaar via de link: https://www.teletrust.de/it-sicherheitsgesetz.

De ITSiG bepaalt uitgebreide veranderingen voor KRITIS exploitanten en bedrijven die Telemediawet diensten aanbieden. Exploitanten van kritieke infrastructuur moeten conform BSIG § 8a lid 1minimaal voldoen aan een niveau van IT-beveiliging dat overeenkomt met de State of the Art. Ze zijn ook verplicht om bepaalde IT-beveiligingsincidenten te melden bij de BSI. Het classificeren van een organisatie als kritieke infrastructuur kent twee niveaus: Enerzijds moet worden nagegaan of sprake is van een sector die inherent als kritisch is aangemerkt (sectorgebondenheid) en anderzijds of sprake is van een bijzondere veiligheidsrelevantie (foutimpact relevantie). Indirect zijn de wettelijke bepalingen ook van invloed op dienstverleners en leveranciers aan wie de KRITIS exploitanten contractueel de relevante verplichtingen opleggen.

Op grond van BSIG sectie 10 lid 1 is het Bundesministerium des Innern (BMI) bevoegd om een wettelijke regeling uit te werken waarin wordt gespecificeerd welke faciliteiten, installaties of delen daarvan als kritieke infrastructuur in de zin van deze wet worden beschouwd. Hierbij wordt rekening gehouden met de belangen, de betekenis van de dienstverlening en het verzorgingsgebied. Op 13 april 2016 heeft de Duitse federale regering ingestemd met het aannemen van de, door de federale minister van binnenlandse zaken ingediende, ministeriële regeling aangenomen om kritieke infrastructuren te bepalen gebaseerd op de BSIG-Kritis Verordnung (BSI-KritisV). Het eerste deel van de KritisV over het toepassen van de ITSiG is vervolgens in werking getreden op 03.05.2016. Het tweede deel van de KritisV was al op 31 mei 2017 aangenomen en is uiteindelijk in werking is getreden op 01.06.2017. De verordening regelt de classificatie als kritieke infrastructuur voor organisaties in de sectoren energie, water, voedsel, informatietechnologie en telecommunicatie (1e korf) en de sectoren gezondheid, financiën en vervoer en vervoer (2e korf).

Conform BSIG Art. 8a lid 1 hebben exploitanten van kritieke infrastructuren een periode van twee jaar, nadat de wettelijke regeling in werking is getreden, om adequate technische en organisatorische maatregelen (TOM's) te treffen ter voorkoming van verstoringen in beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van hun IT-systemen, onderdelen of processen die essentieel zijn voor de werking van de kritieke infrastructuren die zij exploiteren.

[1] Het Duitse federale bureau voor informatiebeveiliging
[2] De Duitse strafrechtelijke politie
[3] De Duitse atoomenergiewet
[4] De wet op de levering van elektriciteit en gas: https://www.gesetze-im-internet.de/enwg_2005/EnWG.pdf
[5] De Duitse telemediawet: https://www.gesetze-im-internet.de/tmg/
[6] De Duitse telecommunicatiewet: https://dejure.org/gesetze/TKG

Conform TMG § 13 lid 7 moeten aanbieders van telemedia-diensten, ervoor zorgen dat hun technische voorzieningen binnen de grenzen van hun technische en economische grenzen door TOV worden beschermd. Bij het kiezen van deze TOM moet rekening worden gehouden met de State of the Art. Er is geen verplichting om incidenten te melden. Dit beïnvloedt elke organisatie die een telemedia-service exploiteert. In tegenstelling tot de KRITIS Verordnung voorzien de bepalingen van de Telemediawet niet in een overgangsperiode of vrijstelling van micro-ondernemingen.

1.2 Branchespecifieke veiligheidsnormen van BSI voor KRITIS exploitanten

De ITSiG vereist dat KRITIS exploitanten voldoen aan of in ieder geval rekening houden met de State of the Art van IT-beveiligingsmaatregelen. Dit beveiligingsniveau wordt echter niet verder gespecificeerd in de wet. Het is echter toegestaan zogenoemde sectorspecifieke veiligheidsnormen (hierna B3S genoemd) voor de KRITIS sectoren voor te stellen. Het BSI is verantwoordelijk voor het erkennen (en goedkeuren) van, door vertegenwoordigers van de industrie voorgestelde, sectorspecifieke veiligheidsnormen.

De eerste aanwijzingen voor het ontwikkelen van de B3S zijn te vinden door betreffende KRISIS-exploitanten en -verenigingen in het door BSI gepubliceerde: "Orientierungshilfe zu Inhalten und Anforderungen an B3S, Artikel 8a lid 2 BSIG"[7]. Het ontwerp bevat de volgende procedure:

1. definitie van het toepassingsgebied en de beschermingsdoelstellingen van de B3S;
2. beoordeling van de sectorspecifieke risicosituatie;
3. risicoanalyse van de sectorspecifieke risicosituatie;
4. afleiding van gepaste en redelijke sectorspecifieke maatregelen voor.

De B3S is bedoeld om te helpen bij het selecteren van passende maatregelen door te verwijzen naar regelingen en maatregelen in overeenstemming met de gebruikelijke best practices van de industrie. Bovendien moeten de B3S, indien nodig, hun beperkingen vermelden, zoals wanneer meer bescherming en dus aanvullende maatregelen nodig zijn en voorstellen doen voor dergelijke aanvullende voorzorgsmaatregelen en maatregelen.

Wat toereikendheid betreft, daarbij moet in de allereerste plaats rekening worden gehouden met de financiële last die de KRITIS exploitant moet dragen en in het bijzonder de uitvoeringskosten. Ten slotte mogen de benodigde kosten voor de uitvoering niet onevenredig zijn aan de gevolgen van een tekortkoming of aantasting van de betrokken kritieke infrastructuur[8]. Of een maatregel passend d.w.z. economisch is, kan echter alleen op individuele basis worden bepaald, rekening houdend met de eigen vraag naar bescherming en de implementatiekosten van de totale set van benodigde maatregelen.

Vervolgend geeft de richtlijn een lijst van onderwerpen (zoals Asset Management, leveranciers, dienstverleners en derden) die gedekt moeten worden door de B3S. Vervolgens zullen de betrokken KRISIS exploitanten en -verbanden nadere informatie ontvangen over de mate van gedetailleerdheid van de voorzorgsmaatregelen die in de B3S moeten worden beschreven. Ten slotte biedt de richtlijn opties voor de verificatie van de implementatie.

Uit de richtlijn blijkt nogmaals dat het vaststellen van een minimumnorm voor een bepaalde sector afhangt van veel individuele factoren. Daarom moet de minimumnorm nauwkeurig op basis van de individuele behoeften worden bepaald. Dit geldt in het bijzonder voor gereguleerde sectoren die onderworpen zijn aan bijzondere wetgeving, zoals de Telecommunicatiewet.

In de sector water van de sectoren watervoorziening en afvalwaterzuivering is voor het eerst sinds 1 augustus 2017 een branchespecifieke norm (BS3 WA) gedefinieerd en door het BSI gepubliceerd. De BS3 WA bestaat uit een informatieblad en een IT-beveiligingsrichtlijn die jaarlijks worden bijgewerkt. De BS3 WA is gebaseerd op de IT-Grundschutz (Basic Protection Catalogue) van BSI en van sectorspecifieke veiligheidseisen.

Het blijft echter onduidelijk volgens welke criteria de voorgestelde veiligheidsnormen door de

[7] Leidraad voor inhoud en eisen aan branchespecifieke beveiligingsstandaarden (B3S) volgens BSIG § 8a, lid 2. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/b3s_Orientierungshilfe.html

[8] BSIG § 8a lid 1 zin 3

watersector zijn geselecteerd en volgens welke criteria ze vervolgens door het BSI zijn herkend als B3S WA in de zin van de State of the Art.

1.3 Europese implicaties

De BSIG wordt aangevuld met andere Europese richtlijnen. Voor dit doel heeft de Europese Commissie de richtlijn aangenomen betreffende maatregelen om een hoog gemeenschappelijk niveau van veiligheid van netwerk- en informatiesystemen (NIS-richtlijn) te waarborgen, dat in nationaal recht moet worden omgezet. Er zijn geen fundamentele wijzigingen, aangezien de nationale wetgever al een groot deel van de door de Europese wetgever beoogde eisen heeft voorzien door de ITSiG te adopteren. De bijbehorende uitvoeringswet van de NIS-richtlijn, aangenomen op 27 april 2017, leidt dus alleen maar tot een aanvulling op de BSIG.

Op basis van de richtlijn is onder meer BSIG § 8c gecreëerd, dat een aanvullende verplichting creëert voor aanbieders van zogenoemde digitale diensten. Digitale diensten zijn online zoekmachines en marktplaatsen en cloud-computing diensten van een gestandaardiseerde grootte. Deze diensten moeten ook technische en organisatorische maatregelen (TOM) implementeren om de IT-beveiliging te waarborgen en waarbij rekening moet worden gehouden met de State of the Art. De maatregelen zijn bedoeld om een passend beschermingsniveau te waarborgen dat geschikt is voor het risico, waarbij onder meer rekening wordt gehouden met de veiligheid van systemen en installaties, de afhandeling van beveiligingsincidenten en het beheer van operationele continuïteit.

1.4 General Data Protection Regulation (GDPR)

De Europese GDPR, in het Nederlands de Algemene Verordening Gegevensbescherming (AVG), werd in 2016 aangenomen en trad op 25 mei 2018 in werking. Het primaire doel van de GDPR is de bescherming van de persoonlijke gegevens van Europese de burgers. De verordening is gebaseerd op een risicobenadering van haar beschermingsdoelstellingen. Op de technische gegevens moeten passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van natuurlijke personen te beschermen. Daarbij moet ook rekening gehouden worden met het State of the Art element. GDPR Art. 32 en Bijlage 1, dat de beveiliging van de verwerking regelt en § 9 van de Duitse privacywetgeving (DBSG) vervangt, schrijven zeer specifiek voor dat in het kader van de beveiliging van de gegevensverwerking rekening moet worden gehouden met de State of the Art. Daartoe moeten bewerkingsverantwoordelijken en verwerkers passende technische en organisatorische maatregelen nemen. Net als de ITSiG biedt de GDPR geen definitie van State of the Art. Hetzelfde geldt voor de EU-wet inzake de aanpassing en de uitvoering van gegevensbescherming (DSAnpUG-EU) en de daaruit voortvloeiende herziene versie van de Bundesdatenschutzgesetz (BDSG-nieuw). Bovendien moeten, in overeenstemming met GDPR Art.25 de beginselen van gegevensbescherming worden nageleefd door middel van (technologie) ontwerp (privacy by Design) en door gegevensbescherming vriendelijke presets[9] (privacy by default). Deze beginselen moeten ook uitgevoerd door middel van passende technische en organisatorische maatregelen.

De State of the Art moet echter niet alleen in overweging worden genomen bij het toepassen van de richtlijnen, maar ook uitvoerig worden gedocumenteerd. Daartoe zijn uitgebreide en verstrekkende documentatieverplichtingen vastgesteld, in het bijzonder de verplichting om een DataProtection ImpactAssessment (DPIA) uit te voeren en invulling te geven aan de verantwoordingsplicht. In dit verband stelt de richtlijn de documentatieverplichtingen op als haar eigen wettelijke verplichtingen. De technische en organisatorische maatregelen moeten daarom individueel worden bepaald en beschreven of gedetailleerd worden gedocumenteerd.

1.5 Toereikendheid van de maatregelen

De in deze richtlijn beschreven State of the Art richt zich op de inhoud die vanuit de ITSiG en de GDPR is vereist. Het is echter vanuit de ITSiG en de GDPR toegestaan om rekening te houden met andere economische aspecten bij het selecteren van beschermende maatregelen (safeguards) [10]. Of een maatregel economisch verantwoord is, kan echter alleen worden bepaald door een individuele afweging van de eigen beschermingsbehoeften en de uitvoeringskosten van de noodzakelijke maatregelen. Deze reden werd de doelmatigheidscontrole in deze richtlijn achterwege gelaten.

[9] In Vlaanderen wordt hiervoor veelal ‘‘standaardinstellingen zijn altijd zo privacyvriendelijk als mogelijk’’ gehanteerd.

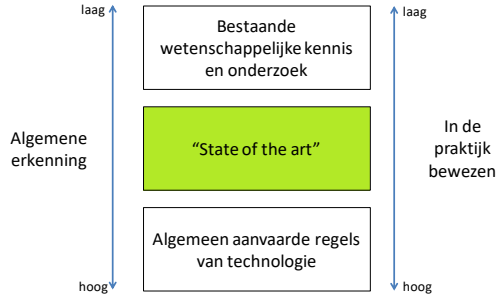
[10] Zie voor van juridische overwegingen bij de wettelijke eisen Bartels/Backer: “Die Berücksichtigung des Standes der Technik in der DSGVO”, DuD 4-2018, 214.

2 Bepaling van de State of the Art

2.1 Toelichting op de richtlijn

Het technologieniveau[11] State of the Art moet worden gedefinieerd in conceptueel vergelijkbare technologische begrippen, zoals algemeen aanvaarde regels van technologie (GART) en de bestaande wetenschappelijke kennis en onderzoek (State of science and research, ESKR)[12] en moet onafhankelijk van elkaar afgebakend zijn. Dit onderscheid is de essentiële basis voor het bepalen van het vereiste niveau van technologie. Zoals veel praktijk voorbeelden laten zien, worden deze drie begrippen in de jurisprudentie, in het algemeen en ook in de praktijk, door elkaar gebruikt en zelfs verward[13].

Deze drie begrippen en de bijbehorende driestappen theorie zijn geïntroduceerd in 1978 in het Kalkar besluit[14] van het Bundesverfassungsgerichts[15]. Op basis van dit besluit kunnen de drie technologieniveaus op gelijke wijze worden gepresenteerd:



Afbeelding 1: De driestaps theorie volgens het Kalkar-besluit

Het technologieniveau State of the Art bevindt zich tussen het meer innovatieve State of Science and Research en de beproefde algemeen aanvaarde regels van technologie. Deze drie technologieniveaus worden geflankeerd door de categorieën algemeen erkend" en "bewezen in de praktijk.

Als gevolg van de wettelijke classificatie wordt een duidelijk onderscheid vereist tussen subjectieve en objectieve criteria. Het State of the Art criterium moet puur objectief worden opgevat. De subjectieve aspecten houden bij de concrete bevindingen rekening met de wetten; ze hebben echter geen betrekking op de definitie van State of the Art.

Zo kan de State of the Art worden omschreven als de procedures, voorzieningen of werkwijzen die beschikbaar zijn in de verkeer van goederen en diensten, waarvan de applicatie het meest doeltreffend kan zorgen voor het verwezenlijken van de respectieve doelstellingen inzake rechtsbescherming[16].

Kortweg: de State of the Art beschrijft de beste prestaties van een onderwerp dat op de markt beschikbaar is om een object te bereiken. Het onderwerp is de IT-beveiligingsmaatregel; het object is het wettelijke doel van de IT-beveiliging.

Technische maatregelen in de State of Science and Research zijn zeer dynamisch in hun ontwikkeling en gaan over in State of the Art, wanneer ze marktrijpheid hebben bereikt (of in ieder geval zodra zij op de markt worden geïntroduceerd). Daar neemt de dynamiek af, zoals door processtandaardisatie

[11] De term technologieniveau wordt gebruikt als vervanging voor State of Technology.
[12] Als alternatief kan "Bestaande wetenschappelijke kennis en technologie" worden gebruikt. In deze richtlijn zal "bestaande wetenschappelijke kennis en onderzoek" worden gebruikt, zodat onderscheid kan worden gemaakt tussen dit en 'state of the art'.
[13] Dr Mark Seibel, rechter in hoger beroep: https://www.dthg.de/resources/Definition-Stand-der-Technik.pdf
[14] BVerfGE, 49, 89 (135 f)
[15] Het Duitse federaal constitutioneel hof
[16] Bartels / Backer: Die Berücksichtigung des Stands der Technik in der DSGVO, 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.

van de processen. Technische maatregelen in het stadium Algemeen aanvaarde technische regels zijn ook beschikbaar op de markt. Hun mate van innovatie neemt af, maar ze hebben hun waarde in de praktijk bewezen en worden vaak beschreven in de relevante normen.

Door vooruitgang kan een verschuiving in de afzonderlijke technologieniveaus worden waargenomen (innovatie gerelateerde verschuiving):

1. een maatregel heeft initieel het stadium State of Science and Research;
2. bij introductie op de markt gaat het over naar State of the Art; en
3. bij toenemende verspreiding en erkenning op de markt worden uiteindelijk worden gekwalificeerd als Algemeen aanvaarde regels van technologie.

Om, gebaseerd op de oriëntatie van de eigen maatregelen, het vereiste bewijs te leveren over de State of the Art, volstaat het niet om de toegepaste maatregelen eenmalig te evalueren en te actualiseren door het installeren van zogenaamde patches. Dit bewijs kan alleen worden geleverd, door de toegepaste maatregel regelmatig en met behulp van een transparante methode te vergelijken met alternatieven die op de markt beschikbaar zijn.

2.2 Methode voor het bepalen van de **State of the Art**

De technische maatregelen beschreven in hoofdstuk 3.2 van deze richtlijn zijn beoordeeld aan de hand van een bruikbare methode gebaseerd op het eenvoudige beginsel van het beantwoorden van kernvragen over de mate van erkenning en de mate van proeftijd in de praktijk. De kernvragen zijn opzettelijk eenvoudig geformuleerd en laten een meer gedetailleerd beeld te zien van de twee dimensies van het onderzoek.

Voor elke kernvraag zijn drie mogelijke antwoorden aangegeven. De antwoorden zijn zo gekozen, dat indeling in een van de drie technologieniveaus mogelijk is. Elk antwoord moet ook gerechtvaardigd zijn. Hoewel de individuele vragen een indeling in een van de drie technologieniveaus mogelijk maken, hebben ze slechts betrekking op deelaspecten. Wat betekent dat de technische staat van een maatregel pas bepaald wordt, nadat alle vragen voor beide dimensies zijn beantwoord.

De volgende afbeelding toont het door de AK SdT gebruikte sjabloon, samen met de kernvragen voor het evalueren van de State of the Art van de technische maatregelen:

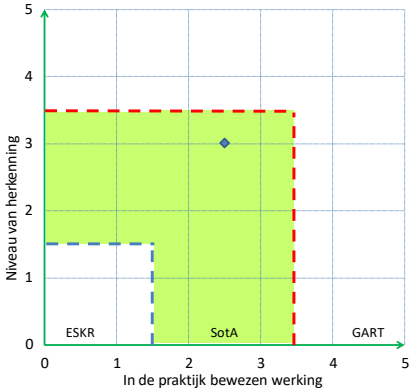
1.1 Vragen over de mate van erkenning			Beoordeling moet worden ingevuld door SotA werkgroep
1) Welke documentatie met betrekking tot de maatregel is openbaar beschikbaar? (beantwoord de vraag door de vakjes aan te vinken)			
☐ wetenschappelijke publicatie	☐ technische publicatie	☐ Massamedia	wetenschappelijke publicatie technische publicatie massamedia
(licht uw antwoord hier toe)			
2) Verwijst de maatregel naar nationale of internationale normen? (beantwoord de vraag door de vakjes aan te vinken)			
☐ nee, niet gestandaardiseerd	☐ ja, één	☐ ja, meer dan één	nee, niet gestandaardiseerd ja, één ja, meer dan één
(licht uw antwoord hier toe)			
3) Wordt de maatregel aanbevolen door erkende gremia/commissies? (beantwoord de vraag door de vakjes aan te vinken)			
☐ nee	☐ ja, grote	☐ ja, veel	nee Ja, grote Ja, veel
(licht uw antwoord hier toe)			
4) Wordt de geschiktheid van de maatregel regelmatig onderzocht? (beantwoord de vraag door de vakjes aan te vinken)			
☐ nee	☐ ja, door de fabrikant	☐ ja, door een onafhankelijke instantie	nee Ja, door de fabrikant Ja, door een onafhankelijke instantie
(licht uw antwoord hier toe)			
	Gemiddelde		

1.2 Vragen over het testen in de praktijk			Beoordeling moet worden ingevuld door SotA werkgroep
1) hoe wordt van de maatregel de mogelijkheid tot innovatie geclassificeerd? (beantwoord de vraag door de vakjes aan te vinken)			
☐ hoog	☐ midden	☐ laag	hoog midden laag
(beantwoord de vraag door de vakjes aan te kruisen)			
2) Waar werd de huidige versie van de maatregel getest? (beantwoord de vraag door de vakjes aan te vinken)			
☐ nee, niet gestandaardiseerd	☐ ja, één	☐ ja, meer dan één	nee, niet gestandaardiseerd ja, één ja, meer dan één
(beantwoord de vraag door de vakjes aan te kruisen)			
3) Bestaan vergelijkbare maatregelen in de markt? (beantwoord de vraag door de vakjes aan te vinken)			
☐ nee	☐ weinig	☐ veel	nee weinig veel
(licht uw antwoord hier toe)			
4) Hoe vaak wordt de maatregel conceptueel door de fabrikant de maatregel bijgewerkt? (beantwoord de vraag door de vakjes aan te vinken)			
☐ meer dan één keer per jaar	☐ één keer per jaar	☐ minder frequent	nee Ja, grote Ja, veel
(licht uw antwoord hier toe)			
		Gemiddelde	

Afbeelding 2: Evaluatiecriteria

Op basis van de gegeven antwoorden wordt met behulp van een puntensysteem een gemiddelde score gegenereerd. Met de verkregen waarden kan de actie in het diagram worden geclassificeerd.

Zoals in het diagram is weergegeven, wordt een maatregel geclassificeerd als State of the Art, als deze zich, gebaseerd op de gebruikte methode, binnen het groene veld bevindt.



ESKR	stand wetenschappelijk en onderzoek
SotA	stand van de techniek
GART	algemeen erkende regels van de technologie

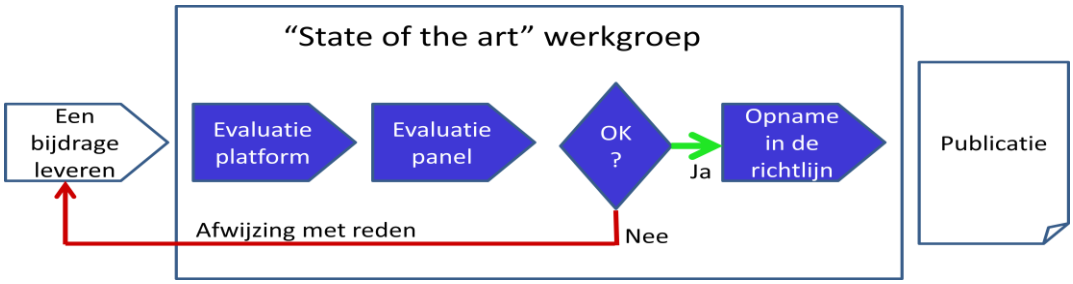
Afbeelding 3: Voorbeeld van de State of the Art classificatie

In deze richtlijn worden technologieën en methoden beschreven en geëvalueerd, dus in strikte zin geen beveiligingsproducten. De geschiktheid van de hier beschreven maatregelen voor het respectieve doel wordt dus geacht te zijn vervuld.

In de praktijk moet een geschikte methode (zoals vergelijkbaar met de hier geschetste methode) worden aangepast aan de omstandigheden van de organisatie, om zo op objectieve wijze de geïmplementeerde maatregelen te beoordelen, te vergelijken met alternatieven en om de verificatiedoeleinden te documenteren[17]

2.3 proces voor kwaliteitsborging van de richtlijn

De AK SdT streeft ernaar een hoge kwaliteit van de inhoud van de richtlijn te waarborgen. Om dit te bereiken, is in de AK SdT een proces vastgesteld, waarin de bijdragen de verschillende stadia succesvol moeten doorstaan:



Afbeelding 4: Procesoverzicht voor het evalueren van technische maatregelen in hoofdstuk 3.2

Nadat een nieuwe of gewijzigde bijdrage volgens een gestandaardiseerd sjabloon is ingediend (zie Figuur 4)), wordt de bijdrage in een evaluatie platform door IT-beveiligingsexperts anoniem geëvalueerd.

De resultaten worden besproken en door het reguliere evaluatiecomité van de AK SdT vastgesteld[18]. De in het sjabloon gedefinieerde, kernvragen en de daarop gegeven antwoorden en de professionele juistheid en actualiteit van de inhoud dienen de centrale zijn onder andere evaluatiecriteria.

Als het evaluatiecomité tot de conclusie komt dat een bijdrage niet voldoet aan de vereiste kwaliteit, dan wordt de overdracht ervan naar de richtlijn op een gemotiveerde wijze verworpen en wordt de auteur daarvan in kennis gesteld. De auteur heeft dan de mogelijkheid om zijn bijdrage bij te werken of aan te vullen en deze opnieuw voor een nieuwe toetsingsronde aan te bieden.

Bijdragen die deze uitgebreide procedure succesvol doorstaan, worden in de richtlijn opgenomen.

2.4 Vereiste beschermingsdoelstellingen

De met de ITSiG ingevoerde wetswijzigingen zijn gericht op de beschermingsdoelstellingen: beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit:

- ***Beschikbaarheid;***

De beschikbaarheid van IT-systemen en -componenten is beschikbaar en kan op basis van hun doel en functionaliteit altijd worden gebruikt.

- ***Integriteit;***

Integriteit is in het bijzonder van toepassing op de gegevens. De integriteit is aanwezig wanneer gewaarborgd wordt, dat verzonden gegevens de geadresseerde ongewijzigd en volledig bereiken.

- ***Vertrouwelijkheid;***

Vertrouwelijkheid bestaat, als gegevens die bescherming verdienen alleen aan bevoegden en op

[17] Lawicki, "Was bedeutet "Stand der Technik?'" gepubliceerd in het TeleTrusT Special supplement "Sicherheit & Datenschutz" in tijdschrift IX 6/2018: http://www.schwerhoff.com/was-bedeutet-stand-der-technik/

[18] Op de webpagina van TeleTrusT wordt een lijst met leden die actief zijn in de Task Force (evaluatiepanel) gepubliceerd: https://www.teletrust.de/arbeitsgremien/recht/stand-der-technik/, (Engelse versie: https://www.teletrust.de/en/arbeitsgremien/recht/task-force-state-of-the-art-in-it-security/)

toegestane wijze beschikbaar worden gesteld.

- ***Authenticiteit.***

Authenticiteit bestaat wanneer de unieke identiteit van de communicatiepartners (en van de communicerende componenten) is gewaarborgd.

Aanvullend op deze op de ITSiG toegespitste IT-beveiligingsdoelstellingen, bestaan, gebaseerd op de GDPR en uit het oogpunt van gegevensbescherming, nog andere beveiligingsdoelstellingen die hier in het bijzonder worden vermeld[19]:

- ***ontkoppelbaarheid (en gegevensminimalisatie);***
- ***transparantie;***
- ***interventievermogen***.

Deze aanvullende doelstellingen zijn deels concurrerend aan bovengenoemde IT-beveiligingsdoelstellingen. Aangezien de wettelijke eisen vanuit de GDPR en de ITSiG gelijktijdig van toepassing zijn, is het doel een gemeenschappelijke, duurzame oplossing met een hoog niveau van IT-beveiliging en gegevensbescherming. Dit kan alleen worden bereikt wanneer de functionarissen voor IT-beveiliging (Security Officers) en gegevensbescherming (Privacy Functionarissen) samenwerken.

Terwijl, vanuit het oogpunt van IT-beveiliging het de bedoeling is gegevens en in het bijzonder de infrastructuur te beschermen, gaat gegevensbescherming over het beschermen van de mensenrechten. Het is belangrijk deze verschillende gezichtspunten te begrijpen, om beschermende maatregelen definiëren en te implementeren.

[19] Geïnspireerd door het onafhankelijke centrum voor privacybescherming Schleswig-Holstein (ICPP): https://www.datenschutzzentrum.de/

3 Technische en organisatorische maatregelen (TOMS)

De ITSiG en GDPR vereisen naleving van de technische en organisatorische maatregelen of op zijn minst het rekening houden met de State of the Art. De wetgever heeft de relevante systemen en componenten niet nader gespecificeerd. Daarom moet de naleving van de State of the Art gebaseerd zijn op alle relevante onderdelen van de gegevensverwerking, met inbegrip van alle opties voor gegevensoverdracht en gegevensopslag.

Omdat IT-infrastructuren sterk afhankelijk zijn van sector en applicaties, is het niet mogelijk om een uitgebreide lijst van de afzonderlijke componenten op te nemen in deze richtlijn. De auteurs hebben zich daarom gericht op het beschrijven van de essentiële componenten en processen.

3.1 Introductie

In het kader van de ITSiG zijn applicaties, met betrekking tot het gebruik, soms zeer specifiek. Dit omvat bijvoorbeeld eenvoudig beveiligde mailcommunicatie en de beveiligde besturingsfunctionaliteit om een elektriciteitscentrale te beveiligen. Als gevolg hiervan is het moeilijk om in deze studie een volledige lijst met applicaties op te stellen en te beschrijven Omdat er veel manieren zijn om een doel te bereiken, veel wegen leiden naar Rome, kan eenzelfde niveau van IT-beveiliging op verschillende wijze worden bereikt; er is dus niet een enkelvoudige van een beveiligde architectuur. Om deze reden moeten de essentiële punten worden genoemd die, in de zin van de huidige bruikbaarheid van IT-beveiliging, kunnen worden opgevat als State of the Art.

In elke specifieke situatie zijn de beveiligingsbehoeften afhankelijk van de specifieke applicatie. Volgens de ITSiG moeten de IT-beveiligingsdoelstellingen als beschikbaarheid, integriteit, vertrouwelijkheid en/of authenticiteit beschouwd worden, zelfs als ze worden geëvalueerd voor de afzonderlijke gevallen met verschillende beveiligingseisen. Dit betekent dat in het bijzonder rekening moet worden gehouden met de volgende beschermingsdoelstellingen:

- bescherming tegen aanvallen gericht op het ongeoorloofd lezen, wijzigen en/of verwijderen van verzonden en opgeslagen gegevens.
-
- bescherming tegen aanvallen op de beschikbaarheid van de respectievelijke diensten en gegevens bij exploitant en gebruiker
-
- bescherming tegen ongeoorloofde manipulatie van besturing- en applicatiesystemen, enz.

Aanvullend op het implementeren van adequate beschermingsmaatregelen, is het ook noodzakelijk dat aanvallen op IT-systemen, -diensten en -gegevens volgens de State of the Art worden gedetecteerd.

De functionaliteit voor het implementeren van de gewenste IT-beveiliging, moet altijd volledig en correct worden geïmplementeerd. Dit moet worden controleerbaar worden onderzocht door een onafhankelijke auditor. Bij de uitvoering moet altijd rekening worden gehouden met geavanceerde procedures, zoals:

- 2-factor-authenticatie (2FA);
- wederzijdse authenticatie;
- versleuteling van communicatie tijdens transport;
- versleuteling van gegevens (zoals tijdens opslag);
- beveiliging van de private-key tegen ongeoorloofd kopiëren;
- gebruik van veilige opstartprocessen;
- veilige software (Secure Software Design) inclusief patchbeheer;
- veilig gebruikersbeheer met actieve vergrendelingoptie;
- beveiligde toewijzing van netwerkzones voor extra beveiliging op netwerkniveau;
- veilige datacommunicatie tussen verschillende netwerkzones;
- veilig browsen op Internet;
- realisatie van het need-to-know principe;
- realisatie van de minimale aanpak (inclusief hardening);
- implementatie van logging, monitoring, reporting en respons management systemen;
- implementatie van bescherming tegen malware;

- gebruik van veilige back-upsystemen om te beschermen tegen gegevensverlies;
- meervoudig systeemontwerp voor de implementatie van hoge beschikbaarheid, enz.

Bovendien moet aanvullend op de afzonderlijke technische toepassingsfunctionaliteiten ook rekening gehouden worden met de volledige beveiligingsarchitectuur. Daartoe moeten in het kader van de eisen (Het BNetzA[20] eist het toepassen van een risico-inschatting Standaard en/of Kritisch voor kritieke processen en applicaties met betrekking tot de IT-beveiligingscatalogus en in overeenstemming met EnWG sectie 11) de volgende punten worden beoordeeld:

- De gebruiker moet kunnen zien onder welke voorwaarden hij het betreffende systeem in de betreffende veilige configuratie kan gebruiken. Als verschillende toepassingsscenario's mogelijk zijn op een apparaat (zoals toegang tot kantoor-IT via sessie-1 en toegang tot het proces via sessie-2), dan moet dit voor elk geval duidelijk aan de gebruiker worden zichtbaar zijn.

- Voor het product of de dienst moeten een holistische beveiligingsarchitectuur en bijbehorende documentatie voor evaluatie door onafhankelijke derde partijen aanwezig en geïmplementeerd zijn.
- De gebruikte versleuteling moet bij de tijd zijn en tot het einde van de levenscyclus van het product up-to-date en veilig zijn. Voor dit doel beveelt het BSI altijd (het gebruik van) up-to-date catalogi met geschikte algoritmen aan.
- Het gebruikte product en de gebruikte dienst mogen geen backdoors bevatten, die het mogelijk maken de gegevens en/of applicaties te lezen of zelfs te manipuleren.
- De fabrikant mag geen toegangsinterfaces hebben die onafhankelijk van de exploitant kunnen worden gebruikt.
- Het is raadzaam om de implementatie van de beveiligingsfunctie te laten controleren door een vertrouwde derde partij.
- De in de applicatie uitgevoerde processen (zoals gebruikersautorisatie, sleutelbeheer, enz.) moeten veilig toegewezen.

Om een product in termen van State of the Art te beoordelen, moet ook aan andere criteria worden voldaan, dit zijn:

- Voor het product of de dienst moet rekening gehouden worden met internationale normen en moet, voor zover deze worden gebruikt, inter-operabel zijn met standaardprotocollen.
- Als er sectorspecifieke normen zijn, dan moet daar rekening mee gehouden worden bij de implementatie.
- Het product of de dienst moet een storingsvrije werking van de componenten mogelijk maken (marktrijpheid / Markt Ready).
- Het product of de dienst moet in de praktijk met succes zijn getest.
- Bij de evaluatie moet ermee rekening gehouden worden dat de oplossing, als een koppeling bestaat van hardware en software, als geheel moet worden beschouwd.
- Het product moet veilig kunnen worden bijgewerkt in termen van beveiliging en toepassingsfunctionaliteit.

Bij het selecteren van een State of the Art oplossing is de fabrikant van betreffende oplossing ook onderworpen aan criteria waarmee rekening moet worden gehouden. De fabrikant kan de investeringszekerheid garanderen voor de betreffende uitvoering, dit betekent dat de volgende controles moeten worden uitgevoerd:

- De financiële achtergrond van de fabrikant garandeert verdere levenscycli voor het product.
- Voor het betreffende product is een vastgesteld productbeheer aanwezig en een roadmap voor de verdere ontwikkeling voor de gebruiksperiode van dat product.
- Het product is tijdens de gehele gebruiksperiode niet aangemerkt als product dat niet meer leverbaar is.
- De fabrikant reageert proactief op bekend geworden kwetsbaarheden die van invloed zijn op zijn product, herstelt deze binnen afzienbare tijde en stelt noodzakelijke software-updates snel beschikbaar.
- De fabrikant produceert de oplossing in een vertrouwde omgeving met vertrouwd personeel.
- De fabrikant beheerst zelfstandig de volledige veiligheidsfuncties en is met betrekking tot de

[20] Het Bundesnetzagentur is het Duitse Federale Netwerk Agentschap

veiligheidsfuncties niet afhankelijk van andere leveranciers.

Wanneer producten van derden worden gebruikt met een lager betrouwbaarheidsniveau, dan zorgen door de beveiligingsarchitectuur van het product en de maatregelen tijdens het productieproces bij de fabrikant ervoor dat de gehele beveiligingsarchitectuur in termen van gedefinieerde beveiligingsbehoeften in takt blijven.

3.2 Technische maatregelen

3.2.1 Beoordelen van de wachtwoordsterkte

De maatregel simuleert praktische aanvallen op veilig opgeslagen/gehashte inloginformatie en meet de objectieve veerkracht gebaseerd op wiskundige methoden, persoonlijk gedrag, enz. De maatregel maakt een grondige inventarisatie en evalueert alle - zelfs onbekende - wachtwoorden. De maatregel bepaalt de mate van conformiteit aan het interne bedrijfsbeleid en ondersteunt of faciliteert de implementatie van andere beveiligingsgerelateerde maatregelen, zoals, conform de GDPR, melden aan de werknemers, wanneer zij onveilige wachtwoorden gebruiken.

Tegen welke dreiging(en) wordt de maatregel ingezet?
De maatregel is bedoeld om het risico van misbruik van accountinformatie (toegangsgegevens) te voorkomen.

80% van de IT-beveiligingsincidenten die resulteren in het ontsluiten van accountinformatie en persoonlijke en zakelijke gegevens, konden worden verkregen als gevolg van zwakke en/of gestolen wachtwoorden (Verizon Report 2017).

Statisch wachtwoordbeleid voor gebruikersaccounts, en het naleven hiervan, is bewezen niet geschikt te zijn als maatregel voor het afdwingen van sterke, veilige wachtwoorden. Het wachtwoordbeleid creëert zo een schijnzekerheid.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?
Bedrijfsnetwerken gebruiken doorgaans een centrale opslag voor gebruikersreferenties die gebruikt worden om gebruikers, die toegang hebben tot services en/of werkstations (zoals Microsoft Active Directory), te verifiëren.

Alle moderne gegevensopslagsystemen gebruiken hash-functies voor wachtwoorden om te voorkomen dat een aanvaller, met toegang tot de centrale database, wachtwoorden met leesbare tekst kan herstellen.

Deze hash-functionaliteit biedt een cruciale bescherming van wachtwoorden tegen onbevoegde toegang, maar voorkomt ook dat een bedrijf de wachtwoorden evalueert. Dit is echter nodig om actie te ondernemen tegen mogelijke aanvallen, zoals het als wachtwoord uitproberen van woorden uit het woordenboek, het gebruik van bekende gecompromitteerde wachtwoorden of het raden van wachtwoorden gebaseerd op persoonlijke informatie over het doelwit.

De wachtwoord beveiligingsbeoordeling definieert de weerbaarheid van wachtwoorden door een werkelijke aanval te simuleren die verschillende mogelijke kwetsbaarheden gebruikt en exploiteert, zoals voorspelbare/zwakke wachtwoorden, wachtwoorden die door meerdere gebruikers worden gebruikt, gebrekkige toepassing van cryptografie, enz.

Op deze manier worden verkregen wachtwoorden verwerkt volgens nationale, regionale en interne regels voor gegevensbescherming, zonder informatie over specifieke gebruikers of wachtwoorden openbaar te maken of op te slaan.

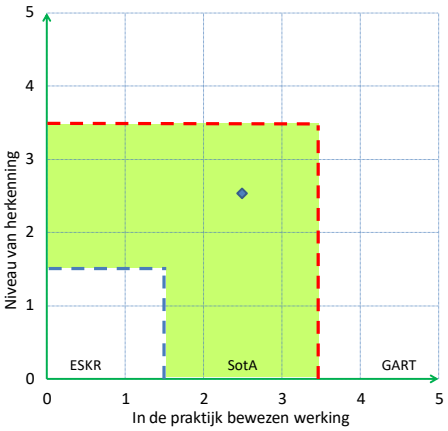
Ontvangen wachtwoorden worden vervolgens beoordeeld gebaseerd op objectieve wiskundige en structurele entropie en subjectieve criteria (het naleven van de wachtwoordrichtlijnen). Zodra de beoordeling is voltooid, worden de leesbare (niet versleutelde) platte tekst wachtwoorden verwijderd en wordt een zinvol rapport gegenereerd.

De resultaten van de wachtwoordbeveiliging assessment (het auditrapport) stellen de organisatie in staat om de exacte veiligheidsrisico's van de wachtwoorden, die worden gebruikt in verschillende veelvoudige en heterogene systemen, te meten. Zo kunnen de beste bewustmaking- en opleidingsmaatregelen voor gebruikers worden gedefinieerd en kunnen centrale handhaving procedures worden geïdentificeerd voor sterke wachtwoorden. Dit maakt het ook mogelijk de doeltreffendheid van al bestaande maatregelen te herzien en te verbeteren.

Welke beschermingsdoelstellingen dekt deze maatregel af?

☐ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☒ Authenticiteit

Classificatie van het technologieniveau



3.2.2 Afdwingen van sterke wachtwoorden

De maatregel dwingt het gebruik van sterke en veilige wachtwoorden af voor alle technische en organisatorische maatregelen die door de organisatie worden gebruikt.

De sterkte van het wachtwoord wordt door middel van een controlemechanisme aangepast aan het beveiligingsniveau van het betreffende gebruikersaccount. Het gedefinieerde beveiligingsniveau is gebaseerd op de potentiële gevolgen van een inbreuk op de beveiliging van het account.

Tegen welke dreiging(en) wordt de maatregel ingezet?

80% van de IT-beveiligingsincidenten die leiden tot in openbaarmaking van accountinformatie - privé, persoonlijke gegevens en bedrijfsgegevens - kunnen worden toegeschreven aan zwakke en/of gestolen wachtwoorden (Verizon Report 2017).

Het is bewezen, dat het naleven van het statische wachtwoordbeleid voor gebruikersaccounts geen adequate maatregel is voor de handhaving van sterke, veilige wachtwoorden; de wachtwoordrichtlijn geeft een schijnzekerheid wat betreft het beveiligingsniveau.

De beschreven maatregel verhoogt het beveiligingsniveau van de wachtwoorden die worden gebruikt voor een niveau dat overeenkomt met het beveiligingsrisico (controle en detectie).

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?

Nieuw ingestelde wachtwoorden worden gecontroleerd op basis van de set regels die zijn toegewezen aan elk account en worden afzonderlijk geparametriseerd voor de verschillende categorieën.

De regels omvatten eisen voor: compositie (lengte, tekenset, symbolen, tekenreeksen en herhalingen), wiskundige en structurele entropiewaarden, uniciteit (het wachtwoord mag niet op hetzelfde systeem in de organisatie worden gebruikt door een ander account), het gebruik van bekende standaard wachtwoorden en het hergebruik van wachtwoorden (historisch). De regels zijn niet beperkt tot blacklisting, maar kunnen afzonderlijk worden geparametriseerd.

De oplossing zal centraal binnen de organisatie worden gebruikt en beheerd via een enkele interface voor alle systemen; dit zorgt voor effectiviteit van het coherente en systeembrede beleid. Het voorkomt ook meervoudig gebruik van wachtwoorden in de verschillende systemen en maakt het mogelijk om de wachtwoordgeschiedenis centraal bij te houden.

Gegevens met leesbare tekst worden nooit opgeslagen of weergegeven. De eindgebruiker krijgt een duidelijk bericht met toelichting op de reden waarom het nieuwe wachtwoord wordt geweigerd. Dit ontlast de Helpdesk en beschermt de privacy van de gebruiker.

Alle communicatie voor het afdwingen van sterke wachtwoorden tussen servers en systemen is beveiligd met behulp van versleuteling.

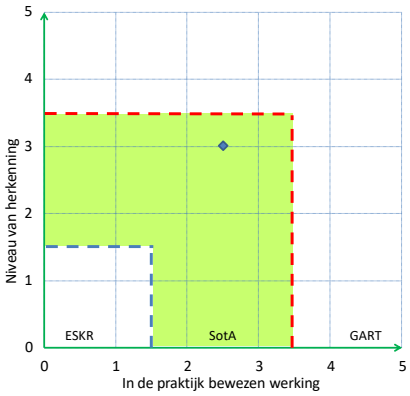
De beschreven maatregel leidt voor elke situatie tot het centraal afdwingen van een adequate wachtwoordsterkte en geeft de organisatie volledige supervisie, controle en documentatie van de wachtwoorden die in de organisatie worden gebruikt. Bovendien kan daardoor een passend beveiligingsniveau voor authenticatie bereikt worden.

Handhaving moet worden geëvalueerd door middel van een maatregel voor het beoordelen en evalueren van wachtwoorden. Van de gebruikte wachtwoorden moet de veerkracht tegen daadwerkelijke aanvallen worden gemeten en vastgesteld en of de regels net zo effectief zijn als verwacht, of dat ze moeten worden bijgesteld om, zoals de omstandigheden dit vereisen, te voorkomen dat zwakke wachtwoorden worden gebruikt.

Welke beschermingsdoelstellingen dekt deze maatregel af?

☐ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☒ Authenticiteit

Classificatie van het technologieniveau



3.2.3 Multi-factor authenticatie

Multi-factor authenticatie (MFA) en Two-factor authenticatie (2FA) zijn verificatieprocessen waarbij meer dan één factor, zoals het wachtwoord, wordt gebruikt om authenticatie objecten veilig te verifiëren. Een MFA- of 2FA-oplossing zorgt ervoor dat het authenticatie object ook echt het authenticatie object is. Deze maatregel wordt, in een volledig onderling verbonden wereld en naarmate de betekenis en mogelijkheden voor toegang tot digitale identiteiten toenemen, steeds belangrijker. De mogelijkheden van moderne MFA-systemen en om digitale transacties te beveiligen spelen ook een interessante rol in de toenemende digitalisering en strengere regelgeving, zoals de EU-richtlijn betalingsdiensten 2 (Payment Service Directive 2, PSD2)

Tegen welke dreiging(en) wordt de maatregel ingezet?

Volgens het Verizon 2017 Data Breach Investigations Report[21] is meer dan 81% van de gecompromitteerde situaties te wijten aan zwakke en/of gestolen wachtwoorden.

[21] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017

Gestolen of zwakke wachtwoorden zijn momenteel de oorzaak van het compromitteren in meer dan 80 procent van alle gevallen. Dit komt omdat wachtwoorden niet empirisch beschermen digitale identiteiten. De redenen hiervoor zijn:

1. Aanvallers kunnen al met 10 gokpogingen, dus binnen de typische goklimiet, al één procent[22] van alle gebruikersaccounts overnemen.

2. Met gebruik van openbare informatie, zoals die van sociale media (gericht raden) meegerekend, maakt aanvallen, om de digitale identiteit over te nemen, mogelijk met een waarschijnlijkheid van 32% (gebruikers met een beveiligingsbewustzijn) tot 73% (normale gebruikers)[23].

3. Bovendien maken gebruikers over het algemeen gebruik van hetzelfde patroon voor het maken van hun wachtwoorden, waardoor de werkelijke wachtwoordruimte in vergelijking met de potentiële theoretische wachtwoordruimte[24] aanzienlijk wordt verkleind. Voorbeelden van patronen zijn:

a. xxxxxnn
een hoofdletter, kleine letter, kleine letter, kleine letter, kleine letter, cijfers en cijfer
b. xxxxxxnn
hoofdletter, kleine letter, kleine letter, kleine letter, kleine letter, kleine letter, cijfer en cijfer
c. xxxxnnnn
hoofdletter, kleine letter, kleine letter, kleine letter, cijfer, cijfer, cijfer en cijfer
d. xxxxxnn!, xxxxxxnn!, xxxxnnnn!
bovenstaande combinaties met een "!" aan het eind.

Daarbij komt dat veel gebruikers hun wachtwoorden hergebruiken voor meerdere applicaties (per gebruiker gemiddeld vijf wachtwoorden voor 26 accounts). Het compromitteren van een van deze diensten leidt al snel tot het compromitteren van alle diensten. Aanvallers proberen systematisch en geautomatiseerd de gepakte gegevens uit op de verschillende diensten. Hoe langer de aanvaller onontdekt blijft, des te meer gegevens kan hij verzamelen en daarmee resultaten boeken en schade aanrichten.

Het gebruik van MFA- of 2FA-systemen reduceert het risico aanzienlijk, dat een aanvaller met een wachtwoord een digitale identiteit kan misbruiken of toegang kan krijgen tot de gegevens die daarmee toegankelijk zijn.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?
MFA en 2FA maken identiteitsdiefstal veel moeilijker. Deze procedures vereisen traditioneel dat aanvullend op het wachtwoord ten minste aan één ander verificatiecriterium (authenticatiefactor) moet worden gegeven, voordat toegang tot een pagina, applicatie of bepaalde gegevens wordt verleend. Een eenvoudige 2FA vereist daarom twee van de volgende drie criteria:

- iets dat de gebruiker weet (zoals een wachtwoord);
- iets (hardware of digitaal) wat de gebruiker meebrengt (zoals een bankkaart of een authenticatie token);
- iets specifieks voor de gebruiker met biometrische identificatiemiddelen (zoals een vingerafdruk of irispatroon);
- iets wat het systeem weet van de gebruiker. (zoals geolocatie, apparaat-ID, tijdsperioden, eerdere transacties).

Moderne multi-factor authenticatie systemen bieden een breed scala aan toepassingen:

1. ondersteuning van verschillende soorten tokens (software, hardware, SMS, spraak, mOTP) die afhankelijk van doel en risico kunnen worden geconfigureerd voor verschillende doelgroepen;

[22] http://www.jbonneau.com/doc/B12-IEEESP-analyzing_70M_anonymized_passwords.pdf
[23] http://www.comp.lancs.ac.uk/~yanj2/ccs16.pdf
[24] https://www.youtube.com/watch?v=5i_Im6JntPQ en https://youtu.be/zUM7i8fsf0g

2. ondersteuning van scenario's van derden met de mogelijkheid om de geldigheid van een token type te beperken in termen van aantal applicaties of tijdsduur;

3. ondersteuning van transacties verbonden tokens. Deze tokens worden alleen gebruikt in combinatie met moderne MFA/2FA-oplossingen en maken het mogelijk processen te beschermen door een eenmalig een wachtwoord (OTP) te genereren op basis van transactiegegevens zoals vereist voor PSD2. Op deze manier kan, naast vertrouwelijkheid en integriteit, de onweerlegbaarheid worden gegarandeerd (non-repudiation).

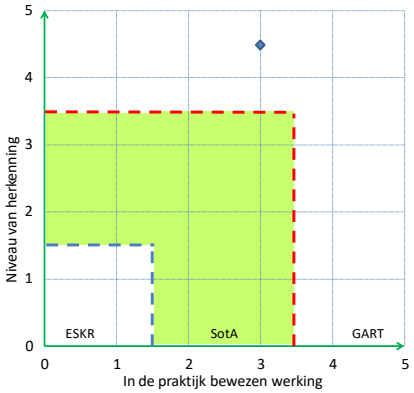
Moderne MFA- en 2FA-systemen kunnen eenvoudig worden geïntegreerd. Door het gebruik van standaardkoppelingen met een Actieve Directory, LDAP, SQL of JSON kunnen applicaties snel worden uitgebreid met een MFA- of 2FA-onderdelen en de daarin beheerde gebruikers worden beschermd. Moderne API's kunnen zeer snel en met slechts enkele regels code worden gebruikt om interne ontwikkelingen, customized software en portals te beschermen.

De moderne transactie tokens maken het mogelijk een hoog niveau van gebruiksvriendelijkheid te realiseren en tegelijkertijd onweerlegbaarheid te garanderen. In dit proces ontvangt de gebruiker een bericht op zijn smartphone met de vraag om de login of kritieke actie in het systeem een tweede keer goed te keuren door op OK te drukken op hun smartphone. Door het gebruik van openbare sleutelmechanismen te combineren met QR-codes, kunnen deze procedures ook worden gebruikt voor toegang tot apparaten en voor offline authenticatie.

Welke beschermingsdoelstellingen dekt deze maatregel af?

☐ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☒ Authenticiteit

Classificatie van het technologieniveau



Opmerking: vooral de voortdurende innovatie en de hoge mate van doeltreffendheid van de maatregel bij het voorkomen van het verlies van digitale identiteiten, resulteren in de hier gemaakte beoordeling in de praktijk bewezen.

3.2.4 Cryptografische methoden

Cryptografische methoden, zoals methoden voor het versleutelen en ondertekenen van gegevens, zijn in wezen afhankelijk van de configuratie, de gebruikte procedure en de sleutellengten. Alleen door de combinatie van alle drie de drie factoren kunnen de beschermingsdoelstellingen in termen van vertrouwelijkheid, integriteit en authenticiteit worden gerealiseerd. Dit hoofdstuk bevat aanbevelingen voor de keuze en het gebruik van cryptografische methoden.

Cryptografische methoden worden voor verschillende doeleinden gebruikt en vormen de basis voor veel IT- beschermingsmaatregelen. Moderne cryptografie wordt gebruikt in:

- authenticatie procedures;
- waarborgen van de authenticiteit;
- toegangscontrole;

- implementatie van weerlegbaarheid en onweerlegbaarheid;
- delen van geheimen;
- implementeren van anonimisering procedures;
- selectie en afstemming (committment procedures);
- crypto-currencies;
- Digital Rights Management (DRM);
- en veel andere scenario's.

Al deze procedures hebben gemeen dat zij in de eerste plaats bedoeld zijn om de vertrouwelijkheid en authenticiteit te waarborgen. Bijvoorbeeld om diefstal van vertrouwelijke gegevens en om ongemerkte manipulatie van gegevens te voorkomen.

Cryptografische methoden zijn bedoeld om voldoen aan het beginsel van Kerckhoff. Open algoritmen kunnen door een grote, wereldwijde gemeenschap van experts systematisch worden geëvalueerd op zwakke punten en worden geoptimaliseerd. Ongeveer op deze wijze is de huidige standaard voor symmetrische codering (AES) ontstaan in een openbare competitie. Het wordt beschouwd als uiterst veilig.

Het beveiligingsniveau van een versleutelingmethode duidt op de inspanning aan die een aanvaller moet leveren om leesbare tekst te krijgen. Simpel gezegd groeit de inspanning met het aantal beschikbare opties voor het kiezen van de sleutel (de bitlengte).

Als gevolg van het toenemen van de rekenkracht, analytische vooruitgang en technische mogelijkheden bestaat het risico dat een aanval op een cryptografische methode bekend raakt en het beschermingsniveau daarmee tot het niveau praktisch haalbaar daalt. Ook is het mogelijk dat iemand erin slaagt een kwantumcomputer te bouwen die een brute force zoekopdracht in veel kortere tijd kan uitvoeren en dat daarmee het beschermingsniveau voor de symmetrische procedure wordt gehalveerd. Veel asymmetrische methoden kunnen volledig worden gekraakt met behulp van de beschikbare kwantumcomputers.

Om deze redenen moeten de gebruikte cryptografische methoden ongeveer één keer per jaar op effectiviteit worden gecontroleerd.

De huidige versie van de aanbevelingen wordt door het BSI gepubliceerd als TR-02102[25][26]. Verdere aanbevelingen zijn te vinden in documenten van de Amerikaanse NIST, ENISA en andere organisaties[27].

Op dit moment kunnen in het bijzonder de volgende aanbevelingen worden gedaan:

- Symmetrische coderingsmethoden: AES-128, AES-192, AES-256 idealiter met GCM als bedrijfsmodus. EAX-modus wordt ook aanbevolen als omwille van resources een stream cypher vereist is en een iets grotere vertraging als gevolg van het versleutelen acceptabel is. Als modus operandi moet in moderne systemen Authenticated Encryption met Associated Data (AEAD) worden gebruikt. Over het algemeen worden bedrijfsmodi zonder extra berichtverificatie (Message Authentication Code of MAC) zonder aanvullende integriteitbescherming als onveilig beschouwd en mogen niet worden gebruikt.
- Asymmetrische versleutelingmethoden: ten minste ECIES-250, DLIES-2000, RSA 2000, curve25519, curve448 of ECC Brainpool. ECIES moet worden gebruikt met 384 of meer bits. Als DLIES of RSA wordt gebruikt, moet 3072 bits of meer bits worden gebruikt.
- Hash-functies: let op SHA-256, SHA-384, SHA-512, SHA3-256, SHA3-384 en SHA3-512.

[25] TR staat voor technische richtlijnen
[26] Zie: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html (Engelse versie: https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/tr02102/tr02102_node.html)
[27] BSI TR-02102-1 "Cryptographic Mechanisms: Recommendations and Key Lengths" versie: 2018-02,
NIST Special Publication 800-57 Part 1 Revision 4: Recommendation for Key Management Part 1: General,
NIST Special Publication 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms,
EU Agency for Network and Information Security: Algorithms, key size and parameters report – 2014,
https://eprint.iacr.org/2015/1018.pdf,
https://safecurves.cr.yp.to/

De SHA1- en MD5-algoritmen zijn niet langer State of the Art.

- Sleutelafleiding functies (KDF) en wachtwoord-hashes: Huidige geschikte algoritmen zijn[28]: Argon2, PBKDF2, scrypt en bcrypt. Nieuwe systemen moeten het Argon2-algoritme gebruiken.
- Willekeurige getalgeneratoren:
  - fysieke generatoren voor willekeurige getallen, functionaliteitklasse PTG.2 of PTG.3[29];
  - deterministische generatoren voor willekeurige getallen, functionaliteitklasse DRG.3 en DRG.4.
- TLS[30][31]: TLS 1.3 gecombineerd met forward secrecy met behulp van beveiligde algoritmen volgens BSI TR-02102-2 tabel 1[32]. Het gebruik van hulpmiddelen zoals: https://www.owasp.org/index.php/O-Saft en https://www.ssllabs.com/ssltest/ helpt bij het inspecteren van de TLS-configuratie.

Opmerking:
Side-channel aanvallers vormen een relevant probleem voor cryptografie. De keuze van 'aanbevolen' algoritmen beschermt wel tegen analytische aanvallen, maar niet tegen side-channel aanvallen. Deze aanvallen worden meestal uitgevoerd door het meten van fysieke parameters, zoals looptijd, energieverbruik, warmte en trillingen.

Potentiële side-channels zijn vooral afhankelijk van het toegepaste algoritme en het gebruikte platform. De side-channel-bestendigheid van IT-beveiligingsproducten varieert per provider. Werk bij twijfel samen met gespecialiseerde dienstverleners.

3.2.5 Versleuteling van harde schijven

Het volledig versleutelen van de harde schijf, volledige schijfversleuteling, beschermt de op een systeem geïnstalleerde gegevensdragers, zoals magnetische harde schijven en op flashgeheugen gebaseerde SSD's, tegen ongeautoriseerde toegang (lezen, wijzigen) door derden. De daar opgeslagen informatie is pas als gewone tekst toegankelijk, als de gebruiker is geauthenticeerd voordat het besturingssysteem van de PC- of smartphone is opgestart.

Tegen welke dreiging(en) wordt de maatregel ingezet?
Deze maatregel beschermt gegevens op vaste schijven van onbeheerde, uitgeschakelde apparatuur, zoals Pc's, laptops, tablets of smartphones (Data at rest). In geval van verlies als gevolg van onoplettendheid of diefstal, of tijdelijke beschikbaarheid voor onbevoegde derden (hotelkamers), kunnen aanvallers de inhoud van de opgeslagen informatie niet inzien of manipuleren. Het kopiëren van de Read-Only geheugens, van de apparaten die op deze manier zijn beschermd, levert alleen nutteloze gegevens op, omdat het is versleuteld.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?
De gegevensdragers die in een systeem zijn geïnstalleerd, zoals magnetische harde schijven of op flashgeheugen gebaseerde SSD's, die het besturingssysteem en/of gevoelige bedrijfsvertrouwelijke gegevens bevatten, worden met maatregelen zodanig versleuteld, ongeautoriseerd lezen hiervan geen leesbare tekst oplevert. Dit is van toepassing op het lezen van de schijf wanneer het systeem is uitgeschakeld of wanneer de harde schijf is verwijderd en ook tijdens het gebruik tegen het aftappen van gegevens aan de interfacezijde van de interne schijf (eSATA, enz.).

In de XTS-modus moet voor symmetrische codering ten minste AES-256 worden gekozen. Een centrale beheerapplicatie vergemakkelijkt het op alle PC's binnen de organisatie toepassen van encryptie aanzienlijk. De cryptografische sleutels mogen nooit in de cloud worden opgeslagen, ook niet voor back-updoeleinden.

---

[28] https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet

[29] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.pdf

[30] Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths Part 2 - Use of Transport Layer Security (TLS)

[31] NIST Special Publication 800-52 Revision 1 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

[32] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf (Englisch version: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-2.pdf)

Bij het kiezen van authenticatiefactoren is het belangrijk om wachtwoorden te kiezen die moeilijk te kraken zijn en gebruik te maken van 2-factor authenticatie, idealiter gebaseerd op kennis en eigendom of met extra tokens. Dit maakt het ook mogelijk om gebruik te maken van hardwareondersteunde vertragingsmechanismen wanneer meerdere keren een onjuist wachtwoord wordt ingevoerd. Dit maakt het zinloos om gegevensdragers te verwijderen om ze in een systeem van een aanvaller te analyseren.

Voor zover het apparaat het toelaat, zoals met Windows 10-systemen, moet ook de zogenaamde Secure boot worden ondersteund. Dit beschermt het hele opstartproces, inclusief 2-factor authenticatie, tegen manipulatie en behoudt de integriteit van het systeem en de encryptie mechanismen.

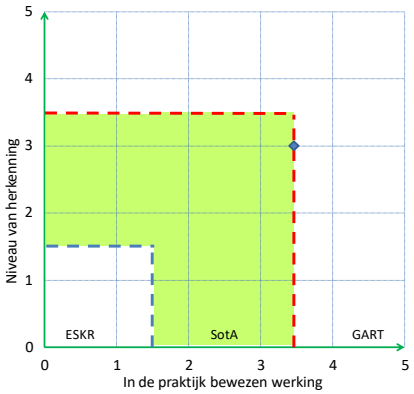
Sommige beschikbare oplossingen ondersteunen ook volledige of op mappen gebaseerde (folder-based) versleuteling van verwisselbare schijven. Binnen organisaties heeft een geautomatiseerde, gebruikerstransparante versleuteling van bedrijfsgegevens de voorkeur om te voorkomen dat gewone tekst wordt opgeslagen als gevolg van bedieningsfouten.

De door BSI voor gebruik door overheidsinstanties goedgekeurde, maar ook in kritieke infrastructuren en bedrijven bruikbare oplossingen zijn beschikbaar voor Windows 7, 8 en 10.

Welke beschermingsdoelstellingen dekt deze maatregel af?

☐ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☐ Authenticiteit

Classificatie van het technologieniveau



3.2.6 Versleuteling van bestanden en mappen

Versleuteling van bestanden en mappen omvat de versleuteling van afzonderlijke objecten, zoals containers, folders of afzonderlijke bestanden, daarom wordt dit type encryptie ook wel object versleuteling genoemd. De voor dit doel beschikbare programma's werken vaak transparant, wat betekent dat gebruikers met de objecten kunnen werken alsof ze niet-versleuteld zijn.

Object versleuteling biedt de mogelijkheid om bestanden en mappen veilig van de ene locatie naar de andere te transporteren en te voorkomen dat onbevoegde gebruikers toegang krijgen. Het is daarom noodzakelijk om ervoor te zorgen dat niemand anders dan de bevoegde personen toegang heeft tot de beschermde informatie. Daarom is het belangrijk ervoor te zorgen dat niemand, anders dan de bevoegde personen toegang hebben tot de beschermde informatie. Dit kan persoonlijke gegevens in gevaar brengen of, in het ergste geval het voortbestaan van de organisatie.

Bovendien is object versleuteling een ideaal hulpmiddel bij het gebruik van clouddiensten, omdat het effectief voorkomt dat de exploitanten de gegevens kan inzien.

Tegen welke dreiging(en) wordt de maatregel ingezet?

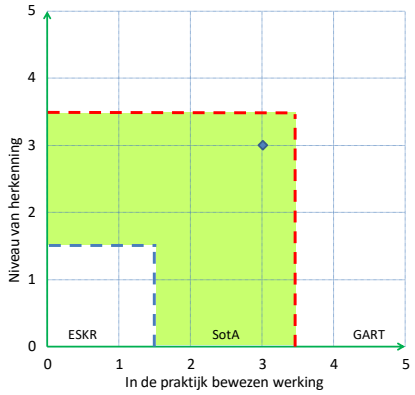
1. onderscheppen en misbruik van gegevens tijdens transport, zoals via e-mail;
2. verlies en diefstal van verwijderbare media, gevolgd door ongeoorloofde toegang tot gevoelige gegevens;
3. misbruik van gegevens die zijn opgeslagen in de cloud.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?
Bestand- en mapversleuteling omvat de versleuteling van individuele objecten, zoals containers, folders/mappen of individuele bestanden. Daarom wordt dit type versleuteling ook wel objectversleuteling of object encryption genoemd. De programma's die voor dit doel beschikbaar zijn, werken vaak transparant, wat betekent dat de gebruiker met de objecten kan werken alsof ze niet-versleuteld zijn.

Object versleuteling biedt de mogelijkheid om bestanden en mappen veilig van de ene naar de andere locatie te transporteren, om ze op elke locatie veilig op te slaan en om toegang door onbevoegden te voorkomen.

Welke beschermingsdoelstellingen dekt deze maatregel af?
☐ Beschikbaarheid
☐ Integriteit
☒ Vertrouwelijkheid
☐ Authenticiteit

Classificatie van het technologieniveau



3.2.7 E-mailversleuteling
Zakelijke e-mailberichten bevatten vaak belangrijke en gevoelige gegevens en ook zijn e-mailadressen meestal gepersonaliseerd; e-mailberichten bevatten in het algemeen persoonsgegevens die beschermd moeten worden tegen ongeoorloofde toegang of wijziging. De beschermingsdoelstellingen kunnen doorgaans worden bereikt door het verzenden van e-mailberichten en e-mailinhoud te versleutelen.

Tegen welke dreiging(en) wordt de maatregel ingezet?

- het bespioneren of manipuleren van e-mailberichten tijdens transport;
- het bespioneren of manipuleren van opgeslagen e-mailberichten.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?
Versleuteling van het verzenden van e-mails (transport versleuteling of TIS)
Versleuteling van de inhoud van e-mails (S/MIME of PGP)

De beveiligingseisen voor e-mail worden onder meer bepaald door het type gegevens dat wordt verzonden en in het e-mail systeem worden opgeslagen. Bij zakelijke transacties kan men in het algemeen ervan uitgaan, dat e-mails op z'n minst voor het bedrijf belangrijke informatie bevatten. Bovendien worden e-mailadressen, indien gepersonaliseerd, nog steeds als persoonsgegevens beschouwd; daarom kan ervan worden uitgegaan dat via e-mailberichten persoonsgegevens worden doorgegeven en opgeslagen. In individuele gevallen en afhankelijk van het gebruik van e-mail kunnen

ook gegevens met speciale beschermingseisen, zoals gegevens over gezondheid en cliëntgegevens, zoals van advocaten of bijzonder waardevolle bedrijfsgeheimen zoals ontwerpgegevens worden verzonden.

Dit resulteert in de volgende beveiligingseisen voor e-mail:
- bescherming tegen ongeoorloofde toegang tot en/of wijziging van e-mailberichten tijdens vervoer en opslag (beschermingsdoel: vertrouwelijkheid);
- bescherming tegen latere wijzigingen van voor lange termijn gearchiveerde e-mailberichten (beschermingsdoel: integriteit).

Deze beschermingsdoelstellingen kunnen doorgaans bereikt door versleuteling toe te passen. Bij het versleutelen van e-mailberichten, moet een onderscheid worden gemaakt tussen versleuteling tijdens de overdracht (transport versleuteling) en versleuteling van de e-mail zelf (end-to-end encryptie). De beschermingsdoelstellingen vereisen noodzakelijkerwijs minstens het gebruik van transportversleuteling, althans bij het verzenden van e-mailberichten via openbare netwerken. De protocollen die worden gebruikt bij het verzenden van e-mailberichten via het Internet, namelijk SMTP, POP3 en IMAP, bieden echter in hun basisvorm ongecodeerde gegevensoverdracht Dit is waarschijnlijk de reden waarom grote delen van het e-mailverkeer nog steeds ongecodeerd worden verzonden, ook al zijn er al lang voldoende hulpprogramma's beschikbaar zijn om e-mail te versleutelen.

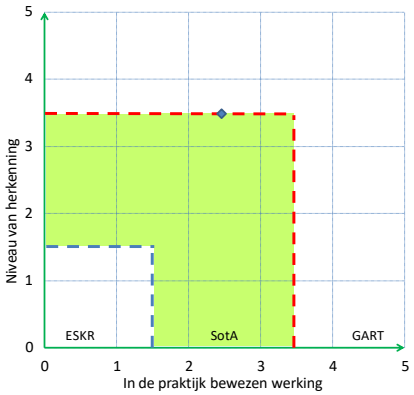
Voor de transportversleuteling van e-mailverkeer moet gebruik worden gemaakt van de huidige versie transportversleuteling (TLS Transport Layer Security) ingezet worden, dit is versie TLS 1.2, gedefinieerd in RFC 5246.Voor de inzet moeten versleutelingmethoden (zoals AES-256) worden toegepast; onveilige versleutelingmethoden (zoals RC4) mogen niet (meer) worden gebruikt. Als algemene maatregel moet Forward Secrecy worden geactiveerd. Daarnaast is het zinvol om de bij TLS gebruikte certificaten te controleren op authenticiteit en geldigheid, zoals met DANE (RFC 7671). Een uitgebreide lijst van aanbevelingen voor TLS is te vinden in de technische richtlijn TR-02102-02, deel 2 van het BSI.

Om bijzonder gevoelige gegevens te beschermen wordt end-to-end versleuteling aanbevolen. Hiervoor zijn twee standaarden vastgesteld: S/MIME (Secure/Multipurpose Internet Mail Extensions, gedefinieerd in RFC 5751) en OpenPGP (Pretty Good Privacy, gedefinieerd in RFC 4880). Beide standaarden gebruiken in principe dezelfde cryptografische technieken, ze verschillen echter in het certificeren van openbare sleutels en dus in het vertrouwelijkheidmodel en zijn niet compatibel met elkaar.

Bij end-to-end versleuteling, heeft geen enkel systeem in het transmissiepad toegang tot de inhoud van het e-mailbericht. Dit betekent echter dat het gebruik van inhoudsfilters, antivirus programma's, anti-spam, preventie van gegevensverlies en archivering volledig wordt geëlimineerd. Daarom kan content versleuteling alleen zinvol worden gebruikt tussen organisaties; d.w.z. dat e-mail berichten worden versleuteld en gedecodeerd in het koppelvlak (de overgang) van het openbare Internet en het particuliere netwerk van de organisatie (gateway) (end-to-end encryptie van de organisatie), of indien nodig gecombineerd met interne versleuteling van de content.

Welke beschermingsdoelstellingen dekt deze maatregel af?
- ☐ Beschikbaarheid
- ☒ Integriteit
- ☒ Vertrouwelijkheid
- ☒ Authenticiteit

Classificatie van het technologieniveau



3.2.8 Beveiligen van elektronisch dataverkeer met PKI

In het elektronische dataverkeer is het belangrijk dat de identiteit van de communicatiepartners en de authenticiteit van de verzonden inhoud gewaarborgd zijn. De verificatie van de elektronische identiteit van personen, organisaties en apparaten kan worden gewaarborgd met 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 versleuteling van het gegevenstransport. Al deze scenario's vereisen een component voor het genereren, beheren en inspecteren van elektronische certificaten die op betrouwbare wijze het bewijs van elektronische identiteiten garandeert: een openbare sleutel infrastructuur (Public Key Infrastructure of PKI).

De eIDAS-verordening[33], die sinds zomer 2016 van kracht is, bepaalt ook het gebruik van PKI.

Tegen welke dreiging(en) wordt de maatregel ingezet?

- identiteitsdiefstal / voorwendsel van een valse identiteit;
- manipulatie van de inhoud van digitale berichten of bestanden;
- manipulatie van de timing van berichten of bestanden.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?

De volgende maatregelen zijn zinvol voor de hierboven beschreven dreigingen:

- het maken van een interne PKI of het gebruiken maken van een externe PKI;
- het gebruik van digitale handtekeningen (handtekeningen, certificaten, stempels) van een erkend Trust Center;
- het gebruik van gekwalificeerde tijdstempels om de authenticiteit en timing van berichten en documenten te bewijzen.

De digitale certificaten worden uitgegeven door de zo genoemde certificeringinstantie (Certificate Authority of CA) van een PKI-organisatie. De geldigheid van openbare sleutels wordt bevestigd door de digitale handtekeningen van de CA. Naast de sleutel zelf bevat het digitale certificaat ook andere informatie, zoals de geldigheidsduur, enz. Als verantwoordelijke instantie is de CA het centrale component van de PKI-infrastructuur. Om de betrouwbaarheid van de CA te handhaven, moet de identiteit van de aanvrager, ongeacht of het om een persoon of organisatie gaat, worden onderworpen aan een ondubbelzinnige inspectie voordat het elektronische certificaat wordt afgegeven. Dit wordt gedaan door de registratieautoriteit (RA).

Een validatie service of validatie autoriteit (VA) is vereist om de geldigheid van digitale certificaten te controleren. Doorgaans wordt een onderscheid gemaakt tussen de controle aan de hand van een gepubliceerde certificate revocation list (CRL) en real-time validatie via een Online Certificate Status Protocol Service (OCSP). De keuze van het type validatie check wordt meestal per geval gebaseerd op het toepassingsscenario.

[33] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex:32014R0910

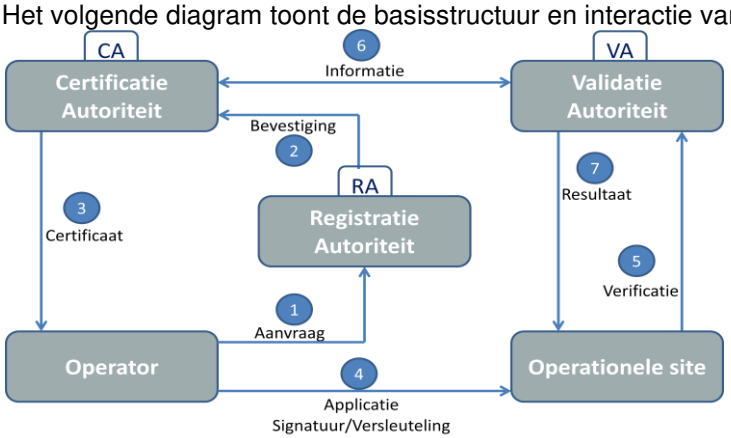
Afhankelijk van de juridische status van de PKI is voor de meeste gebruikssituaties de wettelijk toegestane logging van alle transacties in een PKI zinvol of zelfs noodzakelijk. Voor bepaalde toepassingsgebieden zijn ook gecertificeerde CA-producten vereist.

De toepassingsmogelijkheden van op PKI gebaseerde methoden zijn divers. Als voorbeeld worden de volgende werkwijzen genoemd:

- handtekening en versleuteling van e-mailberichten (S/MIME);
- authenticatie en versleuteling in het Internet der dingen (IoT);
- authenticatie en versleuteling op het Internet (HTTPS);
- authenticatie en versleuteling voor VPN-services;
- authenticatie- en bescherming van de integriteit voor uitvoerbare code (code signing);
- authenticatie- en bescherming van de integriteit voor documenten (digital signature);
- authenticatie van gebruikers/clients op het Internet.

Afhankelijk van de status van de exploitanten en de beveiligingsstandaard van het bijbehorend datacenter, kan een breed scala aan oplossingen worden opgebouwd. Dit varieert van een Root-CA als een zo genoemd vertrouwensanker tot een strikt hiërarchische PKI met meerdere sub-CA's. Ook kan een crosscertificering met andere PKI's worden geïmplementeerd.

Het volgende diagram toont de basisstructuur en interactie van de PKI-componenten in een workflow.



Het gebruik van certificaten is voor bijna alle gebieden zinvol en nuttig. Naast toepassingsgebieden in de publieke sector zijn ze ook te vinden in de energie- en gasvoorziening, e-justitie (met beA, beN, beBPO), de gezondheidszorg, de industrie en non-profit sector (zoals federaties en verenigingen).

De eIDAS-verordening bepaalt specifiek in een uitgebreide reeks gebruiksscenario's. Zo worden o.a. identiteitscontroles en trust services ondersteund door de PKI's (zie onderstaande tabel).

eIDAS voorschriften/toepassingsgevallen	
Identiteiten	Certificaten
	Elektronische ID's
Vertrouwensdiensten (Trust services)	Elektronische stempels (Electronic stamps)
	Elektronische tijdstempels (Time stamps)
	Website authenticatie
	Elektronische bezorgdiensten (Delivery services)
	Bewakingsdiensten (Preservation services)

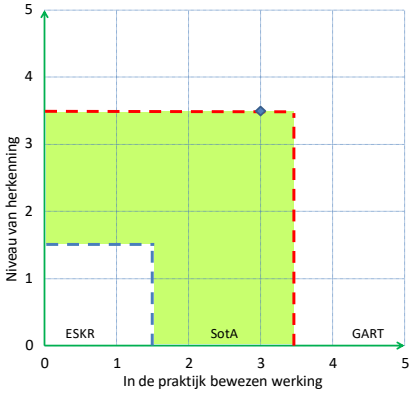
Een voorbeeld van gebruik in de publieke sector is: www.cio.bund.de/Web/DE/IT-Angebot/IT-Beratungsdienstleistungen/Public-Key-Infrastruktur-der-Verwaltung/public_key_node.html, in de energievoorziening sector: www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/PKI/pki_node.html en bij TeleTrust:

https://www.ebca.de.

Welke beschermingsdoelstellingen dekt deze maatregel af?

☐ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☒ Authenticiteit

Classificatie van het technologieniveau



3.2.9 Gebruik van VPN (Layer 3)

Een Layer 3 VPN beschrijft de verbinding van twee of meer netwerken op Layer 3 van het OSI-model[34]. De verzonden gegevens worden versleuteld. Hierdoor kunnen bijvoorbeeld bedrijfsfilialen in verschillende landen veilig en vertrouwelijk via Internet met elkaar worden verbonden.

Tegen welke dreiging(en) wordt de maatregel ingezet?

Het gebruik van VPN's beschermt tegen:

- verlies van vertrouwelijkheid door niet/zwak versleutelde verbindingen;
- externe aanvallers;
- manipulatie van de verbinding.

De gebruikte VPN's zijn zelf ook aan andere dreigingen onderhevig:

- uitstroom van sleutelmateriaal;
- zwakke cryptografie;
- denial of service: de beschikbaarheid van de VPN wordt bedreigd door fouten of aanvallen.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?
Een Layer 3 VPN beschrijft de verbinding van twee of meer netwerken of de koppeling van een client met een netwerk op Layer 3 van het OSI-model. De getransporteerde gegevens worden versleuteld en de VPN-eindpunten authenticeren en autoriseren het respectieve andere VPN-eindpunt. Hierdoor kunnen bijvoorbeeld bedrijfsfilialen in verschillende landen veilig en vertrouwelijk met elkaar worden verbinden via onveilige lijnen van derden, zoals het Internet of diensten van een telecom provider aanbieder. In tegenstelling tot een Layer 2 VPN worden minder gegevens getransporteerd, omdat Layer 2 gegevens, zoals broadcasts, niet worden verzonden. Omgekeerd kan hierdoor een Layer 3 VPN voor alle toepassingen niet transparant worden gebruikt. Complexe topologieën, zoals on-demand VPN-verbindingen, kunnen soms alleen worden tot stand gebracht worden met een Layer 3 VPN of het is aanzienlijk gemakkelijker om dit zo te doen. Hetzelfde geldt voor VPN-configuraties met een groot aantal eindpunten. Een Layer 3 VPN vereist VPN-toegang voor elke deelnemer. Vaak wordt, wanneer een Hub-and-Spoke VPN-architectuur wordt gebruikt, naar het centrale knooppunt verwezen als VPN-concentrator. Aanbevolen wordt een Layer 3 VPN van een fabrikant als oplossing toe te passen.

[34] https://www.itu.int/rec/T-REC-X.200-199407-I/en

Als essentieel onderdeel van een IT-infrastructuur verdient de configuratie en werking van een Layer 3 VPN speciale aandacht. Een Layer 3 VPN-oplossing mag alleen worden geleverd door geautoriseerde en vertrouwde leveranciers. Van fabrikanten van veilige VPN-oplossingen mag worden verwacht dat ze actief patchbeheer bieden en snel reageren op beveiligingsproblemen, zodat u te allen tijde de best mogelijke bescherming hebt. Een fabrikant zonder het bijbehorend patchbeheer kan niet als professioneel worden beschouwd en moet worden uitgesloten van het selectieproces.

Een Layer 3 VPN moet de vertrouwelijkheid van de erdoor getransporteerde gegevens waarborgen. Daartoe moet het apparaat versleuteling en authenticatie uitvoeren met als veilig beschouwde algoritmen en parameters. De fabrikant moet kunnen aantonen dat hij actief werkt aan de beveiliging van de gebruikte cryptografie, of het nu gaat om het vervangen van algoritmen die onveilig zijn geworden of door het kiezen van de juiste parameters. Overal waar dit technisch haalbaar is, moeten veilige authenticatie mechanismen worden gebruikt. De toegang tot het beheer van de Layer 3 VPN moet aanvullende maatregelen beschermd worden. Dit omvat versleutelde toegang met veilige authenticatie (zoals HTTPS voor een WebGUI, SSH voor consoletoegang, in hardware beschermde authenticatie-informatie), maar ook de speciale aandacht van de fabrikant voor de beveiliging van het platform van het VPN-apparaat zelf om ongeautoriseerde toegang vanwege technische tekortkomingen uit te sluiten. Doorgaans wordt gevoelige informatie via een VPN getransporteerd.

Een Layer 3 VPN, waarvan de apparatuur backdoors bevat of waarbij een softwarebug kan leiden tot overname van het apparaat zelf, is een onaanvaardbaar risico. Daarom moeten producten die een hoog niveau platformbeveiliging en zelfbescherming kunnen aantonen, zoals door van onafhankelijke inspecties (certificering of zelfs accreditatie), de voorkeur krijgen. De eisen aan de operationele omgeving moeten blijvend waarborgen dat fysieke toegang tot de VPN-apparaten alleen mogelijk is voor geautoriseerde personen.

Net als bij de beschermingsdoelstelling van vertrouwelijkheid is de integriteit van het platform van cruciaal belang voor het handhaven van de integriteit en authenticiteit van de doorgegeven gegevens. Ook is het belangrijk dat de VPN-apparaten op een extra gehard platform worden opgebouwd, uitstekende zelfbescherming hebben en vrij zijn van backdoors. De beveiligingsprotocollen, die gebruikmaken van een Layer 3 VPN, garanderen ook de integriteit en authenticiteit van de getransporteerde gegevens. Het beheer en het veilige gebruik van sleutelmaterialen spelen ook een cruciale rol. De voorkeur moet gegeven worden aan fabrikanten die kunnen aantonen dat ze op veilige wijze willekeurige getallen kunnen genereren, veilig sleutelbeheer voor de private authenticatie sleutels (zoals op chipkaarten) (zoals op chipcards) vergemakkelijken en de ouderdom van de gebruikte coderingssleutels bijhouden.

Om de beschikbaarheid te waarborgen van Layer 3 VPN's te waarborgen, zijn passende maatregelen vereist voor de hardware en -software van de VPN-endpoints (zoals VPN-concentrators). Van de hardware moet de fabrikant kunnen aantonen dat het platform conform de eisen aan hoge beschikbaarheid is ontworpen en uitgevoerd. Dit omvat bijvoorbeeld redundante voedingen, krachtige rekenkracht en ventilatorconfiguratie waarbij het falen van één ventilator niet tot gevolg heeft dat het hele systeem uitvalt.

Omdat in de praktijk deze maatregelen alleen nog niet voldoende zijn om hardwarestoringen te voorkomen, moet de optie voor redundante werking (configuratie met hoge beschikbaarheid) beschikbaar zijn. Monitoring speelt eveneens een sleutelrol, zodat defecte hardware tijdig wordt gedetecteerd. Hier moet de fabrikant passende monitoring ondersteunen, zoals met SNMP Aan de software kant is, om storingen te voorkomen, bijvoorbeeld speciale aandacht nodig voor de correcte implementatie om. De voorkeur gaat uit naar fabrikanten die bij het ontwikkelen speciale inspanningen leveren in de vorm van code review. Daarnaast moet speciale aandacht worden besteed aan de bescherming tegen Denial-of-Service aanvallen. Natuurlijk is ook hier weer een bijzonder veilig platform een belangrijke vereiste, net als gecontroleerde toegang tot de locaties waar de VPN-eindpunten (VPN-concentrators) in het LAN worden gebruikt.

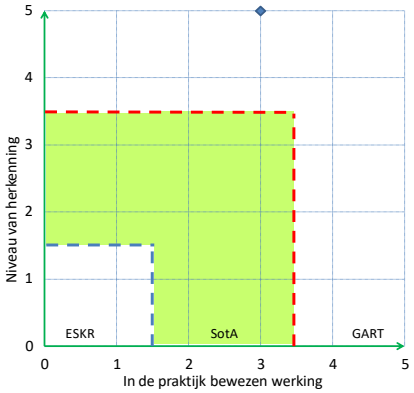
Op de apparatuur van een Layer 3 VPN worden loggegevens verzameld, Deze zijn essentieel voor het detecteren van aanvallen op het netwerk. Deze gegevens moeten echter verplicht zijn voor dit doel. Vergelijkbaar is het belangrijk om administratieve veranderingen te kunnen traceren en dat deze loggegevens verplicht zijn en dienovereenkomstig kunnen worden toegewezen. Daarom moeten er

mogelijkheden bestaan om zulke loggegevens fraudebestendig op te slaan, veilig tegen manipulatie. Dit kan bijvoorbeeld met lokale Append-Only Log's gegarandeerd worden, of door een interface te gebruiken naar externe logservers of SIEM-systemen.

Welke beschermingsdoelstellingen dekt deze maatregel af?

☒ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☒ Authenticiteit

Classificatie van het technologieniveau



Opmerking: hoewel er geen twijfel bestaat over de fundamentele noodzaak om VPN's te gebruiken, innoveren fabrikanten regelmatig om hun beveiligingsniveau, gebruiksgemak en bedienbaarheid te verhogen. De State of the Art voor VPN's wordt dus niet alleen bepaald door hun bestaan, maar ook door de gedaante van deze kwaliteiten.

3.2.10 Layer 2 versleuteling

Layer 2 versleuteling is een beveiligingsoplossing alternatief aan Layer 3 VPN's, en wordt toegepast op de payload van Ethernet-frames in plaats van op de IP-packets. De IP-headers hoeven niet te worden verwerkt (wat tijd bespaart) en de belasting van de lijncapaciteit vanwege de overhead door de versleuteling is veel lager dan de versleuteling door Layer 3 of hoger.

Tegen welke dreiging(en) wordt de maatregel ingezet?

Het vastleggen (recording) en beoordelen (evalueren) van enorme hoeveelheden gegevens van netwerkkoppelpunt locaties over de backbone van het bedrijfsnetwerk of de cloud-verbinding door veiligheidsgaten in de netwerkhardware, zowel bij netwerk serviceproviders, als onbewaakte ondergrondse en zeekabels en radio- of satellietverbindingen en DDoS-aanvallen op versleutelde Layer 3 verbindingen.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?

Het beschermen van de WAN-communicatie tussen bedrijfslocaties en datacenters met behulp van versleuteling. Gebruik van onderhoudsvrije en bandbreedteneutrale cryptografieoplossingen met zeer weinig vertraging voor Layer 2 WAN-backbones en directe koppelingen (zoals dark fiber of Satcom).

Layer 2 versleuteling is een beveiligingsoplossing die voor bepaalde applicaties als een geschikt alternatief voor Layer -3 VPN's functioneert. Het wordt toegepast op de payload van Ethernet-frames in plaats van op de IP-packets. IP-headers hoeven niet te worden verwerkt (wat tijd bespaart) en er is geen overhead als gevolg van versleuteling (de lijn lijnbandbreedte is volledig beschikbaar). Vereist voor gebruik voor een Ethernet gebaseerd netwerk (Point-to-Point, Hub-Spoke of Fully Meshed) via speciale kabels (koper/glasvezel) of een Layer 2 service die wordt geleverd door netwerkaanbieders (zoals Carrier Ethernet-services).

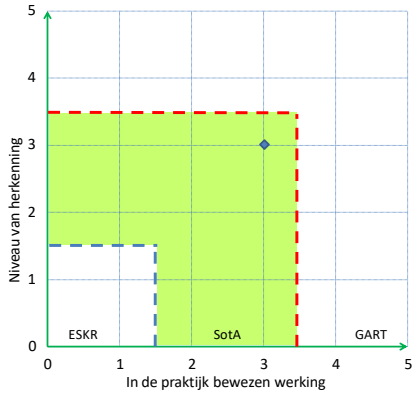
Typische toepassingen van Layer 2 versleuteling zijn het beschermen van WAN backbone-lijnen (ook internationaal) en datacenter verbindingen binnen het bedrijfsnetwerk of trusted clouds en collocation providers, evenals het beschermen van campus backbone-lijnen die buiten de gebouwen en over het eigendom van derden lopen.

De prestatievoordelen zijn de moeite waard, in het bijzonder bij het gebruik van centrale IT-services, massale desktop virtualisatie, consolidatie van datacenters en gedistribueerde en redundante opslagsystemen (SAN/NAS) met een groot aantal kleine/relevante real-time IP-packets (zoals VoIP, IoT en Smart Grid) en waar IPsec-overhead en -vertraging onaanvaardbaar zijn.
Het gebruik van deze netwerkversleuteling technologie vereist geen wijziging van de bestaande IP-routeringsconfiguraties. Dit type versleuteling is transparant voor vrijwel alle netwerkdiensten en -toepassingen van OSI-lagen 3 en hoger en heeft geen meetbare invloed op de netwerkprestaties.

Externe crypto-stations en periodieke wijzigingen van cryptografische sleutels worden automatisch gesynchroniseerd en geauthenticeerd. Het genereren en distribueren van de sleutels in Layer 2 encryptie-apparatuur is gedecentraliseerd, waarbij sleutel-servers als single points of failure worden vermeden en waardoor de beschikbaarheid van het netwerk toeneemt. Goedgekeurde BSI-oplossingen zijn beschikbaar.

Welke beschermingsdoelstellingen dekt deze maatregel af?
☒ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☒ Authenticiteit

Classificatie van het technologieniveau



3.2.11 Cloud-gebaseerde gegevensuitwisseling

Met de voortschrijdende digitalisering en geografisch spreiden van de manier van werken, worden cloud-gebaseerde gegevens uitwisselingsdiensten, cloud-based data exchange services zoals ze worden genoemd, steeds vaker toegepast in de IT-omgeving (zoals Dropbox, OneDrive, Google Drive). Om dergelijke diensten veilig te kunnen gebruiken en te beschermen tegen bekende dreigingen, moeten passende maatregelen worden genomen.

Tegen welke dreiging(en) wordt de maatregel ingezet?

De gegevens die zijn opgeslagen in een cloud-based data exchange service, zijn onderhevig aan de volgende dreigingen:

- Ongeoorloofde toegang en inzage door de exploitant van de dienst
- hacking door derden tijdens transport via internet;
- diefstal of ongeoorloofd gebruik van de identiteit die is overeengekomen met de cloud-service.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?

Om opgeslagen gegevens te beschermen, zijn de volgende maatregelen geschikt:

1. versleutelde overdracht van bestanden van en naar de data exchange service;
2. client zijde end-to-end versleuteling van de voor de ontvanger bedoelde gegevens voorafgaand aan overdracht naar de cloud;

- door in de Data Exchange service geïntegreerde versleuteling in tot de van de cloud deeluitmakende de client-software;
- -door afzonderlijke end-to-end encryptie software op de client.

In het bijzonder moeten de volgende vragen worden beschouwd:

1. Wie exploiteert de service en heeft de exploitant toegang tot de gegevens nodig?
2. Hoe worden de gegevens beschermd tijdens het transport van en naar de exploitant?

Als de service wordt beheerd door een vertrouwde instantie, dan is end-to-end versleuteling van de gegevens zelf in sommige gevallen niet nodig, maar in principe is ook bij vertrouwde exploitanten nuttig.

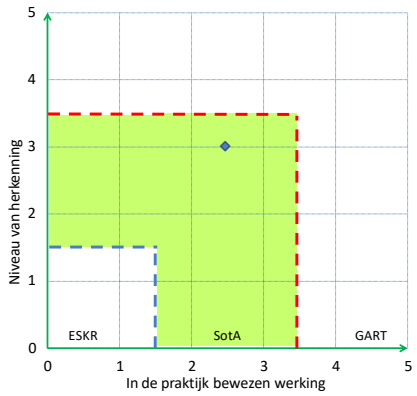
Er zijn data exchange services waarbij gegevens transparant worden versleuteld voordat ze worden geüpload, dat wil zeggen zonder speciale actie van de gebruiker en na het downloaden opnieuw worden gedecodeerd. In deze gevallen ziet de exploitant alleen gecodeerde gegevens. Als alternatief kan client-side encryptie software worden gebruikt, die end-to-end versleuteling van gegevens biedt vóór het uploaden en na het downloaden. Deze oplossingen brengen echter over het algemeen extra kosten voor de gebruiker met zich mee. Encryptie moet zich richten op het gebruik van veilige encryptiemethoden, het genereren van sleutels en sleutelbeheer.

In geen geval mogen gegevens onversleuteld worden getransporteerd van en naar de exploitant (Transport encryptie, doorgaans TLS).

Welke beschermingsdoelstellingen dekt deze maatregel af?

☐ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☒ Authenticiteit

Classificatie van het technologieniveau



3.2.12 Gegevensopslag in de cloud

In gedecentraliseerde cloud-infrastructuren zijn beschermingsstrategieën die alleen de IT-infrastructuur zelf beveiligen, niet meer toereikend. In de wapenwedloop met aanvallers, is de meest elementaire maatregel de veiligste: het versleutelen van gevoelige gegevens zodra deze een beveiligde interne omgeving verlaten om te worden verwerkt of opgeslagen in de cloud. De cryptografische sleutels dienen uitsluitend in het bezit te blijven van de gebruikersorganisatie om ongeautoriseerde toegang tot gegevens door externe beheerders uit te sluiten. Een state-of-the-art oplossing moet daarom een adequaat volledig intern sleutelbeheer mogelijk maken. Interne distributie van beheerfuncties naar meerder personen maakt het ook moeilijker om gevoelige gegevens in gevaar te brengen. State of the Art oplossingen zijn oplossingen die geen beperking inhouden voor belangrijke functies zoals het zoeken of filteren van gegevens, rapportage of geautomatiseerde verwerking van versleutelde gegevens in cloud-applicaties.

Tegen welke dreiging(en) wordt de maatregel ingezet?

Gevoelige gegevens die in de cloud worden opgeslagen of verwerkt, zijn vatbaar voor vele vormen

van compromitteren, zoals:

1. ongeoorloofde toegang tot de cloud-opslag (door zowel interne als externe gebruikers);
2. toegang door externe beheerders van cloud-providers of datacenters;
3. onderschepping tijdens overdracht tussen de organisatie en de cloud;
4. diefstal van cloud-opslag.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?
Een encryption-gateway is een proxy gebaseerde oplossing die zendt tussen de applicatie van de eindgebruiker de cloud. Deze gateway versleutelt alle gegevens die een vooraf gedefinieerde, beveiligde interne omgeving verlaten en decodeert de door de geautoriseerde eindgebruikers gevraagde informatie uit de cloud. Met dit type oplossing moeten de cryptografische sleutels uitsluitend in het bezit blijven van de gebruikersorganisatie om de gegevens soevereiniteit te waarborgen en om en de toegangsrechten centraal te beheren.

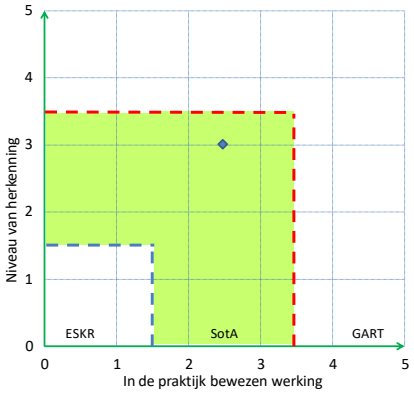
Een dergelijke State of the art oplossing moet daarom een volledig intern sleutelbeheer mogelijk maken. Sleutelbeheerfuncties moeten intern over meerdere controllers worden verdeeld, dit zorgt ervoor dat belangrijke gegevens niet door individuen kunnen worden gecompromitteerd. Intern moeten de taken voor sleutelbeheer worden gedistribueerd naar meerdere controllers. Dit zorgt ervoor dat de belangrijkste gegevens kunnen niet worden aangetast door individuen. Intern sleutelbeheer is veiliger dan native versleutelingoplossingen van externe cloud-providers (Bring Your Own key, enz.). In het laatste geval kan het nooit volledig worden uitgesloten dat derden (zoals databasebeheerders) leestoegang tot gevoelige informatie hebben. Met een encryption-gateway kunnen externe gegevensverwerkers nog steeds beheertaken uitvoeren, maar geen gevoelige gegevens in leesbare vorm lezen. De oplossing biedt ook bescherming in het geval van gegevensdiefstal: zonder de cryptografische sleutels kunnen aanvallers niets aanvangen met de verkregen versleutelde gegevens.

De centrale factor bij het gebruik van een encryption gateway moet zijn dat beveiligde gegevens nog steeds kunnen worden verwerkt. Dit kan worden bereikt door gedeeltelijke versleutelingmethoden te gebruiken.

Met oog op de toekomst is het raadzaam een encryption gateway te kiezen die de gebruikersorganisatie de vrijelijk de te gebruiken versleutelingalgoritmen kan wisselen. Met de voortschrijdende ontwikkeling van extreem krachtige kwantumcomputers kunnen methoden die vandaag als veilig zijn geclassificeerd in de nabije toekomst al achterhaald zijn. Ideal is daarom een oplossing die nu al compatibel is met algoritmen van post-Quantum Cryptography (PQC).

Welke beschermingsdoelstellingen dekt deze maatregel af?
☐ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☒ Authenticiteit

Classificatie van het technologieniveau



3.2.13 Gebruik van mobiele spraak- en datadiensten

Mobiele telefoongesprekken en -gegevensoverdracht zijn gemakkelijker te onderscheppen dan vaste telefonie. Daartegen beschermen versleuteling van mobiele spraak en gegevensoverdracht, net als hardening en configuratie.

Tegen welke dreiging(en) wordt de maatregel ingezet?

De klassieke vaste en mobiele telefonie is ook nu, in tegenstelling tot chat en webconferentie applicaties een van de meest directe en persoonlijke hulpmiddelen voor communicatie. Ze heeft echter enkele risico's en biedt potentiële aanvalsvectoren. Het overgrote aantal telefoontjes afkomstig van vaste apparaten vinden plaats met de deelname van een mobiele telefoon.

- Hacking van mobiele gesprekken en dataverkeer in vaste lijnen van mobiele en telefonie en netwerk exploitanten, dat de basisstations met elkaar en met de vaste lijnen verbinden en welke op Internet technologie is gebaseerd, enz.

- Hacken van mobiele telefoon gesprekken en verkeer, en ook de overdracht van en naar Command & Control (aanval)servers, door op de mobiele telefoon geïnstalleerde malware te exploiteren en zo via app kwetsbaarheden in het besturingssysteem directe toegang te krijgen tot microfoons, luidsprekers, touch screen toetsenbord en scherm, en waarmee de encryptie app ongedaan is gemaakt.

- Niet-versleutelde mobiele telefoongesprekken en dataverkeer kunnen met goedkope hardware op de etherinterface worden onderschept. Daarvoor hoeven aanvallers de mobiele telefoon niet te infecteren of in te breken in het communicatienetwerk. Zij moeten zich echter wel binnen het ontvangstbereik van de betreffende mobiele telefoon bevinden. Aanvallers doen zich bijvoorbeeld voor alsof ze deel uitmaken van het mobiele netwerk om de mobiele telefoon op hun luister apparaat te registreren en vervolgens gesprekken en dataverkeer direct op te nemen en te analyseren.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?

De vertrouwelijkheid van gesprekken kan door spraak- en gegevensversleuteling toe te passen op OSI- Layer 7 (de communicatie laag) worden zeker gesteld. Hier worden gesproken woord en chat gegevens en eventuele bestandsoverdrachten real-time op het apparaat versleuteld en vervolgens zodra ze de ontvanger bereiken gedecodeerd en weergegeven.

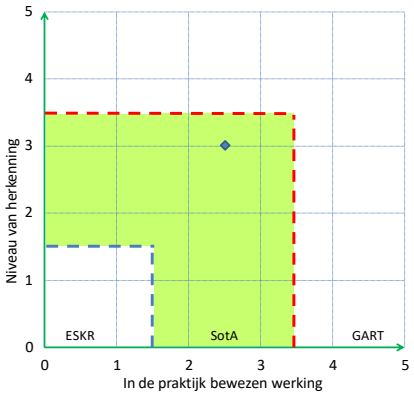
De volgende tegenmaatregelen worden aanbevolen:

- versleuteling van spraak- en datacommunicatie door geschikte en vertrouwde apps of hardware die naar de huidige coderingsstandaarden en toepasselijke regels voor gegevensbeveiliging voor end-to-end encryptie doorvoeren;
- aanvullend, centrale configuratie van de eindapparatuur die door de organisatie is uitgegeven of door de organisatie ondersteunde en met Mobile Device Management en Enterprise Mobility Management (MDM/EMM-systemen) beheerde Bring Your Own Devices (BYOD);
- voor hogere betrouwbaarheidsniveaus het gebruik van mobiele telefoons met gehardende bedieningssystemen, welke garanderen dat microfoon en luidspreker alleen gebruikt kunnen worden door de encryptie-app en voorkomen dat willekeurig welke malware de encryptiesleutel kan hacken.

Welke beschermingsdoelstellingen dekt deze maatregel af?

☐ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☒ Authenticiteit

Classificatie van het technologieniveau



3.2.14 Communicatie via Instant Messenger

Instant Messaging is de een vorm van digitale communicatie waarbij twee of meer partijen communiceren via snel doorgegeven tekst-, beeld- en spraakberichten. Daartoe gebruiken de partijen een gemeenschappelijke Instant Messenger om de berichten via een netwerk te verzenden. Als een communicatiepartner op het moment dat een bericht wordt verzonden niet online is, dan wordt het bericht meestal op een later tijdstip aan de ontvanger afgeleverd. Secure Instant Messaging streeft ernaar Instant Messages te beschermen tegen ongeoorloofde toegang en wijziging.

Tegen welke dreiging(en) wordt de maatregel ingezet?
Wanneer informatie wordt uitgewisseld met behulp van Instant Messaging, dan moeten de volgende dreigingen worden overwogen:

1. het vastleggen, analyseren en wijzigen van de inhoud door een niet-geautoriseerde derde partij (Man-in-the-Middle aanval);
2. identiteitsdiefstal binnen een communicatiesysteem;
3. diefstal van apparatuur met als doel om vervolgens zonder toestemming de Instant-Messaging gegevens te analyseren.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?

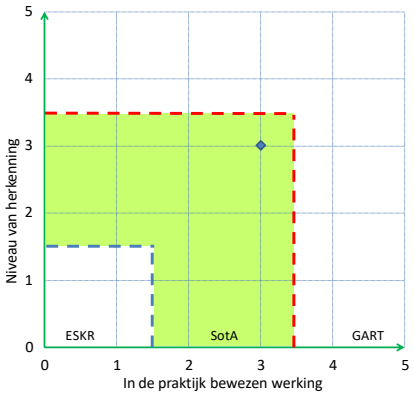
1. Secure Instant Messaging bevat technische maatregelen ter bescherming van de integriteit en vertrouwelijkheid van de communicatie-inhoud;

- gegarandeerde berichtenoverdracht op de transportroute met de actuele versie van TLS;
- gebruik van asymmetrische end-to-end versleuteling met een minstens aan RSA 2048 bit vergelijkbaar beschermingsniveau;
- Forward Secrecy moet deel uitmaken van de architectuur om de gegevens tegen latere decodering te beschermen, ongeacht of de lange termijn sleutel is gebruikt.

2. betrouwbare verificatie/authenticatie van identiteiten;
3. beveiliging van toegangsopties en toegangspaden naar inhoud;
- schermvergrendeling op het gebruikte mobiele apparaat (sterk wachtwoord);
- geactiveerde apparaatversleuteling;
- de gebruikte communicatie-app moet onafhankelijke, veilige gegevensopslag bieden en bescherming bieden tegen decodering door onbevoegde partijen.

Welke beschermingsdoelstellingen dekt deze maatregel af?
☐ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☒ Authenticiteit

Classificatie van het technologieniveau



3.2.15 Beheer van mobiele apparaten

De inzet van Mobile Device Management (MDM) oplossingen reduceert de veiligheidsrisico's die ontstaan door het ongecontroleerde gebruik - voor zakelijke doeleinden - van mobiele apparaten. MDM-oplossingen maken het mogelijk het beheer en de configuratie van de gebruikte mobiele apparaten te centraliseren.

Tegen welke dreiging(en) wordt de maatregel ingezet?

1. Gegevensverlies: als belangrijke data is opgeslagen op mobiele apparaten en het apparaat raakt verloren of vernietigd, dan moet het bedrijf accepteren dat deze gegevens in sommige situaties onherroepelijk verloren gaan.
2. Diefstal: als een mobiel apparaat wordt gestolen, dan heeft de dief mogelijk toegang tot vertrouwelijke bedrijfsgegevens.
3. Malware: door openbare WiFi-netwerken (WLAN) te gebruiken, het niet installeren van beschikbare updates en het ongecontroleerd installeren van applicaties vanuit een twijfelachtige bron, raken mobiele apparaten vaak geïnfecteerd met malware.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?

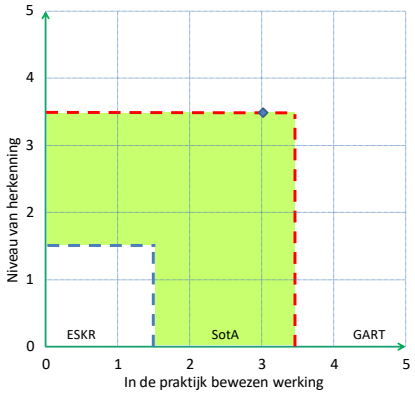
Mobile Device Management (MDM) oplossingen stellen beheerders in staat om de toegang tot en het gebruik van mobiele apparaten, die voor zakelijke doeleinden worden gebruikt, op verschillende manieren en op basis van vooraf gedefinieerde beveiligingsrichtlijnen te beheren. MDM-oplossingen kunnen de patchstatus van mobiele apparaten bepalen en updates activeren zodra ze beschikbaar en gecontroleerd zijn. Bovendien kunnen adequate wachtwoordbeveiliging, reguliere back-up en apparaatversleuteling centraal worden afgedwongen. In het geval van diefstal of verlies van het apparaat kan een geforceerde verwijdering (Remote Wipe) worden uitgevoerd om de vertrouwelijkheid van bedrijfsgegevens te beschermen. De beheerder kan gebruikersrechten voor het mobiele apparaat zo instellen, dat de installatie van applicaties van potentieel onveilige bronnen niet is toegestaan.

Om te voldoen aan de toenemende functionaliteiteisen voor het, voor zakelijke doeleinden, gebruik van mobiele apparaten, hebben sommige fabrikanten de huidige MDM-functies uitgebreid met Mobile Application Management (MAM) en Mobile Information Management (MIM) functies inclusief cloud-verbinding met zogenaamde EMM-oplossingen (Enterprise Mobility Management).

Welke beschermingsdoelstellingen dekt deze maatregel af?

☒ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☐ Authenticiteit

Classificatie van het technologieniveau



3.2.16 Routerbeveiliging

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

In de B2B-sector (business to business sector) worden routers niet alleen gebruikt als Internet toegangsapparatuur of voor het routeren van gegevens. In de meeste gevallen bouwen ze ook VPN-netwerken op. Tijdens de migratie van de telefonie-infrastructuur (vervanging van ISDN/analoge technologie door IP-technologie), worden routers als ISDN-IP-gateways ingezet, om de nog aanwezige ISDN-systemen ook in IP-netwerken te kunnen blijven gebruiken. Beide toepassingen maken de router tot een bedrijfskritisch component met specifieke beveiligingseisen.

Vanwege het wereldwijde aantal in zakelijke, sociale en privénetwerken geïnstalleerde routers, maakt de router tot doelwit voor verschillende soorten aanvallen, die door passende beschermingsmaatregelen moeten worden voorkomen. In deze sectie wordt een overzicht van de dreigingen voor routers en de huidige beveiligingsmaatregelen beschreven en beoordeeld.

Tegen welke dreiging(en) wordt de maatregel ingezet?
Routers zijn ontworpen om gegevens betrouwbaar en veilig te routeren (redirecten/om te leiden) en tegelijkertijd te beschermen tegen ongeautoriseerde toegang tot deze gegevens. De volgende dreigingen/risico's brengen deze doelstellingen in gevaar:

1. manipulatie van de configuratie
2. aanvallen via bekende nog niet gesloten beveiligingsgaten;
3. aanvallen exploiteren van met nieuw ontdekte beveiligingsgaten (zero-day exploits);
4. aanvallen via IP-telefonie verbindingen;
5. diefstal (vooral routers voor buiten/mobiele communicatie);
6. beschikbaarheidaanvallen (DoS-aanvallen);
7. toegang via niet-gedocumenteerde interfaces (zoals backdoors/achterdeuren);
8. uitvoeren van code van derden en integratie in botnets;
9. aanvallen via onvoldoende beveiligde WLAN's.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?
Voor de bovenstaande dreigingen bestaan meerdere beveiligingsmaatregelen om het risico van de bovenstaande dreigingen te minimaliseren, dat hieronder kan worden samengevat als een pakket van router beveiligingsmaatregelen:

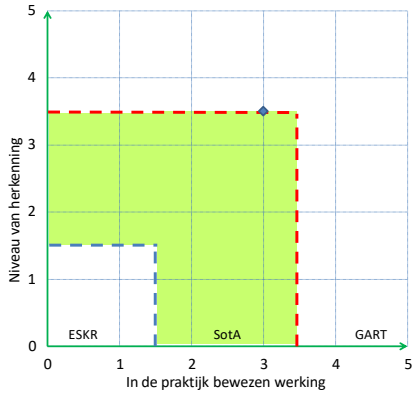
1. wachtwoordbeveiliging: gebruik van beveiligde, tegen toegang van derden beveiligde, toegangsgegevens en het vermijden van het gebruik van standaardaanmeldingen;
2. regelmatig updaten van router-firmware;
3. servicecontracten met de fabrikant en een vastgestelde maximum responstijd in het geval dat een ernstig beveiligingsgat wordt ontdekt;
4. als de router-fabrikant geen updates verstrekt na het bekend worden van een beveiligingslek, dan moet het inzetten van alternatieve apparaten van andere fabrikanten worden overwogen, die niet door het beveiligingslek worden getroffen;
5. de router moet worden geplaatst in een beveiligde locatie, zoals een afsluitbare ruimte met

toegang bewaakt door verantwoordelijke beheerders Buitenshuis is het vaak niet mogelijk om de router op een beveiligde locatie te plaatsen. Daarom moet de router zijn uitgerust met een GPS-functie. De router moet zo worden geconfigureerd, dat na bijvoorbeeld een stroomstoring wordt gecontroleerd of deze zich nog steeds op de locatie bevindt. Als dit niet het geval is, dan moet de werking ervan worden onderbroken;
6. ter bescherming tegen DoS-aanvallen moeten, conform RFC 2267, in de firewall ongeldige adressen worden gefilterd en Blacklists (zwarte lijsten) worden ingesteld;
7. alle open en niet benodigde poorten en interfaces moeten worden gesloten;
8. Zo mogelijk moet de router tijdens inactiviteit (zoals 's nachts) automatisch worden gedeactiveerd om het aanvalsvenster te verkleinen. Deze maatregel mag de installatie van updates niet beperken;
9. om de impact van geslaagde aanvallen op routers te minimaliseren moeten verschillende netwerkzones worden ingesteld(netwerksegmentatie);
10. WLAN-router: geen open netwerken of alleen voor gasttoegang (directe uitgaande lijn), en anders het toepassen van de hoogste versleutelingstandaarden;
11. VPN-router: zet geen VPN-verbindingen op met eerder gedeelde sleutels (pre-shared) maar zo mogelijk op basis van een certificaat;
12. router als all-IP/ISDN-gateway: pas apparaten met geïntegreerde Session Border-Controller toe. Firewalls zijn niet in staat om op Session Initiation Protocol (SIP) gebaseerde spraakpakketten te verwerken, zodat hierdoor het risico van een aanval via Voice-over-IP-verbindingen ontstaat. De werking van de router moet centraal worden bewaakt.

Welke beschermingsdoelstellingen dekt deze maatregel af?

☒ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☒ Authenticiteit

Classificatie van het technologieniveau



3.2.17 Netwerkbewaking met behulp van IDS (inbraakdetectiesysteem)

Een intrusion detection system (IDS) of intrusion prevention system (IPS) identificeert en logt afwijkingen in het IT-netwerk. Het doel van beide systemen is zo mogelijk het binnendringen en distribueren van malware te detecteren voordat schade optreedt. In tegenstelling tot een IDS, dat alleen informatie van afwijkend gedrag aantoont en alarmeert, kan een IPS ook automatisch ingrijpen. Daarmee moet de verdere verspreiding van malware via het netwerk worden voorkomen. Zoals gezegd kan de directe tussenkomst van een IPS rechtstreeks van invloed zijn op de beschikbaarheid van onder andere van industriële en productiesystemen, volledig geautomatiseerde bestel-/leveringsprocessen en melding- en veiligheidsprocessen (inclusief brandbeveiliging).

Tegen welke dreiging(en) wordt de maatregel ingezet?

1. informatielekken door afluisteren van gevoelige gegevens;
2. misbruik van diensten en communicatieprotocollen;
3. toegang van externe IT-systemen tot het IT-netwerk;
4. exploitatie van mogelijkheden van toegang tot gekoppelde IT-systemen;
5. manipulatie van informatie of software;

6. verspreiding van malware in het IT-netwerk.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?
Er is een onderscheid tussen netwerkgebaseerde en op host gebaseerde IDS/IPS. Netwerk gebaseerde IDS/IPS maken gebruik van interne componenten en/of netwerkinfrastructuur om de communicatie te bewaken. Host gebaseerde IDS en IPS gebruiken informatie uit IT-systemen (via software-agenten, logfile-analyses, enz.). In de architectuur van gedistribueerde systemen moeten de gegevens voor uitwisseling of opslag worden versleuteld en ondertekend.

Detectie is gebaseerd op twee verschillende methoden. Bij de zogenaamde patroon matching wordt bekende malware gedetecteerd op basis van patronen (signatures/handtekeningen). Nieuwe aanvalspatronen moeten zo snel mogelijk worden geanalyseerd en hun handtekeningen direct - – tegen manipulatie beschermd - bijgewerkt worden, omdat anders aanvallen op basis van deze patronen onopgemerkt blijven.

De tweede methode is gebaseerd op het detecteren van door een aanval veroorzaakte wijzigingen in het communicatiepatroon van netwerkonderdelen. Alle communicatie buiten het verwachte netwerkverkeers profiel wordt als een anomalie beoordeeld. Daardoor kunnen ook nieuwe aanvallen worden gedetecteerd. Het bijhouden van aanvalspatronen in een database is niet nodig. Wel moet echter worden gedefinieerd welke communicatiepatronen als normaal netwerkverkeer beschouwd moeten worden.

Een IDS moet bij detectie van malware of als afwijking is geconstateerd van de geldige nominale tostand van de communicatie, automatisch bijbehorende incidentmeldingen genereren Alle incidentmeldingen moeten lang genoeg voor analysedoeleinden in het systeem worden bewaard en zo nodig in een open of gestandaardiseerd formaat worden geëxporteerd.

De gebeurtenisberichten moeten alle relevante informatie bevatten voor het analyseren van gebeurtenissen en het initiëren van tegenmaatregelen, zoals gedetecteerde handtekening of afwijkende communicatieverbinding. De alarmberichten moeten op de beheerconsole werkelijk zichtbaar zijn, als mail naar gedefinieerde accounts worden verzonden en via een export interface beschikbaar zijn op een algemeen alarmsysteem (Zie SIEM).

Een IPS moet ook zelfstandig alle aan aanvalsgedrag toegeschreven netwerkcommunicatie blokkeren. Daarbij moet ervoor worden gezorgd, dat voor zover mogelijk geen communicatie wordt verhinderd dat duidelijk aan niet-aanvalsgedrag kan worden toegeschreven.

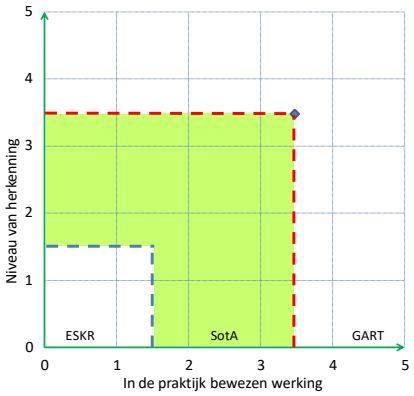
Een IDS/IPS moet componenten leveren voor het analyseren van alle communicatie bij netwerk overgangen en/of binnen IT-systemen (hosts) die voor stabiele werking automatisch opnieuw synchroniseren na een tijdelijke onderbreking.

Ongewenste communicatie van IDS/IPS-componenten naar derden mag niet worden toegestaan. Bovendien moeten alle IDS/IPS-componenten niet-identificeerbaar zijn, het dataverkeer niet beïnvloeden, geen diensten aanbieden en zelf beschermd zijn.

Aanvullend op handtekening en sleutellengte van de gebruikte certificaten moeten ook symmetrische en asymmetrische algoritmen worden gebruikt, volgens de huidige aanbevelingen van het BSI.

Welke beschermingsdoelstellingen dekt deze maatregel af?
☒ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☒ Authenticiteit

Classificatie van het technologieniveau



3.2.18 Bescherming van het webverkeer

Webservers zijn een van de belangrijkste manieren om malware te verspreiden. Door geïnfecteerde websites wordt, meestal zonder dat gebruikers dit bemerken. malware op het systeem geladen en uitgevoerd. Als tijdens het browsen/surfen het gegevensverkeer door een webfilter wordt geleid, dan kunnen zulke aanvallen worden gedetecteerd en geblokkeerd.

Tegen welke dreiging(en) wordt de maatregel ingezet?

Webservers zijn een van de belangrijkste manieren om malware te verspreiden. Ze maken vaak gebruik van geïnfecteerde webservers, waarbij de exploitant niet direct bij de aanval betrokken is. Een groot percentage van webservers heeft permanente beveiligingsgaten, en daarop kunnen hackers zich richten en vervolgens malware, meestal zogenaamde rootkits, op het systeem opslaan.

Deze websites worden normaalgesproken door de gebruiker beheerd. Bij het bezoek aan een geïnfecteerde website wordt de malware zonder dat de gebruiker dit merkt op het lokale systeem geladen en geactiveerd (drive-by downloads).

Bovendien worden door aanvallers ook speciaal hiervoor ingerichte webservers ingezet, die vaak een andere website nabootsen. Bij zgn. phishing worden deze valse kopieën van bekende websites beschikbaar gesteld, om gevoelige informatie van de gebruiker af te tappen; meestal gebruikersnamen en wachtwoorden, daarnaast bankgegevens, creditcardinformatie, adressen, enz.

Vaak wordt het daadwerkelijke bestemmingsadres (de URL met kwaadaardige code of de URL van een geïnfecteerde of valse webpagina) verborgen door automatische omleiding (redirecting) en vaak ook door URL-verkortingen (bit.ly, TinyURL, enz.), hoewel deze niet rechtstreeks betrokken zijn bij de daadwerkelijke aanval. Via links welke in e-mailberichten, op sociale media, enz. zijn geplaatst, Gebruikers worden via gerichte links in e-mails, sociale media, enz. direct doorgelinked naar de dedicated aangeboden websites.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?

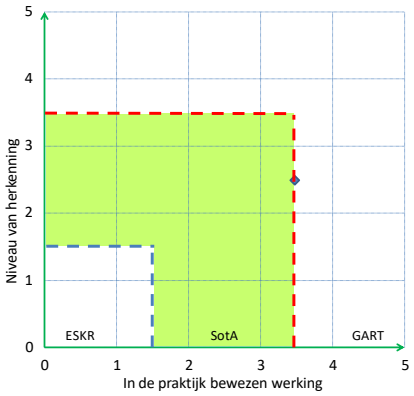
Om tegen dit soort aanvallen te beschermen wordt het webgegevensverkeer via webfilters geleid. Webfilters beschermen tegen deze aanvallen door de betreffende websites te blokkeren en de gegevens die van websites zijn geladen te analyseren op schadelijke code.

Webfilters kunnen centraal worden uitgevoerd als webfilters in de cloud, als lokale software (appliance on premise), of als software die lokaal actief is op het eindgebruikers systeem.

Welke beschermingsdoelstellingen dekt deze maatregel af?

☒ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☒ Authenticiteit

Classificatie van het technologieniveau



3.2.19 Bescherming van webapplicaties

Een Web Application Firewall (WAF) beschermt webapplicaties (homepages, online winkels, thuisbankier portals, enz.) tegen aanvallen. Daarvoor inspecteert het WAF de communicatie tussen gebruikers en webapplicaties op toepassingsniveau en blokkeert potentieel schadelijk gegevensverkeer, zoals SQL-injecties en cross-site scripting. Voor communicatie tussen machines (machine-to-machine)wordt veelal de term Web Service Firewall (WSF) gebruikt.

In tegenstelling tot een netwerk-firewall die werkt op OSI-lagen 3 en 4, werken WAF's op OSI Layer 7-(gegevensverkeer) en beschermen ze zo tegen dreigingen die gericht zijn op het misbruik van beveiligingskwetsbaarheden in de applicaties.

Tegen welke dreiging(en) wordt de maatregel ingezet?

Aanvallen op webapplicaties of webservice-interfaces, zoals:

- SQL injectie;
- Cross-Site Scripting (XSS);
- gelekte informatie;
- Command Injection;
- andere OWASP-dreigingen.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?
Gebruik een Web Application firewall (WAF) of Web Service Firewall (WSF) die actief is voor de webserver (upstream).

Een Web Application firewall (WAF) beschermt webapplicaties (homepages, online winkels, thuisbankier portals, enz.) tegen aanvallen. Daartoe analyseert de WAF op toepassingsniveau de communicatie tussen gebruikers en webapplicaties en blokkeert mogelijk schadelijk dataverkeer. Wanneer beveiligingsgaten in webapplicaties snel moeten worden gesloten, volstaat het meestal om de WAF aan te passen. Het aanpassen/patchen van de te beveiligen webapplicatie kan vervolgens daarna worden uitgevoerd met voldoende aandacht voor de uit te voeren tests. Bij aanvallen wordt vaak een combinatie van verschillende kwetsbaarheden gebruik gemaakt. Daarom kunnen met het blokkeren van een centrale kwetsbaarheid per WAF veel aanvallen snel worden afgewend.

De Web Services firewall (WSF) is een speciale vorm van de WAF voor machine-naar-machine communicatie en werkt vergelijkbaar voor via http/https. De aanvalsvectoren voor WAF en WSF lijken erg op elkaar. Het volgende is van toepassing op de WAF en vergelijkbaar voor de WSF.

Moderne webapplicaties en -services bieden vaak een programmeerinterface (API) die een breed scala aan functies biedt voor flexibel machinegebruik, maar wat zelden de beste vorm van bescherming is.

De WAF beëindigt versleuteld gegevensverkeer aan de gebruikerszijde, analyseert de inhoud en stuurt als ongevaarlijk geclassificeerde aanvragen versleuteld door naar de webserver. Schadelijke aanvragen worden geblokkeerd.

De werking van webapplicaties zonder gebruik van een appliance of Virtuele Upstream WAF kan niet langer als State of the Art beschouwd.

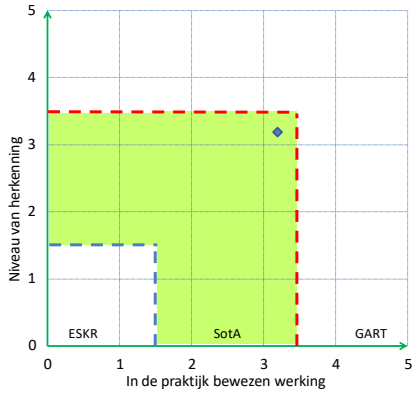
Een WAF moet de volgende functies hebben:

- loggegevens overdracht naar een SIEM en naar anomaliedetectie systemen, met de mogelijkheid om wachtwoorden, creditcardinformatie, etc. te verbergen;
- clustering mogelijkheden voor hoge beschikbaarheid en verdeling van de belasting (loadbalancing);
- bescherming tegen OWASP top 10-aanvallers, zoals SQL-injectie, cross-site scripting (XSS) en Directory Traversal door middel van blacklisting, whitelisting en patroonherkenning;
- sterke authenticatie van webapplicaties en gebruikers van services;
- sessiebeheer, d.w.z. inspectie- en manipulatiebeveiliging van sessiecookies;
- Broken Access Control, dat ongeoorloofde toegang tot paden (Path Traversal), bestanden en API-functies voorkomt;
- filters tegen onnodige http-headers;
- bescherming tegen Cross-Site Request Forgery (CSRF) door header evaluatie van http-verzoeken, zoals doorverwijzingsinformatie (referrer-information).

Welke beschermingsdoelstellingen dekt deze maatregel af?

☒ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☒ Authenticiteit

Classificatie van het technologieniveau



3.2.20 Externe toegang tot netwerken / onderhoud op afstand

Externe netwerken moeten via internet toegankelijk zijn voor onderhoud en software-updates. In de industriële omgeving zijn deze deelnemers machinebesturing componenten, zoals PLC, aandrijfunits en bedieningspanelen. In het geval van onderhoud of een software-update, moet de externe gebruiker online met de tools van de fabrikant (zoals PLC programmeersoftware) toegang hebben tot deze systemen.

Tegen welke dreiging(en) wordt de maatregel ingezet?

- ongeautoriseerde toegang tot het bedrijfsnetwerk;
- ongeautoriseerde toegang tot doelsystemen;
- externe (onderhoud) toegang kan niet worden getraceerd;
- blootstelling of aftappen van data tijdens externe (onderhoud)toegang.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?

Om afstandsbediening mogelijk te maken, worden de doelsystemen meestal via routers met het Internet verbonden. Vervolgens wordt een VPN-verbinding opgezet naar een zogenaamde centrale server (intermediate server). Dit (centrale) koppelpunt is de verbinding tussen het doelsysteem en de externe afstandbediening, die vergelijkbaar een VPN-verbinding heeft opgezet met de centrale server.

Omdat beide deelnemers een eigen verbinding hebben, kan elke deelnemer zelf op elk gewenst moment de verbinding beëindigen. In dit proces is de taak van de centrale server om alleen de goedgekeurde doelsystemen voor de respectieve externe afstandsbediening/gebruiker vrij te geven. Idealiter kan dit voor externe gebruikers en doelsystemen worden beperkt tot op Layer 3 (IP, poort, protocol). Daarmee is de applicatiespecifieke verbinding met de server gewaarborgd. Afhankelijk van de applicatie kunnen voor extern onderhoud ook zuivere terminalverbindingen tot stand worden gebracht, zoals Web-, RDP-, VNC-of SSH-verbindingen. Dit is afhankelijk van de beschikbaarheid op het doelsysteem. Een rechtstreekse 1op1-koppeling van de externe gebruiker naar het netwerk van het doelsysteem moet echter vermeden.

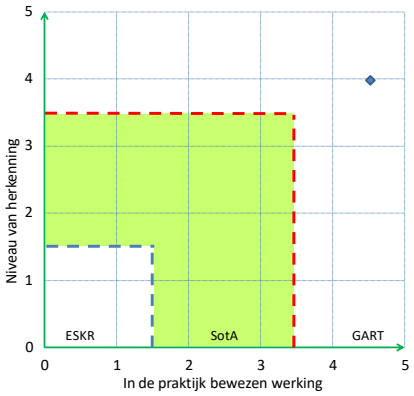
Met versleutelde VPN-verbindingen wordt de gegevensintegriteit en bescherming tegen aftappen van gegevens gegarandeerd.

Elke externe onderhoudssessie moet worden geregistreerd. Dit is nodig om, in geval van een beveiligingsincident, de meest recente toegang tot het netwerk/router te kunnen identificeren. Als dit gebeurt, moeten de identiteit van de externe gebruiker (IP-adres en naam) en de tijd en duur van de verbinding worden vastgelegd. Idealiter wordt dit op de centrale server opgeslagen.

Welke beschermingsdoelstellingen dekt deze maatregel af?

☐ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☒ Authenticiteit

Classificatie van het technologieniveau



3.2.21 Serverhardening

Aangezien op serversystemen essentiële (vaak gevoelige) bedrijfsgegevens en persoonsgegevens worden verwerkt en opgeslagen, moeten de gebruikte systemen voorzien zijn van speciale beschermende maatregelen. Een zeer effectieve beveiligingsmaatregel is Serverhardening. Deze maatregel beveiligt het besturingssysteem, ongeacht of het een fysieke, virtuele of cloudgebaseerde server betreft.

Gangbare serverbesturingssystemen (zoals Microsoft Windows Server en Linux Server) hebben standaard geen zeer beperkende beveiligingsconfiguratie en zijn potentieel uitgerust met ongebruikte onderdelen. Juist deze ongebruikte en niet-geconfigureerde functies worden vaak door aanvallers als aanvalsvector misbruikt.

Met server hardening worden deze functies en hun interfaces uitgeschakeld en wordt een sterke beveiligingsconfiguratie ingesteld, die het beveiligingsniveau van de server systemen aanzienlijk verhoogt. Daarom moet server hardening een vast onderdeel uitmaken van de technische beveiligingsstrategie van de organisatie.

Tegen welke dreiging(en) wordt de maatregel ingezet?

De belangrijkste dreigingen bij niet gehardende servers zijn:

- manipulatie van persoonsgegevens en gevoelige bedrijfsgegevens;
- afluisteren van gegevens (zoals kopiëren van volledige databases van databasesystemen);
- manipulatie van applicaties op het serversysteem of aangesloten systemen;
- manipulatie, sabotage of spionage met gebruikmaking van bedrijfs- en productieprocessen;
- identiteitsdiefstal, zoals aanvallen op domeincontrollers;
- binnenbrengen van malware van welke aard dan ook en het verspreiden van de malware naar andere systemen;
- misbruik van servercapaciteit voor processen van de aanvaller (zoals Crypto-Mining);
- Host-jumping waarmee aanvallers andere systemen kunnen aanvallen.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?

Voor het hardenen van serversystemen komen in het bijzonder de volgende maatregelen in overweging:

1. deactivering van componenten:
- het regelmatig controleren of geactiveerde diensten nog nodig zijn voor de werking;
- het uitschakelen of de-installatie van niet-noodzakelijke onderdelen/diensten van het besturingssysteem inclusief achtergrondservices;
- het uitschakelen van niet benodigde auto start of tijdgestuurde processen;
- het deactiveren van onnodige, technisch verouderde of onveilige Interfaces of protocollen;
- het deactiveren van telemetrie gegevens gegevensoverdrachten, tenzij ze conform beleid vereist zijn voor centrale bewaking;
- het uitschakelen van ongebruikte bestand-shares;
- het deactiveren of beperken van toegang tot (beheerfuncties van) websites;

2. activering van hardware georiënteerde beschermingsfuncties:
- het activeren van CPU-beveiligingsfuncties, zoals Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP) en het en verifiëren van de goede werking van de applicaties;
- het activeren van BIOS-wachtwoordbescherming en het beperken van de opstartvolgorde tot de benodigde apparaten;
- het zo nodig activeren van beschermingsprocedures tegen Side-Channel aanvallen;
- het zo nodig activeren van veilige opstartprocedures;

3. beveiligingsconfiguratie:
- het gebruik van communicatieprotocollen om te borgen dat gevoelige gegevens en authenticatie-informatie versleuteld worden verzonden;
- het gebruik van certificaten voor het uitwisselen van cryptografische sleutels;
- het uitschakelen van opstart mechanismen (zoals USB-media);
- het activeren van een screensaver met wachtwoordbeveiliging;
- het activeren van een sterk gebruikersaccount beheer (User Account Control);
- het al tijdens het opstarten activeren van antivirus bescherming op het systeem;
- het verwijderen van niet-noodzakelijke certificaten van Trust Stores;
- het voorkomen van het lekken van systeeminformatie, zoals over geïnstalleerde services en versienummers;
- het uitschakelen van fout- of foutopsporingsberichten voor eindgebruikers, of deze vervangen door neutrale foutberichten;
- het met een specifiek serviceaccount en met minimale rechten uitvoeren van services, zo mogelijk in een geïsoleerde omgeving;
- het activeren van de logging;

4. toekenning van minimale toegangsrechten (autorisatie op basis van need-to-know en least privilege principes):
- het regelmatig verifiëren van verleende machtigingen
- het toekennen van minimale rechten voor administratieve activiteiten;
- het toekennen van minimale rechten voor bestandssysteem en externe gegevensinterfaces;
- het toekennen van minimale rechten voor onderhoudsinterfaces/-toegangen;
- het beperken van de toegang tot de configuratie van het besturingssysteem, beperkte toegang tot bestanden op fysieke servers (in het bijzonder om te voorkomen dat ongeautoriseerd externe gegevensdragers verbinding maken);

5. accounts en wachtwoorden:

- het gebruik van sterk uniform wachtwoordbeleid voor gebruikerswachtwoorden (zoals wachtwoordlengte, complexiteit, vergrendelingsteller, wijzigingsintervallen), of het gebruik van 2-factor authenticatie (zie hoofdstuk 3.2.1 e.v.);
- het - conform het wachtwoordbeleid - beschermen van alle accounts met ten minste een wachtwoord;
- het - conform het wachtwoordbeleid - vervangen van alle bestaande standaard (default) wachtwoorden door eigen wachtwoorden;
- het - na meerdere verkeerd invoeren van het wachtwoord - blokkeren van het lokale beheeraccount (Local Administrator Account);
- het gebruik van eigen persoonsgebonden beheeraccounts (Administrator Accounts);
- het deactiveren of hernoemen van standaard gebruikersaccounts;
- het uitschakelen van lokale gastaccounts (Local Guest Accounts);
- het inzetten van niet-gemachtigde gebruikersaccounts om processen uit te voeren;
- het blokkeren van - via het netwerk aanmelden van - lokale gebruikersaccounts;
- het uitschakelen van standaard (default), test- en anonieme accounts voor alle geïnstalleerde services/softwareonderdelen;

6. netwerkcomponenten

- het instellen van restricties voor netwerkinstellingen (zoals TCP/IP-configuratie) en het afsluiten van ongebruikte netwerkprotocollen;
- het tot het noodzakelijke minimum beperken van verbindingen die door een service worden uitgevoerd;
- het - zo nodig - activeren van pakketfilters/firewalls en het slechts openstellen van de minimaal vereiste toegangpoorten.

Voor de gangbare server besturingssystemen zijn op internet gedetailleerde hardening-richtlijnen publiekelijk beschikbaar:

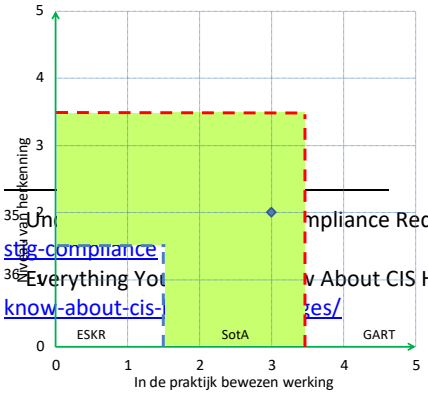
- STIGs[35] (Security Technical Implementation Guides): https://iase.disa.mil/stigs
- CIS-benchmarks[36] (Center for Internet Security, Inc.): https://www.cisecurity.org/cisbenchmarks
- Microsoft-beveiligingsrichtlijnen: https://blogs.technet.microsoft.com/secguide/

Een groot aantal van de vermelde hardening maatregelen kan worden gerealiseerd door technische instellingen. Deze instellingen kunnen met een hardening-pakket (zoals scripts) automatisch worden gedistribueerd naar alle serversystemen van de organisatie. Nieuwe serversystemen moeten direct na installatie met het hardening-pakket worden gehard. Bij het hardenen van bestaande systemen, met een hardening-pakket, kan hardening leiden tot falen van functionaliteit, daarom moet vooraf een gegevensback-up worden gemaakt en het gehardende serversysteem moet uitgebreid worden getest.

Welke beschermingsdoelstellingen dekt deze maatregel af?

☒ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☒ Authenticiteit

Classificatie van het technologieniveau



[35] Un mpliance Requirements: https://www.solarwinds.com/federal-government/solution/disa-stig-compliance
[36] Everything Yo v About CIS Hardened Images: https://www.cisecurity.org/blog/everything-you-need-to-know-about-cis- es/

3.2.22 Eindpuntdetectie en respons platform

De bescherming van eindapparaten (bijv. PC's, laptops, smartphones of tablets) vereist nu veel meer dan alleen een antivirusprogramma. Moderne oplossingen (Endpoint-Detection & Response platforms, EDR) combineren de nieuwste beveiligingstechnologieën om alle soorten cyberaanvallen op client- en server systemen in verschillende besturingssystemen te stoppen en om de initiators te identificeren. In tegenstelling tot conventionele oplossingen is specifieke voorkennis, zoals handtekeningen of een eerste slachtoffer, niet nodig.

Tegen welke dreiging(en) wordt de maatregel ingezet?

- Malware
- Uitbuiting
- Kwaadaardige scripts
- Hacker activiteit
- Misbruik van beheertools en tools met kwade bedoelingen

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?
EDR-platforms combineren effectieve detectie-en preventie technieken om het compromitteren van clients en servers, waaronder computers en besturingssysteemlimiteringen, te voorkomen en zelfs om actieve aanvallers in computernetwerken te ontmaskeren.

Lichtgewicht agents bieden de aanvalrelevante proces telemetriedata, gebruiken lokaal effectieve machine-learning modellen (kunstmatige intelligentie) en correleren en visualiseren de tactieken, technieken en procedures op holistische wijze.

Door de allernieuwste sensor architectuur belasten de next generation EPP-oplossingen een computer slechts een fractie vergeleken met een klassieke AV-scanner en het regelmatig downloaden van handtekeningen is niet meer nodig. Dat betekent:

- signature-loze detectie en actieve blokkering van schadelijke code door machine learning-modellen (bij voorkeur lokale runtime);
- controle en registratie van programma-activiteiten over de procesketens heen en optioneal het blokkeren van schadelijk gedrag;
- bescherming tegen misbruik van kwetsbaarheden binnen legitieme applicaties (exploits en geheugen manipulatie);
- idealiter worden detecties weergegeven op een gecorreleerde manier en de techniek en tactiek (met inbegrip van de tools die worden gebruikt, zoals malware, Trojaanse paarden, PowerShell scripting, en het doelwit van de aanvaller,(ongeautoriseerd vrijgeven (exfiltratie) van gegevens, het opzetten van een backdoor, laterale beweging binnen de organisatie, rechten escalatie, enz.), worden weergegeven;
- aanvullende bedreigingsintelligentie laat zien wie de vermoedelijke acteur/vijand is (cybercriminaliteit of nationaal gemotiveerde aanval) en welke doelen en branches de aanvallers nastreven;
- Een volledig geïntegreerde sandbox-verbinding zorgt voor een veilige "detonatie" van gevonden kwaadaardige code voor verdere analyse, zonder afbreuk te doen aan de productie.

EDR-platformen pakken de volledige levenscyclus van een aanvalspoging aan. Dit is de enige manier om conclusies te trekken over de actoren en hun motivatie, die idealiter met up-to-date dreiginginformatie worden aangevuld Bovendien kunnen telemetrie gegevens van het systeem door externe deskundigen worden gecontroleerd op schadelijke indicaties.

Ook moet worden vermeld dat met het oog op een holistische bescherming van eindapparatuur, als deze aspecten niet door de respectieve EDR-oplossing zelf worden verstrekt , met name rekening moet worden gehouden met de volgende punten:

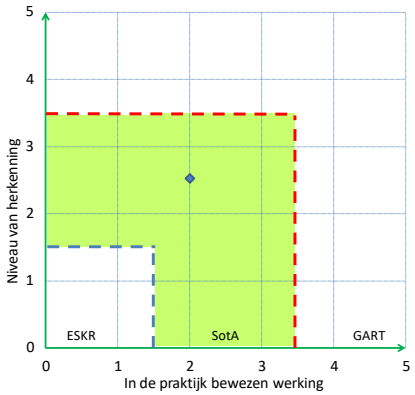
- machtigingen/rollen (trefwoord: beheer(ders)rechten);
- update mechanismen (besturingssysteem en software);
- beperkingen/controle van geïnstalleerde software;
- versleuteling van eindapparatuur;

- bescherming tegen zoals hierboven beschreven dreigingen/malware;
- voorschriften/richtlijnen voor toegestaan gebruik (privégebruik, gebruik in niet-bedrijfsnetwerken, gebruik tijdens reizen, gebruik van gegevensdragers, opslag van gegevens, back-up, enz.); In het bijzonder als de gebruiker beheer(ders)rechten heeft;
- gebruik van authenticatiemethoden (gebruikersnaam/wachtwoord, pincode, biometrie, enz.).

Welke beschermingsdoelstellingen dekt deze maatregel af?

☒ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☒ Authenticiteit

Classificatie van het technologieniveau



3.2.23 Processen

Web Isolation scheidt de werkplek van de gebruiker van de browsersessies en maakt veilig Internet gebruik mogelijk zonder beperkingen op inhoud of functies. Browser gebaseerde cyberaanvallen, data uitstroom/verlies, en de bijbehorende productiviteitsbeperkingen en imagoschade worden effectief voorkomen.

Tegen welke dreiging(en) wordt de maatregel ingezet?

Een infectie van de Workstation computer, bijvoorbeeld door:

- Browser kwetsbaarheden, drive-by downloads, infectieuze websites;
- Ransomware, APT, trojans, virussen, wormen;
- Zero-day exploits;
- kwaadaardige links in e-mails, waardoor het verspreiden van malware op het bedrijfskritische netwerk.

Welke maatregel (procedure, uitrusting of bedieningsmodus) wordt in deze sectie beschreven?
De isolatie van de browsersessies kan op verschillende manieren worden bereikt. De gebruikte architectuur en de bijbehorende beveiligingsmechanismen zijn hierbij doorslaggevend.
Voorbeelden hiervan zijn de zogenaamde "op afstand bestuurde" browser omgevingen en meerlaagse lokale browser isolaties.

Een eenvoudige isolatie van de browseromgeving (bijv. via eenvoudige virtualisatie op basis van Hyper-V of zogenaamde browser Sandboxing) biedt onvoldoende bescherming tegen de bovengenoemde bedreigingen, bijvoorbeeld, omdat ze niet een standaard een veilig gehard besturingssysteem bevat waarin de browser wordt uitgevoerd; geen gebruik maakt van extra veilige netwerksegmentatie; geen beveiligde copy & paste functie heeft, of geen extra beveiligingsfuncties benut, zoals gegevens vergrendelingen. Daarom is deze methode niet geschikt voor het bestrijden van de bedreigingen.

Op afstand bestuurde browseromgevingen op basis van ReCoBS
Het op afstand bestuurde browser systeem (ReCoBS) scheidt het Internet gebruik fysiek van de

werkcomputer van de gebruiker. Elke browsersessie wordt buiten het gevoelige netwerkgebied in een speciaal geïsoleerde omgeving uitgevoerd, binnen een speciaal gehardend systeem, op afzonderlijke hardware en in een afzonderlijk netwerksegment (DMZ).

Via een technisch beveiligd communicatiekanaal wordt de browser op afstand bediend via de videostream op het externe systeem van het werkstation. Het merendeel van de aanvallen gericht op Windows-gebaseerde kwetsbaarheden worden in de geharde Linux-omgeving succesvol afgeweerd. Andere beveiligingsmechanismen en zones in de overall architectuur bieden ook nog betrouwbare bescherming tegen aanvallen, zelfs als de browser is aangetast. De fysieke scheiding van werkstation en het browsersysteem biedt ook bescherming tegen hardware gerelateerde aanvallen (Spectre, Meltdown, ZombieLoad of kwetsbaarheden in de hypervisor).

Op gezette tijden (standaard eenmaal per dag) moet het externe systeem via een systeemkopie worden teruggezet in de oorspronkelijke staat, zodat schadelijke code effectief wordt verwijderd. Het is belangrijk om ervoor te zorgen dat de kopie van de systeeminstallatie integer wordt bewaard.
Het werkstation van de gebruiker heeft niet op elk moment een directe toegang tot het Internet nodig en is daarom extra beschermd, bijvoorbeeld tegen het opnieuw laden van schadelijke code door infectieuze documenten die de computer via andere middelen hebben bereikt, bijvoorbeeld via e-mail of USB-stick.

Aangezien de ReCoBS-architectuur de standaardfuncties van de browser in principe op het externe systeem uitvoert, zijn aanvullende ontwikkelingen noodzakelijk voor de acceptatie van de gebruikers, zodat de op afstand bestuurde browser niet significant verschilt van het gebruik van de lokale browser en alle gebruikelijke functies zoals persoonlijke bladwijzers, copy & paste, afdrukken en up- en down-loads in principe beschikbaar zijn.

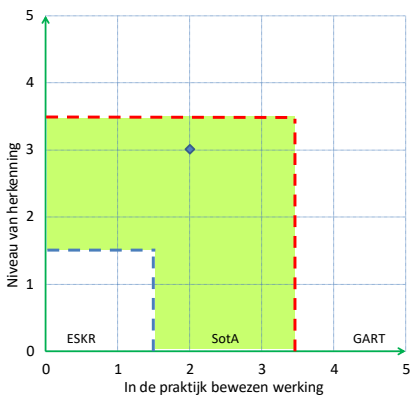
Voor de optionele overdracht van bestanden (browser downloaden/uploaden) tussen het externe systeem en het werkstation, moeten aanvullende controlemechanismen worden opgegeven, die opvallende bestanden in quarantaine plaatsen en beheerders waarschuwen. Een voorbeeld van een dergelijk controlemechanisme is de anti-virus bescherming in de data-gateway. Het is ook raadzaam dat de algemene oplossing centraal worden beheerd, zodat een bestaande directory-service kan worden gekoppeld en gebruikt om de gebruikersrollen te beheren.

Webisolatie op basis van lokale virtualisatie van de browser toepassing
Een andere benadering van webisolatie is gebaseerd op het lokaal inkapselen van de browser toepassing via veilige virtualisatie in combinatie met een in rechten beperkt Windows-gebruikersaccount, een gehard gastbesturingssysteem en het via afzonderlijke VPNTunnels scheiden van internet/intranet naar de internet-gateway. Dit voorkomt directe toegang van de browsersessie tot de Hardware van de PC.

Een voordeel van lokale browser isolatie is, dat ze zelfstandig gebruikt kan worden op mobiele workstations. De niet-aanwezige fysieke scheiding tussen het gevoelige werkstation en het browsersysteem kan echter leiden tot misbruik van lokale beveiligingskwetsbaarheden in de hardware of -software van de processor, om in het eindapparaat in te breken via een all-Layer exploit package.

Welke beschermingsdoelstellingen dekt deze maatregel af?
☐ Beschikbaarheid
☒ Integriteit
☒ Vertrouwelijkheid
☒ Authenticiteit

Classificatie van het technologieniveau



3.3 Organisatorische maatregelen

Omdat informatie- en communicatievoorzieningen in beginsel niet altijd zijn ontworpen voor beveiliging, en technische beveiliging alleen effectief is wanneer deze adequaat gepaard gaat met organisatorische en personele maatregelen, heeft elke organisatie een systeem van methoden, procedures en regels nodig voor het beheren van de operationele informatiebeveiliging; met andere woorden: een informatiebeveiliging beheersysteem (Information Security Management System of ISMS).

Vanuit een ISMS worden regels gesteld en implementeert voor het classificeren van en omgaan met gevoelige informatie. Het ISMS is een belangrijk onderdeel van het beheersysteem en loopt door alle belangrijke geledingen van de organisatie. Het ISMS bevat procedures voor regelmatige inspectie en documentatie van organisatorische en technische wijzigingen.

Een belangrijk aandachtspunt van het ISMS is het onderzoeken van veranderingen in informatiebeveiliging, bij geplande veranderingen en onderhoud van de belangrijke elementen van de IT-infrastructuur. Een ander aspect is regelmatige training en bewustmaking van het personeel. Het ISMS bepaalt ook hoe noodpreventie moet worden uitgevoerd en hoe kan worden gereageerd op mogelijke beveiligingsincidenten. Het doel van het ISMS is het waarborgen van permanente naleving en het waarborgen van een efficiënt en altijd adequaat beveiligingsniveau.

Met het document “Informationssicherheitsmanagement - Praxisleitfaden für Manager" geeft TeleTrusT een bruikbare richtlijn voor het beheren van informatiebeveiliging. Het document toont dat met informatiebeveiliging beheer en bijbehorende compliance- en risicocultuur, een strategisch controle-instrument beschikbaar kan zijn, dat de veiligheidssituatie in een oogopslag zichtbaar maakt.

3.3.1 Normen en standaarden

Er zijn een aantal internationale standaarden en normen die kunnen dienen als basis voor het implementeren van een ISMS. In tegenstelling tot technische maatregelen zijn de voortdurende veranderingen in organisatorische maatregelen een permanent fenomeen, zodat verwijzing naar standaarden en normen mogelijk is, ook in de context van State of the Art. De ISO/IEC 27000-serie wordt gebruikt als referentiepunt voor verdere standaarden en normen. Er zijn enkele overlappingen; de overlappingen kunnen gewoonlijk als synergie worden gezien, zodat zij in termen van informatiebeveiliging een positieve invloed kunnen hebben op de standaarden. Voor zover aanvullende normen of normen worden toegepast voor het beheer van IT-diensten, -processen of -risico's, moeten de behandelde overlappingen worden geïdentificeerd en gebruikt.

De ISO 27000-standaarden

De ISO/IEC 27000-serie (kortweg ISO27K) is een reeks IT-beveiliging standaarden. Deze standaarden worden gepubliceerd door de International Organization for Standardization (kortweg: ISO) en de International Electrotechnical Commission (kortweg: IEC).

ISO/IEC 27001 is de bekendste standaard in de ISO/IEC 27000-serie, het formuleert de eisen waaraan een ISMS moet voldoen. Voor concrete implementatie bestaan ook andere standaarden en richtlijnen.

De ISO/IEC 27000-serie bevat onder andere de volgende hoofditems, die elk fungeert als een afzonderlijke standaard en samen een normenreeks vormen.

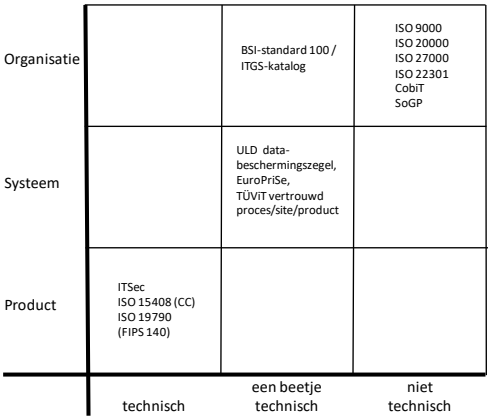
Standaard	Gebruikt voor de volgende taken
NEN-ISO/IEC 27000	Managementsystemen voor informatiebeveiliging, Overzicht en woordenlijst
NEN-ISO/IEC 27001	Managementsystemen voor informatiebeveiliging, Eisen (voor een ISMS)
NEN-ISO/IEC 27002	Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging
NEN-ISO/IEC 27003	Managementsystemen voor informatiebeveiliging, Handleiding
NEN-ISO/IEC 27004	Managementsystemen voor informatiebeveiliging, Monitoring, meting, analyse en evaluatie

NEN-ISO/IEC 27005	Beveiligingstechnieken, Risicobeheer voor informatiebeveiliging
NEN-ISO/IEC TR 27019	Beveiligingstechnieken, Besturingselementen voor informatiebeveiliging voor de energie-industrie
NEN-ISO/IEC 27031	Beveiligingstechnieken, Concepten en principes met betrekking tot IT-ondersteuning voor bedrijfscontinuïteit
NEN-SO/IEC 27034	Informatietechnologie, Applicatiebeveiliging deel 3: beheerproces
NEN-ISO/IEC 27035	Beveiligingstechnieken, Incidentbeheer deel 1: principes

Tabel 1: Overzicht van de ISO/IEC 27000-serie

Andere standaarden en normen
Informatiebeveiliging standaarden en criteria kunnen, afhankelijk van het beschouwingniveau, worden geclassificeerd als bedrijfs-, systeem- en productstandaarden. Op basis van hun formulering kunnen ze worden ingedeeld in technische, minder technische en niet-technische normen.

Geïnspireerd op een eerdere presentatie van initiatief D21 kunnen bovenstaande structuurniveaus als volgt worden geschetst:



Figuur 5: Structuurniveaus van – voor informatiebeveiliging - relevante standaarden en normen

De in ISO 27001 uiteengezette specificatie van de beperkingen van ISO 9001, ISO 20000-1, ISO 22301, **CObIT** en The Standard of Good Practice (**SoGP**) zijn in niet-technische taal geformuleerd en zijn in het bijzonder van toepassing op bedrijven en openbare instellingen (organisaties).

ISO 27000 e.v.
De reeks standaarden in ISO 27000 e.v. bevat verschillende standaarden met betrekking tot het ISMS. De kern van de reeks is ISO/IEC 27001, waarin eisen worden beschreven voor een functionerend ISMS in de context van een organisatie (zie 3.3.1.1).

ISO 27001 op basis van de BSI IT-Grundschutz
Dit betreft de implementatie van ISO 27001 met behulp van de BSI IT-Grundschutz (de IT basisbescherming catalugus) van het BSI (ook gedocumenteerd in BSI-standaard 100-2).

De BSI-standaard 100-1 definieert de algemene eisen aan een ISMS. In principe is deze compatibel met ISO-standaard 27001 en bovendien worden de aanbevelingen van andere ISO-standaarden in de ISO 2700x-familie, zoals ISO 27002, in overweging genomen. Het biedt geïnteresseerden een gemakkelijk te begrijpen en systematische inleiding en een reeks instructies, ongeacht welke methode gebruikt wordt om deze samenwerken te implementeren.

BSI-standaard 100-2 biedt elementaire IT-bescherming:

- specifieke en methodische hulp voor het stapsgewijs invoeren van een ISMS;
- gericht op de individuele fases van het informatiebeveiliging proces;

- oplossingen uit de praktijk, d.w.z. best practice benaderingen;
- mogelijkheid tot certificering.

De begrenzing van de originele ISO 27001-en de implementatie van de basis beschermingsaanpak van de BSI is te zien in onderstaande tabel:

categorie	**ISO 27001**	**BSI** Grundschutz
reguleringsgebied (scope)	relevante normen <100 pagina's	BSI Grundschutz-Katloge > 4000 pagina's
eisen (requirements)	abstracte en generieke randvoorwaarden	concrete voorbeelden van praktische maatregelen
risicoanalyse	volledige analyse van elk doelobject	vereenvoudigde analyse in geval van verhoogde beschermingseis
maatregelen	ongeveer 150 conceptuele eisen	> 1100 concrete maatregelen
certificering	certificering	auditcertificaat + certificering
geldigheid	3 jaar, jaarlijkse observatie-audits	3 jaar, jaarlijkse observatie-audits

Tabel 2: Differentiatie van ISO 27001 versus de BSI IT-Grundschutz

ISO 20000-1
Deze norm specificeert eisen aan (interne of externe IT) organisaties met betrekking tot de uitvoering van procesgerichte services. Een deel van de vereiste processen (voornamelijk informatiebeveiliging beheer, incidentbeheer (incident & event management) en service continuïteitsbeheer) overlappen met ISO 27001. Conventioneel wordt ISO 20000-1 toegepast op IT-organisaties, terwijl het bereik van ISO 27001 van toepassing kan zijn op alle soorten organisaties.

ISO 22301
Deze standaard betreft het veiligstellen van de bedrijfscontinuïteit (Business Continuity Management, of BCM) en specificeert eisen voor BCM-systemen in organisaties. BCM-systemen zoals beschreven in ISO 22301 verwijzen ook (maar niet beperkt tot) naar IT. Het onderwerp BCM is ook een onderwerp binnen de ISO 27001, maar alleen vanuit het perspectief van informatiebeveiliging (d.w.z. In hoeverre de bedrijfscontinuïteit kan worden aangetast door informatie beveiligingsincidenten).

ISO 9001
Deze standaard specificeert eisen voor kwaliteitmanagement systemen (KMS), maar omvat ook een enorm aantal informatiebeveiliging overwegingen, zoals sommige met betrekking tot verplichtingen ten aanzien van:
- labeling, opslag, bescherming en herstelbaarheid van logs;
- onderzoek, levering en onderhoud van infrastructuur, zoals gebouwen, werkplekken en bijbehorende nutsvoorzieningen, procesapparatuur (zoals hardware en software) en ondersteunende diensten (zoals communicatie- en informatiesystemen);
- bescherming van eigendom van klanten, zoals intellectuele eigendom, persoonsgegevens, enz.

Control Objectives for Information and related Technology (CObIT)
CObIT is een methode om de risico's die voortvloeien uit de inzet van IT, ter ondersteuning van bedrijfsrelevante processen, te beheersen. CObIT is een op revisie en control gerichte toolkit voor het management, dat met het meten diensten en resultaten (prestatiemeting) voor alle IT-processen definieert; elk met gedefinieerde besturingsdoelen, volwassenheidsmodellen en maatregelen. CObIT heeft betrekking op alle IT-processen, terwijl ISO 27001 zich richt op de beheersing van informatiebeveiliging processen, elk met gedefinieerde besturingsdoelen, volwassenheidsmodellen en maatregelen. CobiT is specifiek gericht op alle IT-processen, terwijl ISO 27001 zich richt op het beheersen van de informatiebeveiliging processen.

De Standard of Good Practice for Information Security (SoGP)
De SoGP van het ISF is een goede praktijkbenadering voor bedrijfsinformatiebeveiliging, die ook het

benchmarken van beveiliging mogelijk maakt. De standaard behandelt verschillende thematische onderdelen van informatiebeveiliging (zoals IT-beveiliging beheer, bedrijfskritieke applicaties, informatieverwerking, communicatie/netwerken en systeemontwikkeling) vanuit een zakelijk perspectief en biedt een alternatief, deels complementair zicht op de ISO 27001.

3.3.2 Processen

Het BSI stelt vast dat het onmogelijk is om industriestandaarden, op een generieke en uitputtend te beschrijven. In plaats daarvan kunnen ze aan de hand van bestaande nationale en internationale normen, zoals DIN- of ISO-standaarden, en met behulp van op het betreffende gebied succesvolle praktijkvoorbeelden, worden bepaald.

Voor organisaties die direct of indirect te maken hebben met ITSiG, betekent dit dat een verscheidenheid aan algemene en branchespecifieke normen en normen moet worden nageleefd, gecontroleerd en, indien nodig, gecertificeerd.

De volgende secties bevatten een korte beschrijving van de noodzakelijke organisatorische maatregelen, evenals een beoordeling van de normen van de ISO/IEC 27000-reeks moeten worden toegepast om te voldoen aan de State of the Art. De inhoud van dit hoofdstuk dient als leidraad.
De voortdurende vooruitgang van de technologie zorgt er echter voor, dat ook de officiële kaders en standaarden regelmatig worden bijgewerkt.

De beschouwing van de State of the Art vereist daarom individueel onderzoek naar de mate waarin een individuele maatregel of reeks van maatregelen op een bepaald moment geschikt, noodzakelijk en passend is.

In tegenstelling tot de technische maatregelen volgens welke systemen of technische processen ervoor zorgen dat informatie wordt beschermd, beschrijven organisatorische maatregelen processen, werkinstructies, richtlijnen e.d. die een organisatie zich zelf oplegt en welke bedoeld zijn om de beveiliging te vergroten. Implementatie en naleving zijn meestal de verantwoordelijkheid van de betrokken personen en worden het best ondersteund door technische maatregelen. Regelmatige controle en training zorgen ervoor dat de geplande maatregelen correct worden uitgevoerd.

De actieve ondersteuning van het management en de samenwerking met gespecialiseerde afdelingen is van noodzakelijk voor de introductie van een ISMS. Het is belangrijk om de risico's te identificeren en te beoordelen, die van invloed zijn op de bedrijfswaarden van infrastructuur, personeel, IT, processen, informatie en daarbij negatief effect hebben op een of meer kernwaarden van informatiebeveiliging (zoals vertrouwelijkheid, integriteit, beschikbaarheid).

Hieronder volgen de primaire organisatieprocessen en -maatregelen die kunnen worden afgeleid van de State of the Art praktijk.

3.3.2.1 Beveiligingsorganisatie

Beveiligingsorganisatie streeft naar het invoeren van een beheerskader. De beschrijving van beveiligingsorganisatie omvat de taken en verantwoordelijkheden die betrokken zijn bij het initiëren en bewaken van de bewaken van de werking van informatiebeveiliging binnen de organisatie.

Opdat een ISMS met succes kan worden geïntroduceerd en geëxploiteerd, moet het hoogste management:

- dragen van de algemene verantwoordelijkheid voor het ISMS en voor de informatiebeveiliging in de organisatie;
- sensitief zijn en alle relevante verantwoordelijke personen en medewerkers informeren over mogelijke risico's en persoonlijke aansprakelijkheid in geval van het niet naleven van de eisen en – indien van toepassing - van een ISMS; en het doorgeven van verantwoordelijkheden met betrekking tot informatiebeveiliging;
- een effectieve beveiligingsorganisatie in de vorm van rollen, verantwoordelijkheden en taken definiëren, implementeren en continu verbeteren;
- organisatiestructuren (zoals afdelingen, groepen, competentiecentra), rollen en taken bepalen met het oog op het beheer van informatiebeveiliging.

De minimumeisen waaraan een beveiligingsorganisatie mort voldoen zijn:
- het benoemen van een verantwoordelijke manager (waarvan de voorzitter of directeur direct verantwoordelijk is voor informatiebeveiliging); en
- het benoemen van een Chief Information Security Officer (CISO) als een centrale rol binnen de IS-organisatie.

De basisregels die welke onder alle omstandigheden in acht genomen moeten worden zijn:
- de algemene verantwoordelijkheid ligt op managementniveau;
- elke medewerker is voor zijn/haar werkomgeving verantwoordelijk voor informatiebeveiliging.

De belangrijke rollen en verantwoordelijkheden binnen een beveiligingsorganisatie zijn:

Hoger management (directeuren, bestuur):
- strategische verantwoordelijkheid (dedicated), en in laatste instantie ook de algemene verantwoordelijkheid voor informatiebeveiliging;
- verantwoordelijkheid voor alle risicogerelateerde beslissingen.

Chief Information Security Officer (CISO):
- tactische of (soms) operationele controle van de informatiebeveiliging;
- ondersteuning van het management in IS taakbewustzijn;
- staffunctie met het directe recht en plicht om aan het hoogste managementniveau te rapporteren.

Informatie beveiligingsfunctionaris (ISO):
- operationeel beheer van de informatiebeveiliging, waar nodig tactische taken voor individuele afdelingen;
- organisatorisch rechtstreeks toegewezen aan de CISO.

IS Management Team / IS Management Forum / Beveiliging Stuurgroep:
- permanente commissie voor het coördineren van de planning en implementatie van maatregelen voor informatiebeveiliging;
- bestaat uit CISO, ISO('s), plaatsvervangers voor implementatie, gespecialiseerde managers, functionaris voor gegevensbescherming (DPO/FG) en vertegenwoordigers van het senior management;
- overleg- en controlefunctie voor de CISO.

Functionaris voor gegevensbescherming (FG of DPO):
- niet noodzakelijkerwijs onderdeel van het IS-managementteam, maar in plaats daarvan een belangrijk contactpersoon op het gebied van compliance, idealiter regelmatig betrokken bij het Informatiebeveiliging beheerproces.

Auditmanager:
- centraal contact voor interne en externe audits
- coördineert en beheert de planning en uitvoering van audits;
- ondersteunt CISO in hun taken.

Organisatorische maatregelen zijn State of the Art, als ze worden uitgevoerd in overeenstemming met de huidige standaarden. Voor de maatregelen moeten ten minste de normen uit 27000-27005 (uit de ISO/IEC 27000-serie) worden nageleefd. Als verdere toepasselijke eisen, normen of resultaten van risicoanalyses dit vereisen, kunnen nog aanvullende organisatorische maatregelen nodig zijn.

3.3.2.2 Requirements management (Vereisten beheer)
Een gerichte en effectieve ISMS kan alleen worden opgezet ingericht in de context van de specifieke organisatie en haar eisen aan informatiebeveiliging. Daarom moeten de eisen die relevant zijn voor beveiliging worden bepaald en de implementatie ervan worden gepland, gerealiseerd, gecontroleerd en voortdurend worden verbeterd.
Requirements management vormt de basis voor het uitlijnen van informatiebeveiliging als een proces en een conditie binnen de organisatie.

Het voortdurend voldoen aan de eisen is garantie voor de tevredenheid van de belanghebbende

partijen (stakeholders) van een ISMS. Vanwege de complexiteit, is het raadzaam om een beheerproces voor de eisen vast te stellen.

De eisen aan een organisatie kunnen worden ingedeeld in:
- wettelijke eisen;
- contractuele eisen; en
- andere eisen.

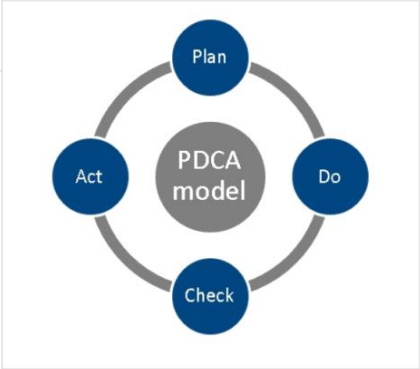
Wettelijke eisen vloeien voort uit verschillende rechtsgebieden, zoals gegevensbeschermingsrecht, arbeidsrecht, IT-recht, strafrecht en nog veel meer (een uniforme wet voor informatiebeveiliging bestaat niet).

Met betrekking tot aantoonbare informatiebeveiliging kunnen eisen (en verwachtingen) in toenemende mate worden doorgevoerd door de verschillende zakelijke partners van de organisatie, zoals door klanten, leveranciers, dienstverleners, outsourcing partners, samenwerkingspartners, verzekeringsmaatschappijen, enz. Wettelijke en contractuele eisen worden vaak ' primaire ' of ' elementaire ' eisen genoemd, omdat ze de basis vormen van het informatiebeveiliging proces.

Andere eisen (en/of verwachtingen/beperkingen) vloeien veelal voort uit de volgende entiteiten:

- markt;
- algemeen publiek;
- het bedrijf, hoofdkantoor;
- aandeelhouders;
- werknemers;
- bedrijfsprocessen (inclusief intern gedefinieerd beleid);
- technologie.

Een State of the Art-proces voor Requirements management kan in een PDCA-model als volgt worden weergegeven:



Afbeelding 6: PDCA model

PLAN: Allerlei eisen en verwachtingen van de organisatie,
- vastleggen;
- analyseren;
- beoordelen; en
- converteren naar interne (beveiligings-)specificaties voor de organisatie.

DO: Het voldoen aan de informatiebeveiliging specificaties van de organisatie (en impliciet ook aan de eisen en verwachtingen van de organisatie), zoals in de vorm van:
- organisatorische maatregelen: beleid, voorschriften, richtlijnen;
- personeel gerelateerde maatregelen, waaronder personeelsbeoordeling, informatiebeveiliging gevoelig/bewust maken, voortdurende training;
- technische maatregelen voor toegangscontrole, codering enz.;
- infrastructurele maatregelen voor toegangscontrole, veiligheidszones.

CHECK: Het monitoren en reviewen van de mate waarin aan de informatiebeveiliging specificaties van de organisatie (en daarmee impliciet ook aan de eisen en verwachtingen van de organisatie) wordt voldaan:

- opvragen van indicatoren en parameters;
- identificeren van tekorten (in interactie met de stakeholders);
- planning van corrigerende maatregelen.

ACT: Het continu verbeteren van de mate waarin aan de informatiebeveiliging specificaties van de organisatie (en daarmee impliciet ook aan de eisen en verwachtingen van de organisatie) continu verbeteren:

- het implementeren van corrigerende maatregelen en het controleren van hun werkzaamheid;
- het communiceren van verbeteringen.

Requirements management garandeert het naleven van wettelijke, contractuele en andere eisen en zorgt ervoor dat schending van wet en regelgeving, van contractuele en andere verplichtingen met betrekking tot informatiebeveiliging worden vermeden. Positieve beoordeling van het ISMS en de bereikte informatiebeveiliging, zorgen ervoor dat ze adequaat worden uitgevoerd en beheerd in overeenstemming met het beleid, procedures en relevante eisen aan de organisatie.

3.3.2.3 Beheer van het toepassingsgebied

De toepassing en reikwijdte van een ISMS moeten altijd rekening houden met de eisen die de organisatie stelt aan informatiebeveiliging. De scope ontwikkelt zich dienovereenkomstig.
Passende wijzigingen moeten zorgvuldig worden gepland en uitgevoerd. Documentatie en verantwoording van het toepassingsgebied moeten worden verstrekt als bewijs van de State of the art.

3.3.2.4 Beheer van informatiebeveiligingsrichtlijnen

Als basis voor een ISMS moet de focus van het management van de organisatie gericht zijn op informatiebeveiliging. Hiertoe dient het management richting aan te geven en de beschermende doelen dienen in overeenstemming te zijn met de bedrijfsvereisten en de relevante wet- en regelgeving.

Om te voldoen aan de State of the Art moeten het beleid en de doelen voor informatie worden gedefinieerd in de vorm van een richtlijn en verplicht worden gesteld binnen de organisatie. Verder moeten ook voldoende middelen beschikbaar worden gesteld en moet het belang van het voldoen aan de eisen worden bekend gemaakt worden. De richtlijn (met inbegrip van de doelstellingen op het gebied van informatiebeveiliging) moet ten minste eenmaal per jaar worden gecontroleerd op relevantie en relevantie en, indien nodig, verbeterd.

3.3.2.5 Risk management (Beheer van risico's)

Risicobeheer bestaat uit systematische risicobeoordeling, identificatie, monitoring van en omgaan met risicogebieden. Het doel is om de kansen en risico's voor de onderneming systematisch te identificeren en deze risico's te beoordelen op basis van de waarschijnlijkheid van optreden en de kwantitatieve gevolgen op waarde van de organisatie.

Om te voldoen aan de State of the Art moeten regels worden gedefinieerd voor risicobeheer, om voor de organisatie de eigen waarden, kwetsbaarheden, dreigingen, effecten en waarschijnlijkheid van gebeurtenissen en de toelaatbare omvang van het restrisico te bepalen. De methodologie voor het implementeren van risicobeoordeling en -behandeling, evenals de vaststelling van restrisico's door het senior management, moet ook worden vastgesteld. Ook moeten de methode voor het uitvoeren van risicobeoordeling en -behandeling, en voor het door het topmanagement accepteren van de restrisico's worden vastgesteld.

De bestaande risico's moeten op basis hiervan worden geanalyseerd, geëvalueerd en aangepakt. De restrisico's moeten aantoonbar door het hoogste management worden overgenomen en de risicosituatie van de organisatie moet voortdurend worden geoptimaliseerd.

3.3.2.6 Beheer van de verklaring van toepasselijkheid

Een verklaring van toepasselijkheid moet altijd up-to-date gedocumenteerd zijn, welke controles van toepassing zijn vanaf bijlage A van ISO 27001 (mogelijk ook andere veiligheidsmaatregelen) en welke niet, de redenen voor dit besluit en een beschrijving van de wijze waarop deze maatregelen moeten

worden uitgevoerd. Volgens de State of the Art biedt de verklaring van toepasbaarheid in de respectieve beoordelingscyclus een actueel beeld van de doelstelling en de feitelijke staat van informatiebeveiliging in een organisatie.

3.3.2.7 Resource management (beheer van bedrijfsmiddelen)

De organisatie moet de noodzakelijke middelen identificeren, leveren en voortdurend aanpassen voor de ontwikkeling, implementatie en onderhoud van het ISMS en deze continu te verbeteren.

State of the Art-praktijk vereist dat de beschikbare middelen minimaal voldoen aan de basis vereisten.

3.3.2.8 Kennis- en competentie management

Wil een ISMS professioneel te kunnen functioneren, dan moeten de personen die hiervoor verantwoordelijk zijn over de juiste competenties beschikken of daartoe worden opgeleid door middel van bijscholing. Om te voldoen aan de State of the Art, moet de behoefte aan kennis en competenties worden bepaald en verworven en voortdurend worden aangepast aan de werkelijke behoefte.

3.3.2.9 Beheer van documentatie en communicatie

Het doel is om zowel de opzet als de feitelijke toestand van het ISMS en de informatiebeveiliging te documenteren, met inbegrip van het verwezenlijken van de doelstellingen, de behandeling van de risico's en het naleven van de eisen, en de doelstelling van de belanghebbende partijen.
Om aan State of the Art te voldoen, moeten - voor alle te controleren maatregelen - de nodige documenten zijn opgesteld en aantoonbaar zijn beschikbaar zijn gesteld.

3.3.2.10 IT-Service management (beheer van IT-diensten)

IT Service Management biedt een aanpak op alle niveaus van IT-beheer en op alle niveaus van bedrijfsoriëntatie, service ontwerp en informatiebeveiliging, tot en met implementatie en infrastructuur en het bijbehorend gebruik van technologie. Het is belangrijk om het beveiligingsproces in te bedden in het proceslandschap van de organisatie.

Aanvullend op de interfaces en processen die worden beschreven in het TeleTrusT-document "Informationssicherheitsmanagement - Praxisleitfaden für Manager", moeten de volgende processen in acht worden genomen, in het bijzonder om te voldoen aan de State of the Art:

Bedrijfsmiddelenbeheer (Asset Management)
Bedrijfsmiddelenbeheer beschrijft drie belangrijke aspecten van de bedrijfswaarden van de organisatie en vormt de basis voorde analyse en beoordeling van risico's (zie ook 3.3.2.5); de verantwoordelijkheden, classificatie en behandeling van media. Om de verantwoordelijkheden te bepalen, worden de bedrijfswaarden geïdentificeerd en wordt een passende verantwoordelijkheid voor de bescherming gedefinieerd. Zodra de waarden en verantwoordelijke rollen zijn gedefinieerd, zorgt classificatie ervoor dat de informatie adequaat wordt beschermd in overeenstemming met het belang ervan voor de organisatie. Beleid voor mediaverwerking zorgt ervoor dat de ongeoorloofde bekendmaking, wijziging, verwijdering of vernietiging van op media opgeslagen informatie wordt vermeden.

Training en bewustzijn
Het verhogen van de bewustwording van werknemers is een essentiële voorwaarde voor de implementatie van het gewenste veiligheidsniveau. Medewerkers moeten het belang van informatiebeveiliging in het bedrijf kennen en hoe ze persoonlijk kunnen bijdragen aan het bereiken van dit doel. Zij moeten zich bewust ook zijn van het gedrag in geval van vermoeden of ontdekken van veiligheidsincidenten. Om hun taken uit te voeren en in het belang van de informatiebeveiliging, moeten de werknemers periodiek worden opgeleid om alle relevante organisatorische en technische voorwaarden te kunnen beheersen. Scholing en training helpen werknemers om (IT) technologie goed te gebruiken en om te voldoen aan alle noodzakelijke voorschriften. Deze aspecten moeten mogelijk worden behandeld als onderdeel van het proces voor resource management (zie 3.3.2.7).

Operatie
De besturing van een beveiligingsorganisatie en- omgeving is ontworpen om alles te doen om netwerk-, computer- en server systemen en applicaties en oplossingen veilig en beveiligd te houden. Het zorgt ervoor dat werknemers, applicaties en servers de juiste toegangsrechten hebben voor de toegang tot de bronnen die hen zijn toegestaan, en dat controle is ingesteld via bewaking, audits en

rapportage. De besturing vindt plaats na het implementeren en testen van een systeem en zorgt voor continu onderhoud, updates en controles.

Referentiemodellen voor IT-Service Management (zoals ITIL) bieden een raamwerk voor succesvolle werking. Op deze manier kunnen de informatiebeveiliging beheerprocessen nauw verbonden zijn met de andere IT-processen.

Incidentbeheer
In reactie op gedetecteerde of potentiële beveiligingsincidenten worden de technische en organisatorische maatregelen binnen het incidentbeheer proces gecombineerd. Aanvullend op detectie, analyse en beheer van problemen, kwetsbaarheden en gerichte aanvallen, wordt ook beschreven en gepland hoe dergelijke incidenten, waaronder ook organisatorische en juridische kwesties, moeten worden afgehandeld.

Het doel van incidentbeheer is het plannen, identificeren en implementeren van voorwaarden, om in geval van incidenten zonder tijdverlies effectieve en efficiënte maatregelen te treffen om de organisatie te bescherming.

Continuïteitsbeheer
Continuïteitsbeheer combineert technische en organisatorische maatregelen ter voorkoming van operationele downtime. Aanvullend op het vastleggen, analyseren en beheren van de standaard risico's en de effecten langs de tijdlijn, beschrijft en plant het ook hoe ingeval van noodsituaties met escalatie van incidenten, die ook organisatorische en juridische kwesties kunnen omvatten, afgehandeld moeten worden.

Het doel van continuïteitsbeheer is het plannen, identificeren en implementeren van voorwaarden, om ingeval van nood zonder tijdverlies effectieve en efficiënte maatregelen te treffen om de organisatie te bescherming.

Inkoop *(p*rocurement)
Voorafgaand aan de daadwerkelijke aanschaf van IT-systemen of -diensten, moeten enkele voorbereidende stappen worden ondernomen, om ervoor te zorgen dat het resultaat voldoet aan de behoeften van de organisatie. Dit geldt zowel voor de inhoud als voor veiligheidsgerelateerde aspecten. Deze punten omvatten bijvoorbeeld:

- analyse van de eisen;
- analyse van de risico's;
- analyse van de beveiliging (van functie en betrouwbaarheid);
- test- en acceptatieplan.

Als leveranciers betrokken zijn bij de lange termijn levering van software, oplossingen of diensten, is het noodzakelijk om ervoor te zorgen dat de bescherming van de bedrijfswaarden, die voor leveranciers toegankelijk zijn, gewaarborgd is. Dit omvat in het bijzonder serviceniveaus en het beveiligingsniveau dat is beschreven in de leveranciersovereenkomst.

Softwareontwikkeling en IT-projecten
IT-projecten moeten van meet af aan op transparante en meetbare wijze het onderwerp informatiebeveiliging behandelen. Projectorganisaties moeten groeien naar een strenger, herhaalbaar proces dat in elke fase de veiligheid als een elementaire bouwsteen omvat en voor elke fase van het project bindende verantwoordelijkheden vastlegt voor het beveiligingsmanager (Security Manager).Deze eisen moeten door het management opnieuw worden bevestigd en gelegitimeerd. Vooral bij faseovergangen moet een formele regel voor goedkeuring worden vastgesteld om het verplichte aspect van Secure by Design in het IT-proces te onderstrepen.

De ervaring leert dat het beveiligingsteam nauw moet samenwerken met het projectteam, in het bijzonder in de planning- en implementatiefase. Het beveiligingsteam moet aanvullende beveiligingseisen en een verplichte beveiligingsarchitectuur definiëren en ook een dreigingsanalyse uitvoeren. De resultaten worden vervolgens opgenomen in het algemene concept en daarmee complexe correcties in latere projectfasen worden voorkomen (zie hoofdstuk 3.3.3).

3.3.2.11 Performance monitoring management (prestatie bewaking)

Dit proces omvat alle activiteiten met betrekking tot bewaking, meting, analyse en evaluatie in relatie tot het ISMS en de daarbij behorende informatiebeveiliging. Dit proces moet conform de State of the Art worden bewaakt en geverifieerd. De protocollen moeten bijvoorbeeld worden geregistreerd en regelmatig worden geëvalueerd, maar ook moeten regelmatig interne audits en technische systeemaudits worden uitgevoerd om informatie te verkrijgen over de vraag of het ISMS en de door gegenereerde informatiebeveiliging(continu voldoen aan de eisen, doeltreffend is geïmplementeerd en wordt gehandhaafd. Het hoogste management moet het ISMS minstens één keer per jaar evalueren om te bepalen of en in welke mate het ISMS voldoet aan het gedefinieerde doel en bijdraagt aan de uitvoering van de informatiebeveiliging doelen. Dit vormt de basis voor verdere besluiten.

Technische systeemaudits en interne en externe audits kunnen worden beschouwd als subprocessen (zie hieronder) van het hier genoemde proces. Hetzelfde geldt voor alle andere categorieën van bewaking, meting, analyse en beoordelingsactiviteiten.

3.3.2.11.1 Technische systeemaudits

Technische systeemaudits (inspecties op netwerk-, systeem- en applicatieniveau) moeten regelmatig door of namens de organisatie worden uitgevoerd. Deze audits worden meestal uitgevoerd als penetratietests of webcontroles.

- Bij een kleine IS-penetratietest worden met betrekking tot de beveiliging configuraties en beleid in de gebruikte IT-systemen willekeurig in de vorm van een technische audit, onderzocht en worden aanbevelingen gegeven voor het elimineren van eventuele kwetsbaarheden. De IT systeeminspectie wordt gezamenlijk met de beheerders uitgevoerd.
- Aanvullend op de technische audit worden, bij een uitgebreide penetratietest, kwetsbaarheden in de geteste IT-systemen door middel van technisch onderzoek en o.a. met behulp van speciale beveiligingshulpmiddelen opgespoord. Voor deze inspectie krijgen de testers ter plekke en onder toezicht van de beheerders toegang tot de IT-systemen.
- Met een IS web controle wordt de beveiligingsstatus van de aanwezigheid van de organisatie op het Internet, intranet en/of extranet geïnspecteerd. Het merendeel van de tests in dit proces wordt met behulp van geautomatiseerde methoden uitgevoerd via het internet en, indien van toepassing, via het interne netwerk (voor intranet en extranet).

3.3.2.11.2 Interne en externe audits, ISMS-certificering

ISMS-audits dienen de volgende doelen:

- het controleren van de voortgang van de implementatie van het ISMS;
- het bepalen van het naleven door de organisatie van de auditcriteria het ISMS;
- het bepalen van het vermogen van het ISMS om te voldoen aan wet en regelgeving en contractuele eisen;
- het controleren van het gebruik en de effectiviteit van het ISMS;
- het identificeren van kwetsbaarheden/potentieel voor verbeter van het ISMS.

Binnen het toepassingsgebied van het ISMS moeten interne audits ten minste eenmaal per jaar worden uitgevoerd worden, als algemene regel door of namens de organisatie.
Om aan de State of the Art te voldoen, wordt elke organisatie-eenheid (of elk onderdeel van het toepassingsgebied, zoals locatie, gebouwen) ten minste eenmaal per drie intern gecontroleerd.

Externe ISMS-audits worden uitgevoerd door belanghebbende partijen, zoals klanten (tweede partij of second party audits), of door externe, onafhankelijke auditorganisaties (derde partij of third party audits).

Als onderdeel van het uitvoeren van certificeringaudits controleert het auditteam of aan de eisen van ISO 27001 is voldaan, die met inachtneming van de normen ISO 27002 en ISO 27005 moeten zijn uitgevoerd. Auditors van certificeringinstanties zijn verplicht om als onderdeel van het auditproces de normen uit ISO 19011-en ISO 27007 te overwegen; ISO/IEC TR 27008 bevat een richtlijn over de controle van ISMS-normen en is eveneens van toepassing.

Als onderdeel van het certificeringproces voert de certificeringinstantie de volgende taken uit:

- controleren van de auditresultaten, inclusief de auditconclusies;
- documenteren van de evaluatie van de auditresultaten, inclusief de auditconclusies;
- certificatierapport met certificaat goedkeuring;
- afgifte van het certificaat.

Gekwalificeerde ISO 27001-certificatie instellingen zijn geaccrediteerd conform ISO 17021 en ISO 27006. een overzicht van de in Nederland geaccrediteerde ISMS-certificerende instanties is te vinden op de website van de Raad voor Accreditatie (https://www.rva.nl)[37].

ISO 27001-certificeringen hebben een geldigheidsduur van 3 jaar en worden als onderdeel van zogenaamde “surveillance audits” audits ten minste jaarlijks opnieuw beoordeeld. Wil men het certificaat na 3 jaar verlengen, dan moet de organisatie voordat de termijn van drie jaar is verstreken met succes een hercertificatie-audit hebben doorstaan.

3.3.2.12 Improvement management (continu verbeteringsproces)

De organisatie moet de geschiktheid, toereikendheid en effectiviteit van haar ISMS voortdurend verbeteren. De belangrijkste activiteiten met betrekking tot het onderhoud en de voortdurende verbetering van het ISMS zijn gericht op het evalueren en continu optimaliseren van de prestaties van het ISMS. In het bijzonder moeten hier de volgende aspecten worden geadresseerd:

- het omgaan met non-conformiteiten die voortvloeien uit het bewaken, meten, analyseren en beoordelen van het ISMS en de informatiebeveiliging die in dit kader wordt gegenereerd;
- het definiëren en uitvoeren van corrigerende maatregelen om de oorzaak van non-conformiteiten te elimineren.

Voortdurende verbetering van de geschiktheid, adequaatheid en doeltreffendheid van het ISMS en de door haar gegenereerde informatiebeveiliging.

3.3.3 Secure Software Development (veilige softwareontwikkeling)

Met de beveiliging van een applicatie moet tijdens het hele softwareontwikkelingsproces rekening gehouden worden. Ongeacht de gebruikte ontwikkelingsmethode moet rekening gehouden worden met maatregelen voor de ontwikkeling van veilige applicaties. Procesmodellen en best practices voor veilige software ontwikkeling worden beschreven in BSIMM, OWASP SAMM, OWASP ASVS, de webrichtlijnen van het Forum Standaardisatie[38], de BSI-richtlijn "Leitfaden zur Entwicklung sicherer Webanwendungen" en bijvoorbeeld ISO/IEC 27034, onderwezen in TeleTrusT Professional voor Secure software engineering T.P.S.S.E. De essentiële beschermende maatregelen binnen het softwareontwikkelingsproces worden vermeld in de afzonderlijke hoofdstukken. De belangrijkste beschermingsmaatregelen binnen het softwareontwikkelingsproces worden vermeld in de afzonderlijke hoofdstukken.

3.3.3.1 Requirements Analyse (Vereisten analyse)

Veilige applicatie ontwikkeling begint met een Requirements Analyse. De basis van de Requirements Analyse is een dreigingsanalyse. De (bedrijfs) activa die moeten worden beschermd, moeten worden gedefinieerd en de bedreigingen die voor deze activa bestaan moeten worden beschreven. De architectuur van de applicatie, in het bijzonder de gegevensopslag en de gegevensstromen evenals de vertrouwensgrenzen daarvan moeten worden overwogen. Vervolgens moeten de risico's van de geïdentificeerde bedreigingen worden beoordeeld en daaruit tegenmaatregelen en veiligheidseisen worden afgeleid. Een nuttige methode voor het identificeren van specifieke bedreigingen is een definitie van zogenaamde gevallen van misbruik. Deze beschrijven specifieke aanvallen evenals het gewenste gedrag van de applicatie in het geval van een aanval. Andere veiligheidsvereisten voor de applicatie ontstaan bijvoorbeeld uit wetgeving of contractuele verplichtingen. Deze beveiligingsvereisten vloeien, net als de functionele vereisten, over in de daaropvolgende ontwerpfase van het softwareontwikkelingsproces en ook in de specificatie van de testcases voor het later testen van de applicatie.

In de Volere-template[39], die vaak wordt gezien als de standaard voor een algemene vereisten

[37] DAkkS is de Duitse accreditatie-instantie.
[38] https://www.forumstandaardisatie.nl/standaard/webrichtlijnen
[39] https://www.volere.org/templates/volere-requirements-specification-template/

specificatie, zijn al een aantal beveiligingsvereisten, die in aanmerking moeten worden genomen gedefinieerd:

- 15a toegangsvereisten;
- 15b integriteitvereisten;
- 15c privacyvereisten;
- 15d controlevereisten;
- 15e immuniteitsvereisten.

3.3.3.2 Ontwerpfase

Een veilig ontwerp moet, om geïdentificeerde bedreigingen aan te pakken, rekening houden met alle beveiligingsvereisten. Het resultaat van het ontwerpproces is onder andere de beveiligingsarchitectuur met inbegrip van een strategie voor gegevens afhandeling. Een beveiligd ontwerp houdt rekening met aspecten, zoals veilige verificatie, cryptografische vereisten, foutafhandeling, systeemconfiguratie, vertrouwensrelatie tussen applicatieonderdelen en de bedrijfslogica van de applicatie.
Onvoldoende aandacht voor beveiliging bij het ontwerp van een applicatie is vaak de oorzaak van kwetsbaarheden in de applicatie, zoals ontbrekende of gebrekkige verificatie en autorisatie, en kan alleen worden opgelost met grote inspanning achteraf. Andere oorzaken zijn in code-ingebouwde sleutels of wachtwoorden, onjuiste verwerking van gevoelige gegevens of onveilige foutafhandeling die nuttige informatie aan de aanvaller verschaft.

Naleving van zogenaamde Secure Design principes helpt een architect om een robuust ontwerp van zijn applicatie te maken. Voorbeelden beproefde ontwerpprincipes zijn: minimale bevoegdheden (Least Privilege), verdediging in de diepte (Defense in Depth) of standaard beveiligd(Secure by Default).

Ontwerpprincipes zoals standaard privacybescherming (Privacy by Default) worden steeds belangrijker, vooral met betrekking tot de Algemene Verordening Gegevensbescherming van de EU. Daarnaast kan een architect zogenaamde ontwerppatronen en aanbevolen procedures voor beveiliging gebruiken, die, in tegenstelling tot de ontwerpprincipes, een meer concrete, maar taalonafhankelijke aanpak biedt om terugkerende problemen op te lossen. Het ontwerp, of althans de ontwerpaspecten die relevant zijn vanuit het oogpunt van beveiliging, moet nog voordat de applicatie wordt toegepast, worden onderworpen aan een ontwerpbeoordeling.

3.3.3.3 Implementatie

Veelvoorkomende implementatiefouten, zoals ongecontroleerde verwerking van invoer, met inbegrip van de uitvoer van deze gegevens of het mengen van code en gegevens, kunnen leiden tot beveiligingsproblemen zoals code-injecties, cross-site scripting en/of buffer overflows. Speciale programmeerrichtlijnen helpen ontwikkelaars zich tijdens de implementatie te richten op de beveiliging.

Deze programmeerrichtlijnen moeten individueel worden afgestemd op de programmeertalen, bibliotheken en kaders die worden gebruikt. Frameworks moeten, wanneer deze worden gebruikt, correct worden gebruikt om hun beveiligingsfuncties niet te ondermijnen. Zo kan bijvoorbeeld vastgelegd worden, dat alleen bepaalde functies en objecten kunnen worden gebruikt of dat software modules alleen met een programma kunnen worden ingecheckt na een geslaagde code analyse. Statische code controles moeten worden gebruikt om de broncode automatisch te controleren op veel voorkomende implementatiefouten. De broncode, of ten minste de delen van de broncode die relevant zijn vanuit beveiligingsperspectief (op basis van de resultaten van de dreiginganalyse), moeten ook worden onderworpen aan een handmatige code beoordeling.
Zwakke punten in de applicatie kunnen echter ook voortvloeien uit het gebruik van onveilige componenten van andere fabrikanten, daarom moeten dergelijke onderdelen zorgvuldig worden geselecteerd en moeten de releases van beveiligingsbulletins van deze leveranciers en de CVE-database met bekende beveiligingslekken voortdurend worden gecontroleerd. Dergelijke controle van externe onderdelen moet automatisch met behulp van een hulpprogramma worden uitgevoerd ter controle op afhankelijkheden. Applicatie-implementatie programma's, zoals containeroplossingen, moeten, als deze worden het gebruikt, ook worden gecontroleerd op bekende beveiligingslekken.

3.3.3.4 Testen van de software

Om kwetsbaarheden in de applicatie te vinden worden Blackbox-/Greybox-en WhiteBox-testemn en

statische en dynamische beveiligingsscans gebruikt. Om de hoogst mogelijke efficiëntie te bereiken, heeft, voor zover van toepassing, een combinatie van BlackBox-/Greybox-en WhiteBox testen en statische en dynamische veiligheidsscans de voorkeur. Zo kunnen bijvoorbeeld gebruikte versleutelingalgoritmen gemakkelijk worden gedetecteerd en geëvalueerd door middel van statistische analyse van de broncode, terwijl beveiligingslekken die voortvloeien uit de integratie van verschillende onderdelen of pas tijdens runtime ontstaan (zoals in de communicatie met een verificatieservice) goed kunnen worden gedetecteerd via dynamische scans van het systeem. In tegenstelling tot handmatige penetratietests, kunnen beveiligingsscans automatisch als onderdeel van het softwareontwikkelingsproces worden uitgevoerd, om te zorgen voor een beveiligingscontrole van elke versie van de software. Bovendien moet de testfase de vereiste beveiligingsmaatregelen van de applicatie controleren, d.w.z. hoe de applicatie wordt beschermd tegen de aanvallen die zijn geïdentificeerd in bedreigingsanalyse. Een goede bron voor het maken van de test case is de gedefinieerde misbruik gevallen.

Deze beveiligingstests bieden echter geen absolute verklaring over de beveiliging van de applicatie. Beveiliging kan niet worden bewezen, zoals in de functionaliteit tests, door het feit dat het verwachte gedrag overeenkomt met waargenomen gedrag. Beveiliging is een negatief criterium, meestal ontworpen om ongewenst gedrag te voorkomen. Hier is de creativiteit van een aanvaller bijna oneindig. Er kunnen dus nog andere bedreigingen zijn en dus ook andere testcases die nog niet in aanmerking zijn genomen. Desalniettemin is het testen van de beveiliging een belangrijk onderdeel van het veilige softwareontwikkelingsproces.

3.3.3.5 Bescherming van broncode en resources

Om de integriteit van (bron)code en middelen (resources) te behouden en zo de applicatie te beschermen tegen manipulaties, zoals backdoors, Trojaanse paarden of veranderingen in de verwerkingslogica, moeten broncode controlesystemen worden gebruikt en, indien nodig, moeten afzonderlijke code onderdelen alleen beschikbaar zijn voor bepaalde Ontwikkelaars. Gevoelige informatie mag niet worden opgeslagen in broncode (controlesystemen), om te voorkomen dat deze onbedoeld openbaar worden gemaakt. Daarnaast moet een veilige ontwikkelomgeving worden gewaarborgd, onder meer door toegangsrechten te beperken en systemen te hardenen, waarbij de ontwikkelaars alleen persoonsgebonden accounts gebruiken, welke geen met beheerderrechten hebben en in beveiliging zijn getraind.

3.3.3.6 Certificatie van de software

Voorafgaand aan de levering van de software, is voorafgaande verificatie en certificering door een neutrale instantie nuttig. Terwijl het testen de functionaliteit van de software heeft verzekerd, zorgt certificering ervoor dat de architectuur, Requirements management, Configuratiebeheer en risicobeheer geschikt zijn voor een veilige ontwikkeling en, belangrijker nog, voor het probleemoplossingsproces (Troubleshooting proces).

Om kwetsbaarheden later te kunnen elimineren, moet architectuur en ontwerp zo zijn ontworpen dat niet alleen bugs kunnen worden opgelost, maar defecte componenten in een noodsituatie kunnen worden vervangen.

Voor meer complexe software is Requirements management essentieel. De vereisten moeten vóór de levering (opnieuw) worden gecontroleerd, om te zien of ze duidelijk zijn gedefinieerd volgens IREB (het International Requirements Engineering Board). De implementatie van de vereisten moet kunnen worden herleid tot de broncode. In het eenvoudigste geval kan dit worden gedaan door identificatoren toe te wijzen, die vervolgens ook als Comments in de code kan worden opgenomen. Hierdoor is het mogelijk snel te kunnen reageren op bekend geworden kwetsbaarheden.

Configuratiebeheer is nauw verbonden met Requirements management. Hierin moet gecontroleerd worden of een software versie met broncode en alle bijbehorende documenten duidelijk kunnen worden toegewezen aan een versie status (en later een software release). In geval dat de vereisten wijzigen, moet duidelijk zijn welke documenten al actueel zijn en rekening houden met de vereisten en welke niet. Aangezien documenten afzonderlijk worden ontwikkeld, hebben de documenten meestal een verschillende status en versie. Daarom moet naast de versie van de documenten ook een zogeheten Baseline worden gedefinieerd waarin beschreven staat welke documenten bij elkaar horen bij welk versienummer en dus bij een bepaalde release. Hiermee is zichtbaar welke bugs en kwetsbaarheden in welke software versie zijn opgelost.

In de eerste instantie moet risicobeheer bewust zijn van mogelijke risico's en gevaren die, onder andere, als gevolg van zwakke plekken manifest kunnen worden. Risicobeheer is in het bijzonder noodzakelijk wanneer mensenlevens in gevaar kunnen worden gebracht. In het geval van software certificering moet, voordat de software wordt geleverd, gecontroleerd worden of een Risico Management systeem aanwezig is, dat:

- risico's identificeert;
- risico's classificeert naar ernst en op kans van optreden;
- risicomitigatie maatregelen definieert;
- risico's, nadat de maatregelen zijn doorgevoerd, (her)classificeert;
- met regelmatige intervallen en in geval van wijzigingen wordt vervolgd.

Als de software wordt uitgevoerd in systeemverband (in een System Group wordt uitgevoerd), moet het hele systeemverband worden gecertificeerd.

3.3.3.7 Levering van software (Software Delivery)

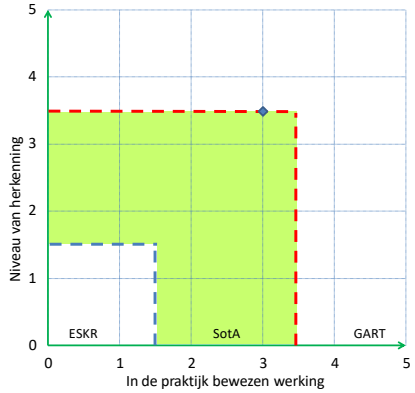
Een kwetsbaarheid bij de levering en installatie van software vernietigt het resultaat van alle eerdere beveiligingsmaatregelen in het softwareontwikkelingsproces. Daarom moet een veilige levering en installatieproces zorgen voor de integriteit van de uitgerold software om te voorkomen dat de productieve toepassingsomgeving wordt aangetast. Voor dit doel kunnen code signatures worden gebruikt. Aanvallen op de uitgerold applicatie zijn echter ook mogelijk door een onveilig geconfigureerde applicatie.
Daarom moet in de productieomgeving een veilige configuratie worden zeker gesteld en moeten ongeautoriseerde wijzigingen van de configuratie worden voorkomen. Als beveiligingsmaatregel zijn juiste standaard instellingen (Secure by Default) en handboeken voor beheerders beschikbaar. Om potentiële schade van een aanval te minimaliseren, moet de applicatie minimale rechten hebben (Least Privilge). Speciaal in container omgevingen worden applicaties vaak als root-gebruikers uitgevoerd, boven alles moet dit voorkomen worden. Voor de beveiliging van de applicatie is het ook belangrijk, dat de applicatie altijd met beveiligingsupdates up-to-date gehouden wordt.

3.3.3.8 Beveiligingsresponse

Aangezien kwetsbaarheden nooit volledig kunnen worden uitgesloten, moet elke fabrikant voorbereid zijn op dergelijke meldingen en snel kunnen reageren.

Het zogenaamde Security Response proces van een fabrikant beschrijft haar aanpak voor het omgaan met bij haar bekend geworden beveiligingsproblemen. Beveiligingspatches zijn tijdkritisch en moeten daarom snel worden afgeleverd. De patches omvatten zowel fixes voor zelf ontwikkelde onderdelen, als voor bekende kwetsbaarheden in de standaard gebruikte software, zoals bibliotheken en frameworks. Om beveiligingsonderzoekers te motiveren om kwetsbaarheden te melden, zijn Responsible Vulnerability Disclosure en Bug-Bounty programma's beschikbaar.
Het is belangrijk dat gerapporteerde beveiligingslekken weer terugvloeien in het software ontwikkelproces, zodat ze worden opgelost.

Classificatie van het technologieniveau



3.3.4 Audits en certificering

Maatregelen worden alleen effectief uitgevoerd als de effectiviteit ervan regelmatig en, indien nodig, door onafhankelijke derden wordt gecontroleerd.

Context informatiebeveiliging

Aangezien het aantal maatregelen snel erg groot kan worden, is het raadzaam deze in het kader van een ISMS vast te stellen. Een ISMS kan door een geaccrediteerde certificatie-instelling worden gecertificeerd volgens ISO 27001 of de BSI IT-Grundschutz.

ISMS-audits hebben de volgende doelen:

- de controle van de voortgang van de ISMS-implementatie;
- het bepalen van de compliance van het ISMS met de auditcriteria van de organisatie;
- het bepalen van het vermogen van het ISMS om te voldoen aan wet en regelgeving en contractuele eisen;
- de controle van het gebruik en de effectiviteit van het ISMS;
- de identificatie van kwetsbaarheden/verbeteringspotentieel van het ISMS;

Binnen de scope van het ISMS moeten interne audits [eerste partij controles] in principe ten minste eenmaal per jaar door of namens de organisatie worden uitgevoerd. State of the Art betekent dat elke organisatie-eenheid (of onderdeel van de scope, zoals locatie, gebouwen) regelmatig intern wordt gecontroleerd. Bij een interne audit is het belangrijk ervoor te zorgen dat afdelingen niet zichzelf controleren. De audit moet altijd door onafhankelijke personen worden uitgevoerd. Hiervoor kunnen onafhankelijke derde partijen ook ondersteuning leveren. De uitvoering van interne audits is verplicht als onderdeel van een ISMS-certificering.

Externe ISMS audits worden uitgevoerd door belanghebbende partijen, zoals klanten (tweede partij audit). Vergelijkbaar kan een externe audit worden uitgevoerd door externe, onafhankelijke auditorganisaties (derden audit). Als uitbestedingnemer (CSC) is het extra belangrijk dat bij de (uitbesteding)provider (CSP) externe audits (leverancier-audits) worden uitgevoerd. De leverancier kan ook aantonen dat aan de eisen voor informatiebeveiliging is voldaan met een geschikt certificaat (ISO 27001 of ISO 27001 op basis van de BSI IT-Grundschutz voor het juiste toepassingsgebied).

Idealiter is een ISMS gecertificeerd. De procedure moet worden afgehandeld door een geaccrediteerde certificatie-instelling. De volgende voordelen pleiten voor certificering:

- bewijs van adequate risicobeoordeling en -behandeling;
- bevestiging door een onafhankelijke derde partij van de functionaliteit van het ISMS;
- bewijs van voortdurende verbetering van het ISMS;
- Vermindering van aansprakelijkheid in geval van een incident, omdat het naleven van een in de EU geharmoniseerde norm leidt tot het vermoeden van conformiteit met de erkende regels van technologie (normen) en de stand van de techniek. De geaccrediteerde certificatie-instelling moet voor de afgifte van het conformiteitcertificaat niet alleen de norm conformiteit toetsen, maar ook de huidige State of the Art of ook innovatieve technologieën op gelijkwaardigheid toetsen en toepassen.

In het kader van het uitvoeren van certificeringaudits controleert het auditteam of de eisen van ISO 27001 of van de BSI IT-Grundschutz worden nageleefd. De audits moeten worden uitgevoerd volgens ISO 27001 in overeenstemming met de standaarden ISO 27002 en ISO 27005 (en indien nodig, andere branchespecifieke toevoegingen aan de serie 27-standaarden). Auditors van certificeringinstanties voor ISO 27001 zijn verplicht om de ISO 19011-en ISO 27007-normen als onderdeel van het auditproces te beschouwen. Voor audits conform de BSI IT-Grundschutz moet het toepasselijke certificatieschema van het BSI worden nageleefd.

Als onderdeel van het certificeringproces neemt de certificeringinstantie de taken over die voortvloeien uit ISO/IEC 17021 i. V. m ISO/IEC 27006. Dit zijn in het bijzonder:

- het plannen van de audit en selecteren van bevoegde auditors;
- het uitvoeren van evaluatie/audit of opdracht aan derden;
- het controleren van de auditresultaten, inclusief de auditconclusies door personen die niet bij de audit betrokken zijn;

- documenteren van het controleren van de auditresultaten, inclusief de auditconclusies;
- het afwijzen van de certificaatuitgifte;
- het afgeven van het certificaat;
- het bewaken van de certificering tijdens de looptijd van het certificaat.

De certificeringinstanties voor ISO 27001 zijn in bezit van een ISO 17021 en ISO 27006 accreditatie. Een overzicht van de in Duitsland geaccrediteerde ISMS-certificerende instanties is te vinden op de website van de Duitse accreditatie-instantie (DAkkS). Het BSI is de verantwoordelijke certificatie-instantie voor de IT-Grundschutz.

Certificeringen volgens ISO 27001, of ISO 27001 op basis van basis de BSI IT-Grundschutz, hebben een geldigheidsduur van drie jaar en worden als onderdeel van zogenaamde monitoring (surveillance) audits ten minste jaarlijks gecontroleerd. Als het certificaat na drie jaar wordt verlengd, dan moet de organisatie vóór het einde van de periode van deze drie jaar met succes een hercertificeringaudit hebben doorstaan.

Afhankelijk van de bedrijfstak/sector kunnen ook zogenaamde sectorspecifieke eisen worden nageleefd. Het is noodzakelijk te controleren of de relevante sectorspecifieke voorschriften een bewijs van een gecertificeerd ISMS vereisen. Bovendien kunnen andere eisen worden gedefinieerd, die volgens het beleid uitgevoerd en beproefd moeten worden. Een overzicht van de gepubliceerde sectorspecifieke standaarden is te vinden op de website van BSI.

Context Privacybescherming
Met betrekking tot de evaluatie van de effectiviteit van maatregelen in relatie tot de eisen vanuit de GDPR, is de implementatie van een management systeem, of meer precies een Data Protection management systeem (DPMS), een optie. De GDPR specificeert dit niet expliciet. Niettemin, toont het op veel plaatsen de noodzaak van een DPMS. GDPR Art. 32 lid 1d[40] vereist bijvoorbeeld een een proces voor het regelmatige testen, beoordelen en evalueren van de effectiviteit van technische en organisatorische maatregelen voor het waarborgen van de veiligheid van de verwerking.

Aangezien een dergelijk proces een geplande en gestructureerde aanpak binnen de organisatie vereist, en dus de implementatie van het klassieke PDCA-model vereist, is het inrichten van een DPMS een ideale oplossing. Als dit op hoog niveau is afgestemd op de elementen van de ISO-structuur, dan kan het ook op basis van ISO 27001worden geïntegreerd in een bestaande ISMS.

Net als een ISMS kan vervolgens het DPMS worden gecontroleerd en het niveau van volwassenheid van het systeem succesvol worden bepaald.

Conforme ISO 19011 kunnen audits worden uitgevoerd op basis van een auditprogramma en een auditplan. Audits kunnen worden uitgevoerd door de functionaris voor gegevensbescherming (*DPO of FG*). In het geval van grotere organisaties kunnen audits ook worden uitgevoerd door medewerkers van de organisatie die een experttraining hebben gevolgd of door in gegevensbescherming gespecialiseerde adviesbureaus.

In het kader van de zogenoemde leverancieraudits kunnen ook verwerkers van de organisatie worden gecontroleerd.

3.3.5 Kwetsbaarheid en patchbeheer
Het proces “kwetsbaarheid en patchbeheer” is ontworpen om beveiligings- en functionaliteits-tekortkomingen in software en firmware te identificeren en te herstellen.

Patches[41] zijn ontworpen om geïdentificeerde kwetsbaarheden aan te pakken en hun uitbuiting te

[40] Zie ook GDPR Art. 5 lid 2 ' de verantwoordelijke (...) moet (...) compliance kunnen aantonen " en Art 24 lid 1 "(...) en te borgen dat aangetoond kan worden (...) dat de verwerking overeenkomstig deze verordening wordt uitgevoerd".
[41] De drie belangrijkste type patches zijn:
- Bugfix: dit is de correctie van fouten (bugs) die optreden in de (programma)broncode;
- Hotfix: dit is de niet uit te stellen correctie van fouten in de toepassingsprogrammatuur;
- Update: dit is de klassieke vorm van het aanpassen van de programmatuur,de update bevat functieverbeteringen, in sommige gevallen ook correcties van fouten.

voorkomen. Het proces van kwetsbaarheid en patchbeheer omvat identificatie, beoordeling, evaluatie en implementatie voor alle producten en systemen van een organisatie. Het proces van kwetsbaarheid en patch management is verantwoordelijk voor het implementeren van patches en het verifiëren van de effectiviteit in de onderneming.

3.3.5.1 Assessment

Om patches en kwetsbaarheden efficiënt te beheren, moet het IT-landschap van de organisatie eerst worden geïnventariseerd. Omdat het landschap in de loop van de tijd kan veranderen, moet een dergelijke inventarisatie regelmatig worden uitgevoerd en up-to-date worden gehouden. Onderdelen die zich niet in het interne netwerk bevinden (zoals smartphones en notebooks van dienstverleners) moeten via speciale richtlijnen worden beheerd. Deze richtlijnen zijn bedoeld om de eigenaren van deze componenten aan te moedigen om zelfstandig de software van hun apparaten bij te werken of om ze regelmatig te verbinden met het bedrijfsnetwerk om ze te updaten.

3.3.5.2 Identificatie en evaluatie

Om kwetsbaarheden, software fixes en bedreigingen te identificeren, moeten relevante informatiebronnen (zoals fabrikant websites, CERTs, CVSS-databases, mailinglijsten van software- en hardwarefabrikanten, nieuwsgroepen van derden) worden gecontroleerd. Ook moet de inzet van professioneel patchbeheer tools voor bedrijven worden overwogen. Alle managers van IT-systemen, applicaties, netwerkcomponenten, etc. moeten periodiek een overzicht/samenvatting van de huidige patch status beschikbaar stellen. Hieruit moet een verslag worden opgesteld voor de beoordeling van de huidige patch situatie en moet worden gebruikt om het huidige risico te beoordelen (bijvoorbeeld CVSS-Score). De volgende oplossingen zijn als behandelingsopties beschikbaar:

- Het doorzetten naar patch management om geïdentificeerde kwetsbaarheid met een geschikte patch (update) te sluiten;
- Het vaststellen van tijdelijke oplossingen vast (work-arounds), zoals het aanpassen van de configuratie en code analyse, om het beveiligingslek op te lossen;
- het afsluiten of isoleren van het getroffen systeem.

Als, om het beveiligingslek op te lossen, patches handmatig worden gedownload, dan moet de authenticiteit ervan met behulp van gestandaardiseerde methoden (cryptografische checksums, handtekeningen en digitale certificaten) worden gecontroleerd. Dit geldt in het bijzonder voor downloads vanaf het Internet. Paches moeten primair rechtstreeks afkomstig zijn van de bronnen van de fabrikant(en). Alleen in uitzonderlijke gevallen (zoals voor geïntegreerde producten van derden zoals runtime-bibliotheken) zijn patches van andere geverifieerde vertrouwde bronnen toegestaan.

3.3.5.3 Deployment

3.3.5.3.1 Voorbereiding

Zodra de authenticiteit van de patches is geverifieerd, moeten ze in testsystemen getest worden. Indien mogelijk, moeten de testsystemen op dezelfde of vergelijkbare wijze worden uitgerust en geconfigureerd als het productiesysteem.

Voordat de patches in de productieomgeving wordt geïnstalleerd, moet eerst een back-up worden gemaakt van de geraakte systemen, zodat de patches in geval van een storing opnieuw kunnen worden geïnstalleerd. In het geval van ongewenste prestaties of beperkte functionaliteit, moeten probleemoplossing maatregelen worden vastgesteld en geïmplementeerd.

3.3.5.3.2 Implementatie

Om het uitvoeringsproces naar behoren te laten functioneren, moeten passende voorbereidingen worden getroffen. Dit omvat bijvoorbeeld het definiëren van de tijdsperiode voor het distribueren van de patches en het informeren van alle systeembeheerders. De installatie moet ook worden aangekondigd aan de gebruikers, zodat ze hun operationele processen op tijd voor de aangekondigde installatieperiode kunnen voltooien.

Normaalgesproken moeten patches automatisch worden gedistribueerd (bijvoorbeeld met een Enterprise Patch Management Tool), maar mogelijk moeten Beheerders afzonderlijke patches lokaal installeren. In dat geval moet de communicatie veilig worden bewaard en moeten de bestanden worden uitgewisseld met een verificatiecontrole.

Om mislukte implementatiepogingen op tijd te detecteren moet, zodra patches worden uitgerold, de voortgang bewaakt en gecommuniceerd worden. Tijdig moeten passende corrigerende maatregelen worden genomen.

3.3.5.4 Behandeling van uitzonderingen

3.3.5.4.1 Niet te patchen systemen

Voor systemen of applicaties waarvoor:

- geen updates van de fabrikant (zogenaamde legacy systemen) beschikbaar zijn;
- de fabrikant nog geen updates van het besturingssysteem heeft uitgebracht;
- een onderhoudsvenster, om operationele redenen (zoals automatisering in procestechniek), niet op korte termijn beschikbaar kan worden gesteld;
- een update het hercertificeren van het gehele systeem vereist;

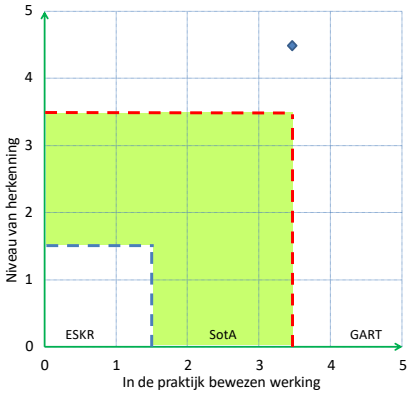
moeten technische maatregelen worden vastgesteld en uitgevoerd. Omdat een shutdown of eenvoudige herconfiguratie meestal onverenigbaar is met operationele eisen, moeten:

- scheiding, zonering, inkapseling of applicatie firewalls, en
- netwerk monitoring via inbraak detectiesysteem worden gebruikt ter bescherming tegen en detectie van misbruik van bestaande beveiligingslekken.

3.3.5.4.2 Goedkeuringen van fabrikanten

Als voor de implementatie van patches goedkeuring door de fabrikant vereist is, zoals voor patches van database of besturingssystemen, dan kunnen, in verband met mogelijk verlies van functionaliteit of gebrek aan garantie, de meeste van de beschikbare patches niet worden toegepast. Om deze reden is de fabrikant contractueel verplicht om tijdsperioden in te stellen voor het vrijgeven en implementeren van patches en updates of voor alternatieve oplossingen voor kwetsbaarheden.

Classificatie van het technologieniveau



Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Bundesverband IT-Sicherheit e.V. (TeleTrusT) is een kennisnetwerk dat bestaat uit nationale en buitenlandse leden uit industrie, administratie, consultancy en wetenschap en thematisch gerelateerde thematisch verwante partnerorganisaties. TeleTrusT belichaamt met haar brede scale aan leden en partnerorganisaties TeleTrusT het grootste competentienetwerk voor IT-beveiliging in Duitsland en Europa. TeleTrusT biedt interdisciplinaire forums voor IT-beveiligingsexperts, organiseert evenementen en faciliteert de uitwisseling van IT-beveiliging gerelateerde informatie tussen leveranciers, gebruikers, onderzoekers en autoriteiten. TeleTrusT biedt forums voor experts, organiseert evenementen en conferenties discussies over technische, politieke en juridische kwesties met betrekking tot IT-beveiliging. TeleTrusT is drager van de European Bridge CA (EBCA, PKI Network of Trust), de IT-expert certificatiecertificaten “TeleTrusT Information Security Professional” (T.I.S.P.) en “TeleTrusT Professional for Secure Software Engineering” (T.P.S.S.E.) en biedt het vertrouwenszegel “IT Security Made in Germany”. TeleTrusT is lid van het European Telecommunications Standards Institute (ETSI). Het hoofdkwartier van de vereniging bevindt zich in Berlijn.

Contact:

IT Security Association Germany (TeleTrusT)
Dr. Holger Muehlbauer
Managing Director
Chausseestrasse 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
IT Security Association Germany (TeleTrusT)

Bundesverband IT-Sicherheit e.V. (TeleTrusT) is een kennisnetwerk dat bestaat uit nationale en buitenlandse leden uit industrie, administratie, consultancy en wetenschap en thematisch gerelateerde thematisch verwante partnerorganisaties. TeleTrusT belichaamt met haar brede scale aan leden en partnerorganisaties TeleTrusT het grootste competentienetwerk voor IT-beveiliging in Duitsland en Europa. TeleTrusT biedt interdisciplinaire forums voor IT-beveiligingsexperts, organiseert evenementen en faciliteert de uitwisseling van IT-beveiliging gerelateerde informatie tussen leveranciers, gebruikers, onderzoekers en autoriteiten. TeleTrusT biedt forums voor experts, organiseert evenementen en conferenties discussies over technische, politieke en juridische kwesties met betrekking tot IT-beveiliging. TeleTrusT is drager van de European Bridge CA (EBCA, PKI Network of Trust), de IT-expert certificatiecertificaten "TeleTrusT Information Security Professional" (T.I.S.P.) en "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) en biedt het vertrouwenszegel "IT Security Made in Germany". TeleTrusT is lid van het European Telecommunications Standards Institute (ETSI). Het hoofdkwartier van de vereniging bevindt zich in Berlijn.

Contact:

IT Security Association Germany (TeleTrusT)
Dr. Holger Muehlbauer
Managing Director
Chausseestrasse 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.