Eine Themenbeilage der
Heise Medien GmbH & Co. KG

II
2017

SICHERHEIT & DATENSCHUTZ

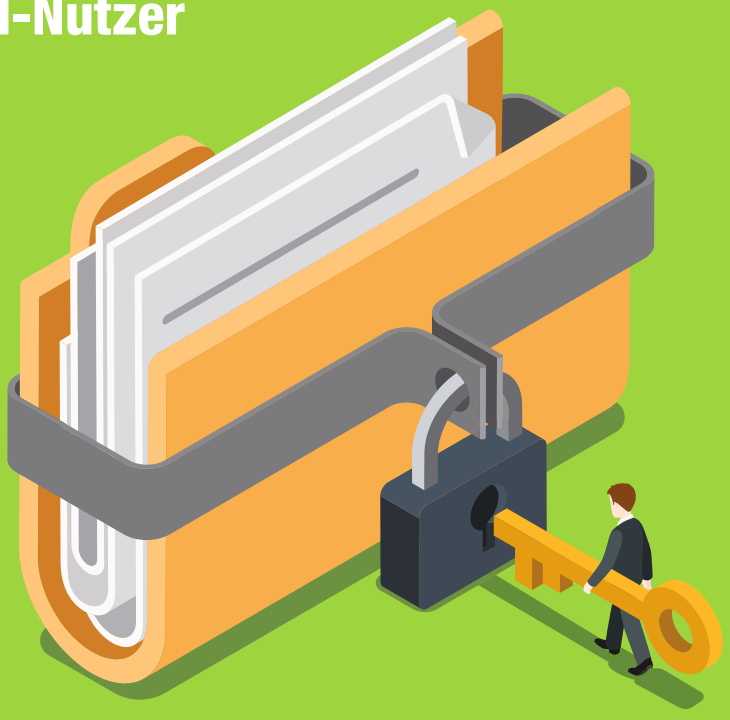
EU-DSGVO, ID-Management und Endpoint Security

Datenschutz-Grundverordnung:
Welche neuen Regeln Cloud-Nutzer beachten müssen

Künstliche Intelligenz:
Wie KI-Anwendungen Ressourcen schonen

Identity Management:
Was eine Authentisierung stark macht

EU-DSGVO:
Warum ein DIMS jetzt empfehlenswert ist



E-Mail-Security:
Wie man fingierte Absender identifiziert

secIT:
Wo sich Security-Experten im Frühjahr treffen

www.it-security-und-management.de

powered by: TeleTrusT Pioneers in IT security. iX

DEVELOPER-KONFERENZEN + -WORKSHOPS 2018

Parallel programming & HPC

Termin: 06.-08.03.2018
Ort: Print Media Academy, Heidelberg

Containerisierung, Docker, Kubernetes & Co.

Termin: 13.-16.11.2018
Ort: Rosengarten, Mannheim

para//el 2018

[Container Conf]

Deep Learning & Data Mining

Termin: 24.-26.04.2018
Ort: KOMED, Köln

MINDS MASTERING MACHINES

» Continuous Lifecycle »

DevOps & Continuous Delivery

Termin: 13.-16.11.2018
Ort: Rosengarten, Mannheim

building IoT

CONTINUOUS LIFECYCLE LONDON

Internet of Things & Industrie 4.0

Termin: 04.-06.06.2018
Ort: KOMED, Köln

Continuous Lifecycle London

Termin: 16.-18.05.2018
Ort: QEII Centre, London

Veranstalter:

Weitere Informationen unter:

www.heise.de/developer/

Datenschutz wird wichtiger denn je

Liebe Leserinnen und Leser,

das Jahr 2017 war (und ist noch immer) aufregend und abwechslungsreich. Doch in der bevorstehenden Adventszeit gibt es wieder Gelegenheit zur Besinnung. Und zu Weihnachten wollen wir alle beruhigt zu Hause sitzen, ohne unentwegt an das Risiko zu denken, dass jemand gerade die Datenkollekte auf unserem Rechner plündert.

Sind meine Daten auch gut geschützt? Baut derzeit jemand meine IoT-Landschaft zum Botnetz aus? Habe ich mich eigentlich schon ausreichend über IT-rechtliche Themen informiert? Diese und viele weitere ähnlich geartete Fragen müssen sich IT-Verantwortliche (im besten Fall die Geschäftsführerinnen und Geschäftsführer selbst) darum rechtzeitig stellen. IT-Sicherheit ist ein existenzielles Thema – es sollte auf höchster Entscheider-Ebene angesiedelt sein.

Das kommende Jahr wird stark im Zeichen der EU-Datenschutz-Grundverordnung stehen. Denn ab 25.05.2018 muss die EU-DSGVO verbindlich angewendet werden – und das betrifft sehr viele Unternehmen. Die DSGVO vereinheitlicht das Datenschutzrecht innerhalb der EU und regelt den Umgang mit bzw. die Verarbeitung von personenbezogenen Daten. Bei Verstößen dagegen drohen drastische Bußgelder.

Gerade in diesem Zusammenhang wird auch die Ermittlung des viel zitierten „Standes der Technik“ in der IT-Sicherheit im Sinne des IT-Sicherheitsgesetzes (ITSiG) im Jahr 2018 eine entscheidende Problematik bleiben. Immer noch gibt es für viele Betroffene erheblichen Klärungsbedarf. Nicht zuletzt wird in der neuen Legislaturperiode eine mögliche (und dringend erforderliche) Neuausrichtung der Digitalpolitik ein spannendes Themenfeld sein.

Deutschland braucht einen starken Datenschutz und bestmöglich abgesicherte IT-Systeme. Wirtschaft und Verwaltung sowie private Anwender sind mehr denn je auf sichere und vertrauenswürdige Informationsinfrastrukturen angewiesen. Als Bundesverband IT-Sicherheit e. V. ist es uns ein zentrales Anliegen, die Sicherheit in der IT zu erhöhen. Mit der TeleTrusT-Initiative „IT Security made in Germany“ ist die deutsche IT-Sicherheitsindustrie bestrebt, mittels zuverlässiger Konzepte hier Unterstützung zu bieten. Alle beteiligten IT-Sicherheitsunternehmen stehen gemeinsam für mehr Vertrauenswürdigkeit und Informationssicherheit ein.

Die vorliegende Sonderpublikation informiert Sie über Lösungen, die deutsche Unternehmen im Bereich der IT-Sicherheit entwickelt haben. Gemeinsam mit den TeleTrusT-Mitgliedern wünsche ich Ihnen eine informative Lektüre und hoffe, dass Sie zahlreiche Anregungen erhalten, um die IT-Sicherheit im Unternehmen, in Ihrer Behörde und auch in Ihrem privaten Umfeld weiter zu stärken – und in diesem Sinne die Festtage ungestört genießen zu können.

Dr. Holger Mühlbauer
Geschäftsführer TeleTrusT – Bundesverband IT-Sicherheit e.V.

Inhalt

Absender, auf die man sich verlassen kann

Standards zur Senderidentifikation sorgen für mehr Sicherheit im E-Mail-Verkehr

Für Sicherheit und Effizienz in der Mailkommunikation stellt die Nutzung von DMARC & Co einen Meilenstein dar. Denn die Bewertung der Reputation des Absenders ist ein verlässliches Instrument im Kampf gegen stetig steigende Mengen an Spam und immer perfider werdende Angriffsszenarien mit Malware.

Namhafte Akteure wie beispielsweise 1&1, Paypal und Microsoft setzen Standards zur Senderidentifikation bereits ein, der Bundesverband IT-Sicherheit e. V. TeleTrusT empfiehlt sie und sogar vermeintlich eher langsam arbeitende Behörden bieten sie ihren Kommunikationspartnern an. Auch international tut sich dazu einiges – die britische Digital-Services-Behörde hat beispielsweise die Verwendung von DMARC ab dem 1. Oktober 2016 verbindlich für alle Behörden in Großbritannien eingeführt. Die britische Steuerbehörde HMRC berichtet darüber hinaus von durchschlagenden Erfolgen bei der Bekämpfung von Spoofing-Attacken im Namen der HMRC seit der Einführung von DMARC.

SPF, DKIM und DMARC

Die automatische Absenderidentifikation ermöglicht es dem empfangenden Server, eindeutig festzustellen, ob eine Mail auch tatsächlich von dem Absender kommt, von dem sie zu stammen vorgibt. Außerdem kann er feststellen, ob der einliefernde Server autorisiert ist, im Namen der absendenden Domain E-Mails zuzustellen. Möglich wird dies durch spezielle Methoden, die als Standardinstrumentarium für E-Mail-Security immer mehr Verbreitung finden. Sie sind unter den Abkürzungen SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) sowie DMARC (Domain-based Messaging, Authentication, Reporting and Conformance) bekannt und bauen aufeinander auf.

Bei der Einführung dieser Technologien gilt es, zwei Aspekte zu berücksichtigen: Zum einen müssen die entsprechenden SPF-, DKIM-, und DMARC-Informationen für die eigenen Domains veröffentlicht und damit den externen Kommunikationspartnern zur Verfügung gestellt werden. So erhält der Kommunikationspartner überhaupt erst die Möglichkeit, zweifelsfrei festzustellen, dass die E-Mail tatsächlich vom korrekten Absender kommt. Nicht zu unterschätzen ist jedoch auch die massive Senkung des Reputationsrisikos für die eigenen Domains und damit des gesamten Unternehmens oder der Behörde. Der zweite Aspekt betrifft die Empfängerseite. Hier muss eine Software zum Einsatz kommen, welche die genannten Informationen abfragen und korrekt umsetzen kann.

Umschlag vs. Briefkopf

Zum besseren Verständnis ist es zwingend erforderlich, zunächst den Unterschied zwischen dem sogenannten „Envelope Sender“ und dem „Body-from“-Absender einer E-Mail zu kennen. Als Envelope Sender wird die E-Mail-Adresse bezeichnet, die während eines SMTP-Handshakes übergeben wird. Die Bezeichnung Envelope ist in Anlehnung an den Briefumschlag gewählt. Wie bei der traditionellen Briefpost ist nur das, was auf dem Umschlag steht, für den Transport ausschlaggebend. Und wie bei der Briefpost wird der Absender auf dem Umschlag (der Envelope Sender) informiert, wenn seine Nachricht nicht zustellbar war – unabhängig davon, welcher Absender in der Nachricht selbst (Body from) genannt wird.

Die Absenderinformation in Form des Body from ist zum einen im Body, genauer gesagt im Header der E-Mail, enthalten und beinhaltet neben der E-Mail-Adresse in der Regel noch weitere Informationen zum Absender, wie etwa Vor- und Nachname oder den Namen des Postfachs. E-Mail-Programme zeigen üblicherweise nur den Body from an. So werden E-Mails im Posteingang des Empfängers beispielsweise als gesendet von „Max Mustermann“ und nicht von „max.mustermann@musterfirma.de“ angezeigt.

Domain-Autorisierung

Im Sender Policy Framework (SPF) gibt der Inhaber einer Domain im Domain Name System (DNS) an, welche Server autorisiert sind, E-Mails im Namen der eigenen Domain zu versenden. Dazu erstellt er in der entsprechenden DNS-Zone einen sogenannten SPF-Record. Technisch gesehen handelt es sich hierbei um einen TXT-Record, dessen Syntax in der RFC7208 exakt spezifiziert ist.

Bei der Zustellung einer E-Mail entnimmt der empfangende Server die Absender-Domain aus dem Envelope Sender einer E-Mail. Anschließend wird im Rahmen einer DNS-Abfrage ermittelt, ob für die Domain ein SPF-Record existiert. Diese Prüfung wird optional zusätzlich für den Host-Eintrag des Absenders (EHLO-Client-ID) durchgeführt. Taucht die IP-Adresse oder der FQDN (Fully Qualified Domain Name) des einliefernden Servers nicht im SPF-Record auf, ist er für den Versand von E-Mails im Namen dieser Domain auch nicht autorisiert.

Zusätzliche Kryptografie

Im Falle von Domain Keys Identified Mail (DKIM) wird ebenfalls ein TXT-Record in Form einer RFC-normierten Syntax in der DNS-Zone der zu schützenden Domain erstellt. Zusätzlich kommt bei DKIM mit dem Public-Key-Verfahren eine kryptografische Komponente zum Tragen. Im Unterschied zu SPF wird bei DKIM die Absender-Domain aus dem Body from der E-Mail untersucht.

Vor der Erstellung des Records wird ein Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel gebildet. Der öffentliche Schlüssel wird in Kombination mit anderen Informationen als DKIM-Record in der DNS-Zone hinterlegt. Der private Schlüssel verbleibt ausschließlich auf dem Server, der für den Versand autorisiert werden soll. Mithilfe des privaten Schlüssels erzeugt der absendende Server für jede ausgehende E-Mail eine kryptografische Signatur, die sowohl Teile des Headers als auch den Inhalt der E-Mail umfasst. Idealerweise verfügt der Server über jeweils einen anderen Schlüssel für jede Domain, für die er E-Mails versenden soll.

Die erzeugte DKIM-Signatur wird als X-Header-Wert in den Header der jeweiligen E-Mail geschrieben. Der empfangende Server einer DKIM-geschützten E-Mail ermittelt dazu zunächst die Absender-Domain der E-Mail, gefolgt vom sogenannten Selektor. Der Selektor ist fester Bestandteil einer DKIM-Signatur und gibt an, unter welchem Namen der passende öffentliche Schlüssel in der DNS-Zone der Absender-Domain zu finden ist. Nachdem er den öffentlichen Schlüssel heruntergeladen hat, wird im Rahmen eines kryptografischen Vorgangs die Signatur geprüft. Schlägt diese Prüfung fehl, liegt entweder der falsche öffentliche Schlüssel vor, oder die E-Mail wurde unterwegs verändert.

Die DKIM-Signatur stellt somit zwei Dinge sicher: Zum einen weiß der empfangende Server, dass die E-Mail samt Inhalt auf dem Transportweg nicht verändert worden ist. Zum anderen weiß er, dass der Inhaber der im Header angegebenen Absender-Domain den Server autorisiert hat. Im Unterschied zu kryptografischen Signaturen mittels S/MIME oder PGP sieht der Empfänger einer E-Mail die DKIM-Signatur nicht. Es ist ein rein serverbasiertes Verfahren. Erst wenn man sich den Header einer E-Mail anzeigen lässt, wird die DKIM-Signatur sichtbar.

Kontrolle durch Reporting

Weder SPF noch DKIM geben dem empfangenden Server klare Anweisungen, was mit E-Mails passieren soll, die die SPF- und DKIM-Prüfung nicht bestanden haben. Diese Lücke schließt DMARC (Domain-based Message Authentication, Reporting and Conformance).

DMARC ergänzt die SPF- und DKIM-Prüfungen um das sogenannte Alignment. Es stellt sicher, dass die Envelope-Sender-Adresse mit der Body-from-Adresse übereinstimmt. Diese Prüfung ist deshalb wichtig, weil die gängigsten E-Mail-Programme lediglich die Body-from-Informationen einer E-Mail anzeigen und der Empfänger somit leicht getäuscht werden kann. Genau diesen Umstand machen sich beispielsweise Angreifer zunutze, die einem Unternehmen mit der Chef-Betrugsmasche, die häufig auch CEO-Fraud genannt wird, Schaden zufügen wollen.

Eine weitere Besonderheit von DMARC ist die Berichtsfunktion. Sie sorgt dafür, dass der Inhaber einer Domain regelmäßig darüber informiert wird, welche Server in seinem Namen E-Mails versendet haben und ob die Prüfung beim Empfänger erfolgreich war oder nicht. So bekommt er nicht nur einen guten Überblick über seine im Internet versendeten E-Mails, sondern auch wertvolle Informationen, ob seine SPF- und DKIM-Einträge vollständig und syntaktisch korrekt sind.

FÜNF SOFORTTIPPS FÜR UNTERNEHMEN

Aktuell kann jedem Unternehmen nur geraten werden, folgende fünf kostenfreie und einfache Sofortmaßnahmen durchzuführen:

1. Die Konfiguration der eigenen Mail-Infrastruktur mit kostenlosen Tools wie ssl-tools.net und mxtoolbox.com testen.
2. Sofern noch nicht vorhanden, SPF-/DKIM- und DMARC Records einrichten.
3. TLS (Transport Layer Security) bei der Kommunikation mit bekannten Partnern erzwingen, wo dies möglich ist.
4. DANE (DNS-based Authentication of Named Entities) nutzen.
5. Prüfen, ob der Hersteller der eingesetzten Mail-Security-Lösung DANE nutzt, und – falls dies nicht der Fall ist – solche Funktionen aktiv einfordern bzw. alternative Produkte in Betracht ziehen.

Um DMARC zu aktivieren, hinterlegt der Inhaber einer Domain eine DMARC-Richtlinie in seiner DNS-Zone. Wie bei SPF und DKIM auch, wird die DMARC-Richtlinie in einem RFC-normierten TXT-Record gespeichert. Sie beinhaltet die Information, welche Prüfungen vom Empfänger gemacht werden müssen (SPF und/oder DKIM). Zusätzlich wird festgelegt, wie sich der Empfänger verhalten soll, wenn die Prüfungen fehlschlagen. Annehmen, in Quarantäne stecken oder Abweisen sind die möglichen Aktionen. Darüber hinaus werden in der DMARC-Richtlinie diejenigen E-Mail-Adressen hinterlegt, an die Berichte geschickt werden sollen. Diese werden von allen Servern im Internet erstellt, die DMARC beim E-Mail-Empfang unterstützen und auch E-Mails von der jeweiligen Domain erhalten haben. Die Berichterstattung erfolgt dann täglich.

Richtiger Einsatz und Risiken

Ein alleiniger Einsatz von SPF-Records für den Schutz der eigenen Domain und bei der Prüfung eingehender E-Mails ist nur bedingt hilfreich. Er birgt sogar gewisse Risiken. Auf den Schutz der eigenen Domain bezogen bedeutet der alleinige Einsatz von SPF, dass der E-Mail-Administrator fortlaufend Änderungen seiner Infrastruktur im Auge behalten muss, um so die Aktualität des SPF-Records sicherzustellen. Dies beinhaltet nicht nur die E-Mail-Server als solche, die für den Versand zuständig sind, sondern auch die dazugehörigen IP-Adressen.

Bei der Betrachtung müssen auch Server berücksichtigt werden, die womöglich nicht im eigenen Netzwerk stehen. Das gilt vor allem für den Versand von Newslettern. Eine flächendeckende Überwachung dieser Infrastruktur ist nur schwer möglich und so kann es schnell zu Lücken in den SPF-Records kommen, die im schlimmsten Fall dazu führen, dass E-Mails vom Kommunikationspartner nicht angenommen werden. Gute Newsletter-Versanddienste kann man übrigens daran erkennen, dass Sie nicht nur Unterstützung bei der Pflege der SPF-Records anbieten, sondern vielmehr den Versand über eigens für diesen Dienst eingerichtete Subdomains empfehlen oder gar verlangen.

Die Abweisung einer E-Mail lediglich aufgrund einer fehlgeschlagenen SPF-Prüfung ist ebenfalls riskant. Die E-Mail könnte gegebenenfalls weitergeleitet, oder über eine Mailingliste verschickt worden sein. Beide Szenarien führen zu Fehlern bei der SPF-Prüfung weil der weiterleitende Server in der Regel nicht im SPF-Record der ursprünglichen Absender-Domain gelistet ist.

Weitergeleitete Nachrichten

Letzteres wird beispielsweise durch den Einsatz von DKIM entschärft. Beim ursprünglichen Versand der E-Mail wird sie um eine DKIM-Signatur angereichert, die im Header der E-Mail verankert ist. Vorausgesetzt, sie wird von den im weiteren Verlauf beteiligten Relay-Servern nicht entfernt, kann sie vom Zielserver erfolgreich geprüft werden. Im Szenario „Weiterleitung einer E-Mail“ würde der empfangende Server feststellen, dass die SPF-Prüfung zwar fehlschlägt, die E-Mail aber über eine gültige DKIM-Signatur verfügt.

Der Einsatz von DKIM ist dabei relativ risikoarm. Bei der Erstellung der DKIM-Signatur muss lediglich darauf geachtet werden, dass die E-Mail danach nicht mehr verändert werden darf. Etwaige Disclaimer oder einfache Signaturen müssen im Vorfeld an die E-Mail angehängt werden. Anderenfalls würde die Signatur brechen. Idealerweise wird deshalb die DKIM-Signatur vom letzten Mail Transfer Agent (MTA) in der eigenen E-Mail-Kette aufgebracht.

Wenn DKIM-Signaturen beim Empfang von E-Mails geprüft werden sollen, sollte dies so früh wie möglich geschehen – idealerweise auf dem ersten MTA in der E-Mail-Kette. Viele Systeme belassen nach der Prüfung die Signatur im Header der E-Mail, damit sie später gegebenenfalls noch einmal geprüft werden kann. Diese Vorgehensweise ist auch durchaus empfehlenswert.

Eindeutige Domain-Zuordnung

Wie oben bereits angedeutet, lassen die Ergebnisse der SPF- und DKIM-Prüfung immer noch die Frage nach dem Willen des Absenders offen. Diese Informationslücke wird mit einer DMARC-Richtlinie geschlossen. In dieser erklärt der Absender zweifelsfrei, wie und mit welchen Technologien seine ausgehenden E-Mails geschützt sein müssen und wie im Fehlerfall mit den E-Mails umzugehen ist. Des Weiteren kann der Domain-Inhaber über die Ergebnisse der Prüfung informiert werden. DMARC erfordert aber auch, dass die Domain im Envelope Sender mit der Domain im Body from übereinstimmt. Dies soll sicherstellen, dass der Empfänger sicher sein kann, dass alle durchgeführten Prüfungen für die Domain erfolgten, die er in seinem E-Mail-Programm angezeigt bekommt.

Angreifern Paroli bieten

Ein Angriff im Namen von Paypal könnte beispielsweise folgendermaßen aussehen: Im Body from wird Paypal als Absender angezeigt, während im Envelope Sender eine gänzlich andere Domain angegeben wird. Unbedarfte Benutzer klicken deshalb eher auf einen Link in der E-Mail oder öffnen eine harmlos erscheinende Anlage. Paypal hat seine Domains jedoch mit einem DMARC-Record geschützt, um Missbrauch einzudämmen. Wenn das empfangende E-Mail-Gateway diese wertvollen Informationen aber nicht auswertet, bleiben sie nutzlos.

Dieses Beispiel zeigt eindrucksvoll, wie wichtig die Prüfung der Absender-Domain im Rahmen eines intelligenten E-Mail-Managements geworden ist. Anders als die oft verwendeten pattern- oder sandbox-basierten Verfahren, unterliegen die Absenderreputationsverfahren nicht dem viel zitierten Hase-und-Igel-Wettlauf zwischen Angreifern und Sicherheitssoftware. Die Prüfung erfolgt zudem in Echtzeit und ermöglicht so eine zeitnahe Zustellung der E-Mail. Wer also weder selbst in Fallen tappen noch seinen guten Ruf aufs Spiel setzen will, sollte möglichst rasch sein E-Mail-Management auf den neuesten Stand bringen.

Stefan Cink
Produktmanager, Net at Work

Treffpunkt für Insider

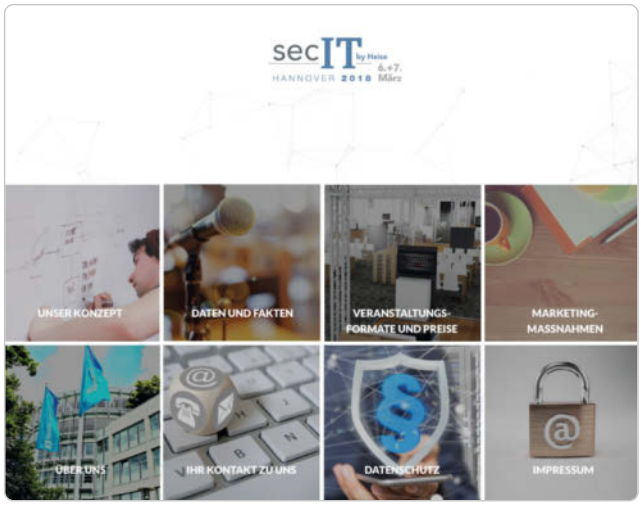
secIT: Im März 2018 gibt es in Hannover ein neues IT-Security-Event

Intensiver Informationsaustausch ist für IT-Sicherheitsexperten unabdingbar. Deshalb will das IT-Medienhaus Heise mit einem speziellen Veranstaltungsformat Security-Firmen und Unternehmensvertretern eine Plattform bieten, auf der insbesondere der persönliche Kontakt im Vordergrund steht.

Offenbar wurde es den CeBIT-Veranstaltern nach mehr als 30 Jahren plötzlich zu kühl im norddeutschen Frühling. Im nächsten Jahr findet die IT-Messe zwar natürlich wieder in Hannover statt, doch dann endlich im – zumindest potenziell – etwas angenehmeren Juni. Und mit ihr zieht auch einer der mittlerweile wichtigsten Treffpunkte der IT-Sicherheitsbranche, die Heise Security Plaza, in den Sommer um. Aussteller und Besucher des Security-Events müssen sich allerdings keineswegs sorgen, dass der gewohnte Frühjahrstermin jetzt gänzlich flachfällt: Heise Medien stellt ein neues Veranstaltungsformat auf die Beine, das mehr als nur die – jahreszeitliche – Lücke füllen soll.

Same time, same place

Doch warum hat man sich für die secIT ausgerechnet wieder Hannover und den kalten März ausgesucht? „Hannover, März, IT-Veranstaltung – das ist seit 30 Jahren einfach gelernt und insbesondere die Aussteller der CeBIT Security Plaza haben betont, wie wichtig für sie eine IT-Security-Veranstaltung im ersten Quartal des Jahres in Norddeutschland ist“, erklärt Jörg Mühle, Vice President Sales und Mitglied der Geschäftsleitung von Heise Medien, und ergänzt: „On top gibt es nun endlich ausreichend bezahlbare Hotelzimmer!“ Auch die langjährigen Sponsoren der Security Plaza zeigen großes Interesse an der secIT. Das beweise das bisherige positive Feedback und die zahlreichen Buchungen der Firmen, die seit der Bekanntgabe eingegangen seien. Außerdem habe man im Vorfeld „im Rahmen von zwei Roundtables das Konzept mit über 50 Unternehmen diskutiert und dadurch wertvollen Input für die Umsetzung gewonnen“.



Quelle: Heise Medien GmbH & Co KG

Auf *https://sec-it.heise.de* erfährt man mehr über das neue Event.

Für die Planung des neu konzipierten Veranstaltungsformats kann Heise Medien darüber hinaus auf reichlich Erfahrung und Expertise aus den eigenen Reihen zurückgreifen. So sei die secIT ein echtes Gemeinschaftsprojekt des Verlagshauses, für das sich insbesondere die Redaktion der c’t engagiert habe. „Konkret hilft uns das Security-Ressort der c’t Redaktion bei der Themenfindung, der Ansprache von unabhängigen Fachreferenten aus dem In- und Ausland, sowie der Umsetzung redaktioneller Workshops die im Rahmen der secIT stattfinden werden“, erläutert Jörg Mühle.

Die Chancen stehen gut dafür, dass das IT-Security-Event zu einer Erfolgsmarke werden kann. Schließlich stehen topaktuelle Schwerpunktthemen auf der Agenda, allen voran Herausforderungen und Problemlösungen in den Bereichen Security im Unternehmen, Digitalisierung, IoT, Industrie 4.0, DSGVO und Endpoint Security. Dabei soll dann nicht allein die technische Perspektive vorherrschen, auch wirtschaftliche Aspekte werden ausreichend Beachtung finden. Man sei deshalb zuversichtlich, dass interessierte Teilnehmer in relevanter Größenordnung auf die secIT ansprechen werden. Erklärtes Ziel sei es, „500+ qualifizierte Fachbesucher für die beiden Tage zu gewinnen“, sagt Mühle.

Aktiver Austausch

Um das Fachpublikum aus der Entscheiderebene zu überzeugen und ein ebenbürtiges Pendant zur CeBIT Security Plaza anbieten zu können, will die secIT noch stärker auf Interaktion und Thementransfer zwischen Anbietern und Anwendern setzen. Neben einer Ausstellungsfläche mit klassischen Ständen von Anbietern, aber auch speziellen Themeninseln geht es um die Präsentation neuester Trends und aktueller Softwarelösungen in Workshops, Expert Talks und Vorträgen auf der Bühne der Niedersachsenhalle. Auf diese Weise sollen die Besucher in den zwei Tagen möglichst viele Informationen und Lösungsvorschläge mit auf den Weg bekommen.

Und wird es auch Vergleichbares wie die berühmt-berüchtigten Live-Hacking-Sessions geben, die auf der CeBIT Security Plaza regelmäßig für Überfüllung sorgten? „Live-Hacking-Sessions sind natürlich ebenfalls in der Planung“, verspricht Jörg Mühle. Wichtig sei den Programmverantwortlichen dabei aber, „den Teilnehmern zu zeigen: Ich werde angegriffen, was ist nun als Erstes zu tun?“ Denn vorrangig gehe es ja darum, neben der Problemerkennung auch Lösungsansätze aufzuzeigen.

Das genaue Programm der secIT steht gegenwärtig noch nicht fest. Derzeit werden weitere namhafte Referenten angesprochen und für das Event mobilisiert. Ab Ende November geht dann ein erster Programmüberblick online. Aber sicher ist schon jetzt das Programm zum Abschluss des ersten Veranstaltungstages: Am 6. März sorgt die secIT-Party für einen heißen niedersächsischen Frühlingsabend.

Rudolph Schuster
Redaktion MittelstandsWiki

KI – die Lösung aller Security-Probleme?

KI-Anwendungen ermöglichen es, mit schlanken Ressourcen effektiv zu agieren

Sicherheit geht einher mit dem Wunsch, das Risiko zu kontrollieren. Zuviel Kontrolle verlangsamt aber bestehende Prozesse und beeinträchtigt das betriebliche Gefüge. Man braucht folglich effiziente Methoden, um bekannte, aber auch bislang noch nicht beobachtete Bedrohungen abzuwehren.

Viele Unternehmen stecken beim Thema IT-Security in einer Zwickmühle: Sie müssen ausbalancieren zwischen dem Wunsch, Informationen zugänglich zu machen, und dem Bedürfnis, sensible Informationen vor unbefugten und missbräuchlichen Zugriffen zu schützen.

Die spektakulären Sicherheitsvorfälle der letzten Zeit haben gezeigt, dass das Modell „Erkennen und Reagieren“ in eine Sackgasse führt. Mit den damit einhergehenden aufwendigen manuellen Kontrollen wird primär Schadensbegrenzung betrieben. Die einzigen Variablen im System sind die „Zeit bis zum Erkennen“ und die „Dauer der Isolation“. Dabei sind ungefähr 60 % aller Angriffe binnen weniger Minuten erfolgreich, und es dauert im Durchschnitt 229 Tage bis ein solcher Angriff erkannt wird.

Versuche, die Situation in den Griff zu bekommen, gibt es viele. Anbieter von Sicherheitslösungen bringen Signatur-Updates in möglichst rascher Folge aus, teilweise im Minutentakt oder per Internet-Feed. Dazu kommen Lösungen, die Signaturen bereits am Perimeter oder im Netzwerk anwenden. Technologien wie Sandboxing sollen helfen, Signaturen automatisiert zu erstellen, um beispielsweise URLs oder bestimmte Pakete im Netzwerkdatenstrom zu erkennen und zu blockieren (wie Bot-Net- und Command-and-Control/C2-Traffic). Dies verhindert aber selten den Erstbefall, sondern lediglich die nachfolgenden Infektionen.

Hohe Erwartungen

Eine Möglichkeit, mit schlanken Ressourcen dennoch wirkungsvoll zu handeln, bieten spezielle Methoden, die auf künstlicher Intelligenz (KI) basieren. Die im Rahmen einer Studie zum Einsatz von KI in Unternehmen befragten IT-Entscheider sind hinsichtlich des Potenzials sehr optimistisch und planen weitere Investitionen. Vorteile versprechen sich die Befragten u. a. beim Analysieren von Sicherheitstrends. 77 % der Befragten bestätigen, mithilfe von KI mehr Datenschutzverletzungen verhindert zu haben als zuvor, und 81 % sagen, dass KI in der Lage ist, Bedrohungen zu erkennen, bevor das den IT-Sicherheitsverantwortlichen gelingt. 74 % geben zusätzlich an, dass sie die durch fehlende Fachkräfte entstandene Lücke ohne künstliche Intelligenz nicht würden schließen können.

Trotzdem hat der inflationäre Gebrauch der Begriffe maschinelles Lernen und künstliche Intelligenz teilweise mehr Verwirrung gestiftet als zur Erhellung beigetragen. Der Machine-Learning- und KI-Hype ruft mittlerweile auch Trittbrettfahrer ohne substanzielle Produktumsetzungen auf den Plan. Inzwischen gibt es aber Technologien, die Angriffe und Malware-Attacken präventiv verhindern. Dazu dient die State-Analyse von ausführbarem Code, bevor dieser ausgeführt wird. Die Software wertet eine enorme Menge an Dateieigenschaften aus und erlaubt auf dieser Basis eine vorausschauende Analyse. Hier sind umfangreiche mathematische Modelle die Grundlage, anders als bei der überwiegenden Zahl traditioneller Antiviren- oder Anti-Malware-Lösungen, die sich meistenteils auf Signaturen oder Heuristik verlassen.

Prävention statt Reaktion

Statt nur zu reagieren, liegt das Augenmerk also wieder auf Vorsorgemaßnahmen. Dazu werden komplett neue Wege beschritten, weg vom massenhaften Erstellen von Signaturen hin zu vorhersagenden statistischen Methoden, die maschinelles Lernen und selbsttrainierende KI-Modelle nutzen. Sie ermitteln das Schadrisiko von ausführbarem Code und entscheiden dann, ob eine Datei sicher ist und ausgeführt werden kann oder in Quarantäne gestellt werden muss. Die Trefferquote solcher patentierter Verfahren ist zum Teil doppelt so hoch wie bei traditionellen Verfahren bei gleichzeitig sehr niedrigem Falsch-Positiv-Anteil.

Technisch betrachtet handelt es sich um eine statistische Analyse. Eine Datei wird vor der Ausführung in hunderttausende Merkmale zerlegt, quasi die DNA der jeweiligen Datei. Neben eingängigen Kennzeichen wie Ersteller, Datum, Version, PE-Header, digitale Signatur, angezeigtes Icon, gibt es heute zirka drei Millionen relevanter weiterer Merkmale, z. B. normalisierte Byte-Strings, die von einem Computer zur statistischen Bewertung herangezogen werden. Das zugrundeliegende mathematische Modell verarbeitet alle diese Merkmale, um anschließend eine Datei als schädlich oder harmlos einstufen zu können. Es übernimmt dabei die Funktion, die in traditionellen Lösungen die Signaturdatenbank erfüllt hat. Wenn man auf diese Weise an die Malware-Erkennung und Malware-Abwehr herangeht, entfallen ständige Pattern- und Engine-Updates, und neue Bedrohungen erkennt man ohne einen „Patient Zero“.

Mathematische Modelle

Zunächst benötigt man einen ausreichend großen Trainingskorpus aus mehr als einer Milliarde Dateien. Diese unterteilt man akkurat in „gut“ und „schädlich“. Alle Merkmale dieser Dateien werden dann extrahiert und bilden die Bewertungsbasis. Anhand dieser Grundlage lernt eine

Maschine, relevante Merkmale zu begreifen und Dateien zu bewerten, um dann schließlich zu entscheiden, ob diese Kennzeichen die einer harmlosen oder schädlichen Datei sind. Eine Phase, die man als „Supervised Machine Learning“ oder „Deep Learning“ bezeichnet. Nach dem initialen Anlernen beginnt man damit, weitere, der Maschine unbekannte Dateien ebenfalls zu klassifizieren. Im Ergebnis entstehen immer wieder neue mathematische Modelle. Die erfolgreichsten bleiben bestehen, während weniger effiziente verworfen werden. Ist die Erkennungsrate im Hinblick auf Falsch-Positive und Falsch-Negative so effizient, wie man es sich wünscht, kann der Prozess vollautomatisch durch die Maschine abgewickelt werden. Selbst für bis dato unbekannte Dateien.

KI-Verfahren, die den Erfolg bewerten, sind beispielsweise neuronale Netze, bei denen für richtige Entscheidungen automatisch neue Entscheidungswege verknüpft werden. Für die Berechnungen werden riesige Computercluster mit mehreren zehntausend Prozessorkernen zusammengeschaltet, die wochenlang fortlaufende Optimierungsberechnungen durchführen. Das Ergebnis ist ein fertiger Algorithmus, der auf einem Computersystem ausgerollt werden kann und binnen Millisekunden eine Bewertung vornimmt.

KI-gestützte Lösungen

Sinnvoll sind diese Technologien in zweierlei Hinsicht. Moderne Endpoint-Schutzlösungen kommen ohne Signatur-basierten Anteil aus. Das schont Systemressourcen, denn der Schadcode lässt sich in den allermeisten Fällen bereits vor der Ausführung stoppen. Gleichermaßen sollte eine Lösung Bedrohungen zuverlässig adressieren, die über Skripte (Powershell, Visual Basic, Makros) auch ohne Payload wirken oder die Exploits ausnutzen. Effizienztests bestätigen, dass KI-gestützte Lösungen dabei sehr gute Leistungen erzielen, welche die Erkennungsraten traditioneller Ansätze deutlich übertreffen. Das deckt sich mit den eingangs erwähnten Studienergebnissen: 86 % der Befragten sagen, dass die von ihnen eingesetzten KI-basierenden Technologien ihr Versprechen eingelöst und die Erwartungen erfüllt haben. 64 % der IT-Entscheider erwarten bereits innerhalb von zwei Jahren einen ROI in Bezug auf die von ihnen eingesetzten KI-Tools.

Ein typisches Manko vieler Antivirenlösungen ist zudem, dass sie sich negativ auf die Performance auswirken. Die KI-basierende Herangehensweise bindet hingegen nur etwa ein Zehntel der CPU- und RAM-Ressourcen. Gleichzeitig braucht man weniger Bandbreite und eine zentrale Massendatenspeicherung für EDR-Systeme wird zumeist überflüssig. Selbst in modernen VDI-Umgebungen lässt sich die Dichte von Benutzersitzungen deutlich steigern. Das funktioniert natürlich nur dann, wenn eine Lösung nicht auf ressourcenintensiven Pattern-Matching-Engines aufsattelt, sondern eigenständig arbeitet, auch autark ohne vorhandene Internetverbindung.

Die unternehmerische Intelligenz setzt sich durch

Das Potenzial von KI-Lösungen schätzen die Studienteilnehmer auch im Hinblick auf die Wettbewerbsfähigkeit ihres Unternehmens als ausgesprochen positiv ein. „KI-basierende Technologien verschaffen unserer IT-Abteilung einen klaren Wettbewerbsvorteil“, sagen stolze 87 % der Befragten. 83 % der Studienteilnehmer investieren bereits ganz gezielt in künstliche Intelligenz, um sich von der Konkurrenz abzusetzen. Schon jetzt nutzen 60 % KI-basierte Tools und Lösungen und 79 % der Entscheider geben an, dass KI zu den Top-Prioritäten auf der Vorstands- und Geschäftsführungsebene gehört.

Nicht jedes Unternehmen ist aus dem Stand in der Lage, auf eine KI-basierte Lösung umzusteigen. Vor allem für kleinere Betriebe stellen die organisatorischen, personellen und finanziellen Investitionen eine große Herausforderung dar. Wer sich mit dem Gedanken trägt, sollte eine Lösung wählen, die sich für den parallelen Betrieb eignet. Das sorgt für einen nahtlosen Übergang, bis die bestehende Technologie endgültig abgelöst wird.

Sascha Dubbel
Senior Sales Engineer DACH, Cylance

Starker Schutz vor Identitätsdieben

Die Sicherheit von Nutzeridentitäten erfordert starke Authentisierungsmethoden

Angesichts der zahlreichen Sicherheitsvorfälle bei Online-Diensten und der damit verbundenen, oftmals millionenschweren Fälle von Identitätsdiebstahl will die kürzlich gegründete Arbeitsgruppe „Starke Authentisierung – jetzt!“ den Weg zum Einsatz geeigneter Authentisierungsverfahren im Internet ebnen.

Obwohl inzwischen viele sichere und benutzerfreundliche Mechanismen zur starken Authentisierung im Internet existieren, werden diese bislang in der Praxis nur selten eingesetzt. Trotz der bekannten Schwächen erfolgt die Anmeldung bei Online-Diensten im Regelfall einfach mit Benutzername und Passwort. Auf der anderen Seite belegt die stetig zunehmende Zahl von Cyberangriffen auf Anbieter von Online-Diensten und die damit einhergehenden kostspieligen Folgen von Identitätsdiebstahl im Jahr 2016, dass statische Passwörter im Internet alleine keinen ausreichenden Schutz mehr bieten. Somit müssen zukünftig im Einklang mit den einschlägigen Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und EU-weit geltenden Regularien stärkere Mechanismen zur Authentisierung eingesetzt werden. Vor diesem Hintergrund zielt die verbandsübergreifende Arbeitsgruppe „Starke Authentisierung – jetzt!“ darauf ab, den praktischen Einsatz von sicheren Authentisierungsmechanismen im Internet durch Sensibilisierung von Nutzern und Anbietern von Online-Diensten zu fördern und die Verwendung geeigneter Verfahren im Internet tatkräftig zu unterstützen.

Was bedeutet starke Authentisierung?

Die Identität einer Entität ist durch die ihr zugeordneten Attribute bestimmt. Diese umfassen bei einer natürlichen Person z. B. Name, Anschrift, Geburtsdatum, Kontonummer, E-Mail-Adresse und Telefonnummer, bei einer juristischen Person neben dem Namen und der Anschrift z. B. eine Registernummer, eine Steuernummer, die Umsatzsteuer-ID und den Verweis auf vertretungsberechtigte natürliche Personen. Aus Gründen der Datensparsamkeit (vgl. § 3a BDSG) wird man nicht in jedem Kontext alle Attribute einer natürlichen Person verwenden, sondern nur die im konkreten Fall notwendige Untermenge (partielle Identität), die gegebenenfalls auch nur aus einem anwendungsspezifischen Pseudonym bestehen kann.

Mit *Authentisierung* bezeichnet man das Aufstellen einer Behauptung über eine solche partielle Identität, die *Authentifizierung* wiederum ist die Prüfung dieser Behauptung. Hierfür können unterschiedliche Verfahren sowie Authentifizierungsfaktoren aus den Bereichen Besitz, Wissen und Inhärenz verwendet werden. Bei einer dynamischen Authentifizierung kommen im Regelfall kryptografische Mechanismen zum Einsatz, sodass sich die Daten zum Nachweis der Identität bei jedem Authentifizierungsvorgang ändern. Von einer starken Authentifizierung spricht man, wenn zusätzlich mindestens zwei unabhängige Faktoren eingesetzt werden.

Bei einer *starken Authentisierung* dienen also zwei Faktoren (2FA) in einem dynamischen Protokoll zum Nachweis der Identität oder der Autorisierung einer Transaktion. Eine starke Authentisierung wird beispielsweise gemäß Artikel 97 der EU-Richtlinie 2015/2366 für den Zugriff auf ein Zahlungskonto gefordert. Artikel 8 der EU-Verordnung 910/2014 verlangt entsprechende Verfahren bei einem elektronischen Identifizierungssystem ab dem Sicherheitsniveau „substanziell“, was auch dem beim Schutz von personenbezogenen Daten gemäß Artikel 32 der EU-Verordnung 2016/679 zu berücksichtigenden Stand der Technik entspricht.

Ein Blick in die Praxis

In der wissenschaftlichen Literatur und in internationalen Standards finden sich unzählige unterschiedliche Verfahren für die Authentifizierung. Eine vollständige Aufzählung aller existierenden Verfahren würde sicherlich den Rahmen dieses Beitrags sprengen, sie erscheint überhaupt grundsätzlich unmöglich. Vielmehr wurde im Rahmen der Diskussion unter den in der verbandsübergreifenden Arbeitsgruppe mitwirkenden Experten ein grobes Klassifizierungsschema entwickelt, in das sich die in der Praxis eingesetzten Verfahren einteilen lassen.

Eine generelle Beobachtung ist, dass von den grundsätzlich möglichen Faktorkombinationen (Besitz + Wissen, Besitz + Inhärenz, Wissen + Inhärenz) in der Praxis die Kombination aus Besitz und Wissen klar dominiert und biometrische Authentifizierungsmechanismen im Internet bislang kaum in der Praxis Verwendung finden. Allerdings ist damit zu rechnen, dass sich dies im Zuge der breiten Verfügbarkeit von Smartphones mit Fingerabdrucksensor und entsprechender Standards wie FIDO-UAF und W3C-WA mittelfristig ändern dürfte. Aktuell werden für die Authentifizierung im Internet insbesondere die nachfolgend aufgeführten Authentisierungstoken, jeweils in Verbindung mit einem zusätzlichen wissensbasierten Faktor (z. B. PIN), eingesetzt.

ID-Cards

Elektronische Ausweisdokumente, wie z.B. der elektronische Personalausweis, können zur starken Authentisierung im Internet genutzt werden. Im Fall des Personalausweises wird hierfür ein geeignetes Kartenterminal oder Smartphone benötigt und das Extended-Access-Control-Protokoll (Version 2) gemäß der BSI-Richtlinie TR-03110 ausgeführt. Der Zugriff auf die im Ausweis gespeicherten Daten setzt ein Berechtigungszertifikat voraus, durch das die Bürgerinnen und Bürger die Identität des zugreifenden Online-Dienstanbieters und

den Zweck des Datenzugriffs erkennen können. Auf dem Personalausweis sind die in § 18 PAuswG aufgeführten Identitätsattribute (d. h. Familienname, Geburtsname, Vornamen, Doktorgrad, Tag der Geburt, Ort der Geburt, Anschrift, Dokumentenart, Ordensname, Künstlername) gespeichert. Außerdem können mit dem sogenannten „dienste- und kartenspezifischen Kennzeichen“ sehr datenschutzfreundliche, anwendungsspezifische Pseudonyme berechnet werden. Darüber hinaus lässt sich auch eine datenschutzfreundliche Altersverifikation oder Wohnortbestätigung durchführen.

Signaturtoken

Bei Hardwarekomponenten wie Signaturtoken wird zur Authentisierung eine digitale Signatur über eine „Challenge“ erstellt, in die eine von der prüfenden Instanz gewählte Zufallszahl einfließt. Wie der letztlich zu signierende Wert gebildet wird, ist bei den verschiedenen auf diesem Prinzip basierenden standardisierten Authentisierungsprotokollen geringfügig unterschiedlich. Das Signaturtoken kann als Signaturkarte ausgeprägt sein, sodass man damit auch qualifizierte elektronische Signaturen erstellen oder Banktransaktionen mittels FinTS absichern kann. Für die Nutzung einer Chipkarte zur Authentisierung ist ein entsprechendes Chipkartenterminal notwendig, das im Regelfall über die USB-Schnittstelle an einen Rechner angeschlossen wird. Um die Benutzerfreundlichkeit zu erhöhen, kann die Chipkarte mit dem Kartenterminal integriert und beispielsweise als USB-Token realisiert sein.

Quelle: ecsec GmbH

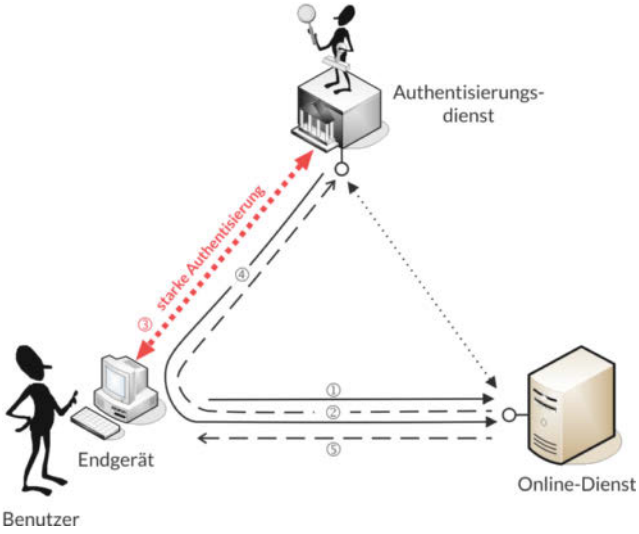
Abb. 1: Direkte Integration

Ein technisch sehr einfach gehaltenes, über USB oder per NFC nutzbares Token, das zur Signatur-basierten Authentisierung – und im Regelfall nur dazu – verwendet werden kann, ist das von der FIDO-Alliance spezifizierte „Universal Second Factor Token“ (U2F).

TAN-basierte Verfahren

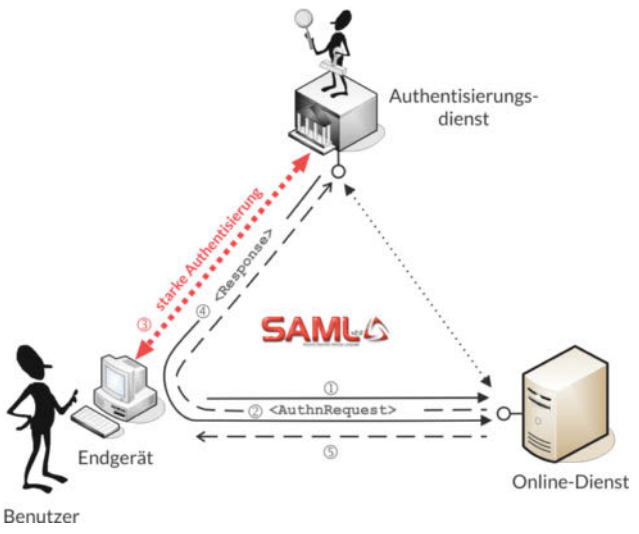
Sowohl beim elektronischen Personalausweis als auch bei den Signaturtoken, muss für die Realisierung des Protokollablaufs eine technische Kommunikationsschnittstelle zwischen dem Endgerät des Nutzers (PC, Tablet, Smartphone etc.) und dem kryptografischen Authentisierungstoken vorhanden sein. Falls eine derartige Schnittstelle nicht oder nur schwer realisiert werden kann, empfiehlt sich der Einsatz von TAN-basierten Verfahren, da hier die Übertragung der als Authentisierungscode fungierenden TAN durch den Nutzer selbst erfolgt. Generell unterscheiden sich die Verfahren danach, ob die TAN beim Benutzer oder auf Serverseite erzeugt wird.

Beim chipTAN-Verfahren wird zusätzlich zu einer Bankkarte ein mobiler TAN-Generator zur Entgegennahme der zu schützenden Transaktionsdaten und zur dezentralen Erzeugung der TAN benötigt. In ähnlicher Form existieren viele verschiedene Einmalpasswortgeneratoren, die in der Regel aus einem geheimen Schlüssel, einer Sequenznummer, dem Zeitpunkt und/oder einer Challenge eine zur starken Authentisierung geeignete TAN erzeugen, die vom Benutzer typischerweise auf einem anderen, vertrauenswürdigen Endgerät, z. B. zusätzlich zu einer Authentisierung mit Benutzername und Passwort, in ein entsprechendes Webformular eingegeben wird. Sofern keine physikalische Trennung vorhanden ist, müssen anderweitige Sicherheitsmechanismen zur zuverlässigen Separation der Ausführungsumgebungen vorgesehen werden, um die Sicherheit des Verfahrens gewährleisten zu können. Die Generierung der TAN muss nicht zwingend dezentral beim Benutzer erfolgen, sondern sie kann zentral erzeugt und wie beim mobileTAN-Verfahren



Quelle: ecsec GmbH

Abb. 2: Integration über spezialisierten Authentisierungsdienst



Quelle: ecsec GmbH

Abb. 3: SAML-basierte Integration

oder der österreichischen Handysignatur als SMS auf ein Mobiltelefon übertragen werden.

Anmeldung per Smartphone

Neben den oben beschriebenen Methoden werden naturgemäß immer öfter Smartphones verwendet. Ein Beispiel für den breitflächigen Einsatz eines Smartphone-basierten Verfahrens zur starken Authentisierung und Identifizierung ist die schwedische „E-Legitimation". Hierbei handelt es sich um ein elektronisches Identifizierungsmittel (eID), das von den schwedischen Banken herausgegeben wird und vom schwedischen Staat legitimiert ist. Mit der BankID/Mobilt BankID können sich Privatpersonen im Internet gegenüber Unternehmen, Banken und Behörden identifizieren und mittels fortgeschrittener elektronischer Signaturen sogar Verträge abschließen.

Alle Privatpersonen, die über eine schwedische Personennummer verfügen, können sich eine BankID ausstellen lassen. Für die mobile Authentisierung benötigt der Bürger die Schwedische Personennummer, die BankID/Mobilt BankID und die BankID-Sicherheits-APP. Die BankID/Mobilt BankID nutzt ein Softtoken, ist zwei Jahre lang gültig und kann über die Bank gesperrt werden. Falls man das Passwort vergisst, muss man eine neue BankID beantragen. Die Verwendung ist sehr einfach: Der Anwender öffnet über einen Browser die Internetseite des gewünschten Dienstleistungsanbieters, z. B. seinen digitalen Behördenbriefkasten. Gleichzeitig muss auf dem Handy die BankID-Sicherheits-APP gestartet sein und der Anwender bestätigt die Legitimation oder die Signaturerstellung jeweils mit seinem achtstelligen Sicherheitscode. Alle wichtigen Lebensbereiche des Bürgers sind bereits abgedeckt. Es kann etwa der Zugriff auf medizinische Daten, Krankenversicherung, Arbeitsamt, den elektronischen Postkasten für Behördenbriefe, Kreditauskünfte und nicht zuletzt auch die elektronische Steuererklärung genutzt werden.

Möglichkeiten der Integration

Wie oben erwähnt, sind grundsätzlich weitere Verfahren zur starken Authentisierung denkbar, die andere Authentisierungstoken und -protokolle sowie zusätzlich oder alternativ zum Faktor Wissen biometrische Merkmale nutzen. Darüber hinaus kann in bestimmten Anwendungsszenarien die Auswertung von weiteren Merkmalen, wie z. B. der aktuelle Ort des Zugreifenden oder der Zeitpunkt des Zugriffs, sinnvoll sein. Doch wie lassen sich die verschiedenen Modelle sinnvoll integrieren?

Direkte Integration: Im einfachsten Fall erfolgt die Integration eines Verfahrens zur starken Authentisierung direkt in den Online-Dienst (Abbildung 1), was insbesondere aus Sicherheitsgründen vorteilhaft sein kann. Auf der anderen Seite ist der Aufwand zur Integration unterschiedlicher Authentisierungsmechanismen oftmals proportional zur Anzahl der unterstützten Verfahren. Der Online-Dienst muss immer dann angepasst werden, wenn Änderungen an der eingesetzten Authentisierungstechnologie notwendig werden.

Spezialisierte Authentisierungsdienste: Um den Prozess der starken Authentisierung von den fachlichen Abläufen in Online-Diensten zu entkoppeln, empfiehlt sich der Einsatz eines spezialisierten Authentisierungsdienstes, der über standardisierte Protokolle für das föderierte Identitätsmanagement angesprochen werden kann. Hierdurch können leicht unterschiedliche Mechanismen zur starken Authentisierung unterstützt und notwendige technologische Fortentwicklungen ohne Auswirkungen auf den Online-Dienst vorgenommen werden (Abbildung 2).

In diesem Fall erfolgt nach dem Zugriff des Benutzers auf den Online-Dienst (1) eine Umleitung zum Authentisierungsdienst (2), der die starke Authentifizierung des Benutzers im Auftrag des Online-Dienstes mit einem geeigneten Verfahren durchführt (3) und das Ergebnis der Authentifizierung zum Online-Dienst zurückschickt (4), bevor der Benutzer im Erfolgsfall Zugriff erhält.

Damit die ausgelagerte Authentifizierung nicht missbraucht werden kann, müssen geeignete Sicherheitsmaßnahmen implementiert werden, die regelmäßig im Rahmen von Zertifizierungsverfahren (z. B. gemäß ISO 27001 auf Basis von IT-Grundschutz) zu prüfen und zertifizieren sind. Soweit im Rahmen der starken Authentifizierung auch personenbezogene Daten verarbeitet werden, sind die Anforderungen des Bundesdatenschutzgesetzes zu berücksichtigen, deren Erfüllung beispielsweise im Rahmen einer Zertifizierung gemäß des Trusted-Cloud-Datenschutzprofils für Cloud-Dienste nachgewiesen werden kann.

Quelle: ecsec GmbH

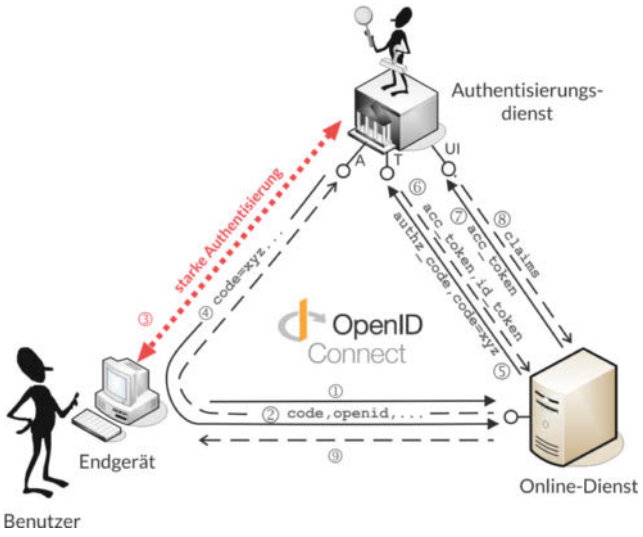


Abb. 4: OpenID-Connect-basierte Integration

Das heute am weitesten verbreitete Protokoll für das föderierte Identitätsmanagement und die Auslagerung der starken Authentisierung an einen spezialisierten Authentisierungsdienst ist das vom Security Services Technical Committee der internationalen Standardisierungsorganisation OASIS standardisierte SAML-Protokoll (Security Assertion Markup Language), bei dem XML-basierte Nachrichten ausgetauscht werden (Abbildung 3). Hierbei wird in Schritt (2) im Zuge der Umleitung an den Authentisierungsdienst ein <AuthnRequest> an den Authentisierungsdienst geschickt und in Schritt (4) das Ergebnis der Authentifizierung in einer <Response>-Nachricht an den Online-Dienst zurückgeschickt.

Ein weiteres Protokoll ist das auf dem OAuth 2.0 Authorization Framework basierende OpenID-Connect-Protokoll (Abbildung 4). Anders als bei SAML bietet der Authentisierungsdienst bei OpenID Connect zusätzlich zum Authentisierungsendpunkt weitere Endpunkte an: Authorization Endpoint (A), Token Endpoint (T) und UserInfo Endpoint (UI). Von diesen müssen zumindest die ersten beiden im Zuge eines Authentisierungsvorganges vom Online-Dienst angefragt werden, um das Ergebnis der Authentifizierung und möglicherweise ergänzende Identitätsinformationen (Claims) zu erhalten.

Hilfe und Informationen

Für die konkrete Integration der starken Authentisierung stellt sich die Frage, welche Open-Source-Softwarekomponenten und zertifizierten Authentisierungsdienste derzeit verfügbar sind. Für diesen Zweck wurden in der 2FA.jetzt-Initative entsprechende Übersichten erarbeitet (siehe https://www.2fa.jetzt/oss/ und https://www.2fa.jetzt/cert/), die von Mitgliedern der offenen 2FA-Community gepflegt und ergänzt werden können.

Umgekehrt ist es insbesondere für Nutzer interessant, welche Online-Dienste bereits Mechanismen zur starken Authentisierung unterstützen. Auch für diese Zwecke wurden in der 2FA.jetzt-Initiative spezielle Übersichtsseiten mit 2FA-fähigen Diensten erstellt (siehe https://www.2fa.jetzt/dienste/), die den Endnutzern eine Orientierung bieten, bei welchen Online-Diensten bereits heute ein sicheres Login-Verfahren zur Verfügung steht und genutzt werden kann.

Fazit

Die kürzlich gestartete Initiative „Starke Authentisierung – jetzt!“ hat bereits erste Schritte auf dem Weg zu einer breiten Nutzung sicherer digitaler Identitäten angestoßen. Doch angesichts der immer noch sehr zögerlichen Verbreitung starker Authentisierungsverfahren gibt es noch viel zu tun.

Interessierte Personen, Unternehmen und Organisationen sind deshalb sehr herzlich eingeladen, an dieser gemeinnützigen Initiative konstruktiv mitzuwirken und mit ihr unter „https://2fa.jetzt“ oder über „ask@2fa.jetzt“ Kontakt aufzunehmen.

Detlef Hühnlein
Geschäftsführer, ecsec Gmb

Den Datenschutz sicher im Griff

Warum die Einbindung der EU-DSGVO-Anforderungen in ein ISMS sinnvoll ist

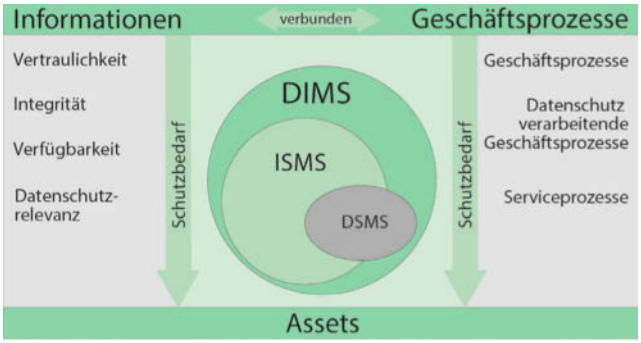
Mit der EU-DSGVO gewinnt das Thema Informationssicherheit deutlich an Bedeutung. Um die neuen Vorgaben im Unternehmen zu meistern, bietet es sich an, die Datenschutzanforderungen in vorhandene Informationssicherheitsmanagementsysteme zu integrieren.

Wer es jetzt immer noch nicht wissen sollte: Am 25. Mai 2018 wird die Anwendung der neuen EU-Datenschutz-Grundverordnung (EU-DSGVO) verbindlich. Mit der EU-DSGVO hat die EU-Kommission ein zentrales Rahmenwerk zur internationalen Harmonisierung des Datenschutzes der EU-Mitgliedsstaaten geschaffen. Neben Neuerungen zur Umsetzung des Datenschutzes wird die Unternehmenshaftung ausgeweitet. Je nach Art des Verstoßes drohen zukünftig empfindlich hohe Bußgelder, im Extremfall bis zu 4 % des Jahresumsatzes.

Interessanterweise beschäftigen sich laut aktueller Studien viele deutsche Unternehmen noch nicht mit diesem Thema. Aufgrund der zukünftig deutlich strengeren Vorschriften und Kontrollen im Datenschutz und der potenziell aus Verfehlungen drohenden Konsequenzen, sollten sich die Unternehmensverantwortlichen, die das Thema noch nicht auf der Agenda haben, jedoch dringend mit den anstehenden Herausforderungen auseinanderzusetzen.

Integrität und Vertraulichkeit

Diverse Positionen der EU-DSGVO nehmen direkt Bezug auf die Etablierung eines Information Security Management Systems (ISMS) im Unternehmen. So besagt etwa Art. 5 der EU-DSGVO u. a.: „Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (Integrität und Vertraulichkeit).“ Integrität und Vertraulichkeit sind bekannte Grundsätze beim Einsatz eines ISMS. In den bisher geltenden gesetzlichen Vorgaben waren sie allerdings in dieser Weise nicht gefordert.



DSMS = DatenSchutz-Management-System
DIMS = Datenschutz-Informationssicherheit-Management-System
ISMS = Informations-Sicherheits-Management-System

Quelle: WMC

Abb. 1: In einem DIMS lassen sich schützenswerte Informationen und Geschäftsprozesse nahtlos integrieren.

Quelle: WMC

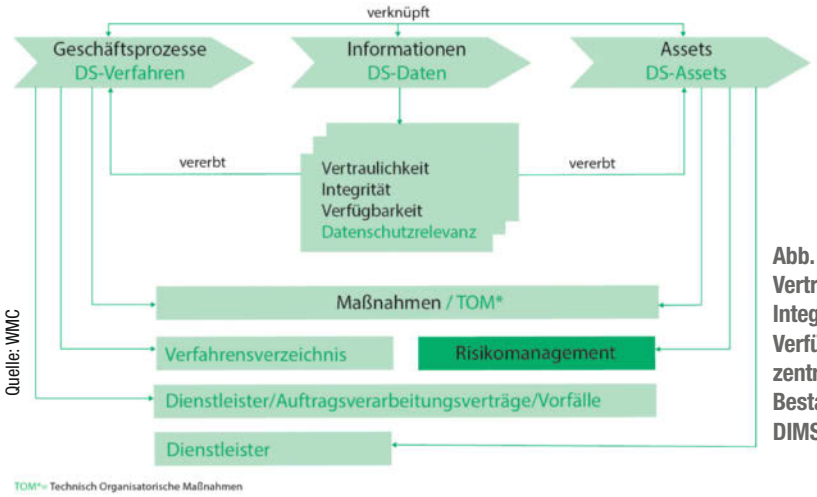
Abb. 2: Der Plan-Do-Check-Act-Kreislauf bei ISMS.

Sicherheit der Verarbeitung

Im Art. 32 Abs. 1 der EU-DSGVO finden sich folgende Bestimmungen: „Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.“ Weiter heißt es in Abs. 2: „Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugtem Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.“

Ein dem Risiko angemessenes Schutzniveau und ein dementsprechendes Risikomanagement sind Hauptbestandteile eines soliden ISMS. Listen von Maßnahmen technischer und organisatorischer Art im Datenschutz sind hier zukünftig keinesfalls mehr ausreichend.

Warum bietet es sich also an, die Anforderungen aus der EU-DSGVO in ein ISMS einzubinden? Eine gemeinsame Berücksichtigung von Datenschutz und Informationssicherheit in Form eines Datenschutz-Informa-



Quelle: WMC

Abb. 3: Vertraulichkeit, Integrität und Verfügbarkeit sind zentrale Bestandteile eines DIMS.

tionssicherheit-Managementsystem (DIMS, Abbildung 1) ist zu empfehlen, weil das gesamte Vorgehen zur Umsetzung der neuen EU-DSGVO-Anforderungen starke Parallelen und Überschneidungen mit der Struktur eines ISMS aufweist. Ein integriertes DIMS erfüllt alle Anforderungen des Datenschutzes und der Informationssicherheit und hat neben methodischem ganzheitlichem Vorgehen auch weitere günstige Auswirkungen auf das Ansehen des gesamten Unternehmens. Zu diesen positiven Effekten zählen u. a.: die nachhaltige, ganzheitliche Risikominimierung; die umfassende Absicherung der Unternehmenswerte; die Überprüfbarkeit durch revisionssichere Dokumentation der Aktivitäten und schließlich auch die Compliance gegenüber Geschäftspartnern, Kunden, Interessenten, Banken und Versicherungen.

Integrierter Datenschutz

Ein DIMS auf Basis der EU-DSGVO und der ISO 27001 oder/und IT-Grundschutz, etabliert anerkannte Verfahren, mit welchen methodisch Prozesse und Richtlinien in einem Unternehmen eingeführt werden, die es ermöglichen, die Risiken zu erkennen und einschließlich aller technischen und organisatorischen Maßnahmen zu steuern, zu kontrollieren und permanent zu verbessern (Plan-Do-Check-Act-Kreislauf bei ISMS, Abbildung 2).

Die neuen Anforderungen aus der EU-DSGVO basieren, wie bisher schon in ISMS, auf Geschäftsprozessen und IT-Systemen. Neu im Datenschutz geforderte Aspekte, wie Datensicherheit und IT-Sicherheit sind bereits Bestandteile von ISMS. Ein DIMS bietet darüber hinaus den Vorteil, alle Informationen zu betrachten, unabhängig davon, ob diese Daten in Papierform oder digital vorliegen und ob sie personenbezogen sind oder nicht.

DSGVO-Vorgaben, wie die Schutzbedarfsanalyse und die Risikobeurteilung, einschließlich der daraus abgeleiteten Maßnahmen zur Risikobegegnung im Datenschutz, lassen sich in einem DIMS methodisch integrieren (Abbildung 3). Die Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von IT-Systemen und -Diensten in Bezug auf die Datenverarbeitung wird in einem DIMS ähnlich wie bei einem ISMS umgesetzt. Ebenso kann die Reifegradbestimmung (Ist-/Soll-Vergleich) der vorhandenen Datenschutzaktivitäten analog dem Vorgehen bei ISMS realisiert werden.

Die EU-DSGVO verpflichtet neben der Etablierung neuer Prozesse und Strukturen auch zu einer erweiterten Dokumentation, wie z. B. zum Führen eines Verzeichnisses von Verarbeitungstätigkeiten. Die Weisung bei Auftragsverarbeitung, mit allen AV-Verträgen und den Dienstleistern je Geschäftsprozess, muss dokumentiert und Datenschutzvorfälle müssen rechtzeitig gemeldet werden. Die komplette und revisionssichere Dokumentation aller Datenschutz- und Informationssicherheitsaktivitäten ist deshalb immer auch ein Bestandteil eines nachhaltigen DIMS.

Fazit

Aus den genannten Gründen ist es in jedem Fall für alle Unternehmen sinnvoll, den Datenschutz und die Informationssicherheit nicht unabhängig voneinander zu betreiben. Leider zeigt die Praxis, dass sich kleinere Unternehmen häufig von der Komplexität der Anforderungen überfordert sehen. An dieser Stelle sei darauf hingewiesen, dass Softwarelösungen für jede Unternehmensgröße angeboten werden, die ein integriertes Vorgehen DIMS zu ISMS und EU-DSGVO ermöglichen, unterstützen und deutlich vereinfachen. Mit MS-Excel oder anderen Bordmitteln lässt sich dieses komplexe Thema nicht mehr lösen. Geeignete Softwarelösungen bieten hier die bessere Alternative, helfen Probleme vermeiden und nicht zuletzt Kosten sparen.

Ellen Wüpper
WMC Wüpper Management Consulting GmbH

Security für die ganze Fabrik

Wirksame Sicherheitskonzepte sollten die gesamte Produktionskette abdecken

Weltweite Datenerfassung und -vernetzung, M2M-Kommunikation und vorausschauende Wartung – die Digitalisierung schreitet unaufhaltsam voran. Nur wer alle Zusammenhänge der industriellen Kommunikation im Blick hat, kann die Bedrohungslage richtig einschätzen und effizient reagieren.

Zu den Sicherheitsrisiken im Unternehmen gehören neben Online-Verbindungen auch mobile Speicher wie USB-Sticks und, nicht zu vernachlässigen, der Anwender als fehlerbehaftetes Individuum. Für eine breite Akzeptanz muss Security-Technologie einfach in der Anwendung sein und dem Nutzer keinen oder möglichst wenig Spielraum für Fehler lassen. Das betrifft sowohl die Administratoren, die industrielle Netzwerke einrichten und betreuen, wie auch den Bediener, Instandhalter oder Servicetechniker als Endbenutzer.

Service-Portale

Bislang war Fernwartung der Hauptgrund für die Internet-Anbindung von Maschinen und Anlagen. Häufig waren sie durch den Betreiber gesteuert nur temporär online. Heute haben wir eine Vielzahl von Teilnehmern, die auf Daten in der Anlage zugreifen möchten: vom Bediener und Instandhalter über das Produktmanagement und die Qualitätssicherung bis hin zur Servicezentrale des Maschinenbauers. Für das Management dieser Zugriffsmöglichkeit haben sich Lösungen bewährt, die auf einem zentralen Remote-Service-Portal basieren. Das Portal dient als intelligente Vermittlungsstelle zwischen den verschiedenen Teilnehmern. Ein hierarchisches Mandantensystem sollte eine getrennte Verwaltung von Anlagen, Kunden und Servicepersonal erlauben – und eine rollenbasierte Rechteverwaltung mit feiner Abstufung bieten.

Sichere Authentifizierung

Viele Anwender verwenden immer noch für mehrere Benutzerkonten das gleiche Passwort. Sicherheitsexperten sehen in dem laxen Umgang mit Benutzernamen und Passwörtern häufig die größten Sicherheitsrisiken. Abhilfe schafft hier die Zwei-Faktor-Authentifizierung (2FA). Damit ist der Schutz gegen unberechtigte Zugriffe wesentlich höher als mit der üblichen Benutzername-Passwort-Kombination. Die 2FA beruht auf zwei unterschiedlichen Erkennungsmerkmalen. Beide muss der Benutzer zur Anmeldung am Portal eingeben.

Eine weitere Möglichkeit, die Vorteile einer 2FA zu nutzen, ist die Verifikation über Google Authenticator. Nach Installation der kostenlosen App auf dem Smartphone oder einem anderen Gerät muss der Benutzer beim ersten Login nur noch einen QR-Code scannen und kann den zweiten Faktor für seine nächste Anmeldung bequem über seine Authenticator App auf dem Gerät erzeugen. Im Vergleich zur 2FA per SMS-Code benötigt der Anwender keine Mobilfunkverbindung und auch kein mobiles Endgerät.

Schutz durch Segmentierung

Ein anderer Weg, die Sicherheit zu erhöhen, ist das Segmentieren des Produktionsnetzwerks in überschaubare logische Einheiten. Das funktioniert z. B. mithilfe von Automation Firewalls, mit denen der Anwender sein Netzwerk strukturieren kann. Die Einrichtung sicherer Zonen entschärft zudem die Update-Problematik. Manche Software ist nur bis zu einem bestimmten Service-Pack freigegeben, sodass der Anwender gar keine Möglichkeit hat, das System aktuell zu halten. Vor solchen Systemen kann quasi als Türsteher eine Automation Firewall geschaltet werden, die nur vorher festgelegte Verbindungen und Dienste zulässt.

Zweckmäßig ist auch ein Bridge-Modus. Er dient zur Anbindung neuer Teilnehmer an bestehende Netzwerke, ohne dass am Bestand Änderungen erforderlich sind. Zur Konditionierung des Datenverkehrs sollte die Automation Firewall auf Grundlage der Ursprungs- und Ziel-MAC/IP-Adressen sowie der Ports den zulässigen sowie den verbotenen Datentransfer filtern können. Über einen integrierten Lernmodus erlaubt die Firewall eine unbeschränkte Kommunikation und zeichnet alle Verbindungen auf. Der Anwender entscheidet anschließend anhand der erfassten Pakettabelle, welche Verbindungen unter den IP-Geräten zulässig und welche unerwünscht sind und deshalb gesperrt werden.

Security auf SPS-Ebene

Die weit verbreiteten S7-300- und 400-Steuerungen bieten selbst keine Schutzmechanismen gegen das Eindringen von Viren und Malware. Klassische Methoden von Virenscannern mit Mustererkennung funktionieren hier nicht. Eine entsprechende Security-Box arbeitet daher nach dem Prinzip der Positivliste. Im ersten Schritt wird ein sogenanntes Referenz-Backup erstellt. Hier werden der komplette Programmspeicher (OB, FC, FB, DB, SFC, SFB, SDB), die Bestellnummer und die Seriennummer aus der SPS ausgelesen und im Speicher abgelegt. Anhand dieser Referenzdaten überwacht das Gerät den statischen Speicherbereich der verbundenen Steuerungen kontinuierlich. Bei Änderungen der Programmdaten, etwa durch Schadsoftware wie Stuxnet, wird der Verantwortliche je nach Einstellung per E-Mail oder SMS alarmiert oder es wird ein digitaler Ausgang an der Security-Box gesetzt, der eine Warnleuchte oder Sirene aktiviert. Manipulationen durch Malware und Viren werden erkannt und signalisiert, bevor ein Schaden entsteht.

Fazit

Industrielle Anlagen sind einem breiten Spektrum an Bedrohungen ausgesetzt. Die Security-Konzepte müssen entsprechend umfangreich ausfallen und alle vorstellbaren Szenarien abdecken. Security ist jedoch kein Produkt, das man einfach kauft – sondern ein Prozess, der von den Verantwortlichen fortlaufend weiterentwickelt und an neue Risiken und Bedrohungen angepasst werden muss.

Siegfried Müller
Geschäftsführer, MB Connect Line

Datenschutz in der Cloud

Auch beim Cloud Computing gelten ab Mai 2018 neue Regeln

Angesichts der Anforderungen der EU-Datenschutz-Grundverordnung gilt es, auch den Cloud-Datenschutz kritisch zu überprüfen. Was ändert sich? Wie werden etwa Datenübermittlungen in Drittstaaten geregelt? Welche Möglichkeiten der Cloud-Zertifizierung existieren? Und worauf können Nutzer und Unternehmen setzen?

Vieles wird bleiben, es wird sich jedoch auch vieles ändern. Zu den aus dem Bundesdatenschutzgesetz (BDSG) bekannten Vorgaben gehören etwa die Datenschutzprinzipien Datensparsamkeit und -vermeidung, Verbot mit Erlaubnisvorbehalt, Zweckbindung sowie die Transparenz der verarbeiteten Daten. Wie bisher auch, muss es also mit Wirksamkeit der EU-Datenschutz-Grundverordnung (DSGVO) eine rechtliche Basis für die Verarbeitung von Daten geben. Weiter sollen ausschließlich Daten erhoben werden, die tatsächlich erforderlich sind. Daten werden exklusiv für den Erhebungszweck verarbeitet, falls eine Änderung des Zwecks nicht explizit gestattet wurde. Betroffene Personen haben zudem einige Informationsrechte, die Auskunft darüber erlauben, was mit den Daten konkret geschieht.

Auch die Datensicherheit ist von grundlegender Relevanz. Die DSGVO fordert, dass neben dem Cloud-Nutzer als Auftraggeber auch der Cloud-Anbieter Schutzmaßnahmen zu ergreifen hat. Diese Maßnahmen müssen den aktuellen Stand der Technik berücksichtigen, außerdem müssen Implementierungskosten, die Art, die Umstände sowie der Datenverarbeitungszweck und etwaige Risiken abgewogen werden.

Cloud-Nutzer sind Auftraggeber

Es existiert eine klare Rollenverteilung: Der Cloud-Nutzer ist der Auftraggeber, der Cloud-Anbieter hingegen der Auftragsverarbeiter. Art. 28 Abs. 1 DSGVO erklärt, der Auftraggeber ist dazu verpflichtet, Cloud-Anbieter zu beauftragen, die „hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet."

Das heißt: Der Nutzer ist in der Pflicht, das Datenschutzniveau sowie die Datensicherheit des gewählten Cloud-Anbieters zu prüfen. Dieser Check umfasst auch die Frage nach etwaigen Subunternehmen oder nach Datenübermittlungen in Drittstaaten. Um die neuen europäischen Datenschutzrichtlinien einzuhalten, bleibt oft nur der Weg zu einem europäischen Cloud-Anbieter. Jedoch lohnt auch der Blick auf Zertifizierungen.

Cloud-Zertifizierungen

Um Cloud-Nutzern einen besseren Überblick liefern zu können, betrachtet der Gesetzgeber Zertifizierungen als eine gute Möglichkeit. Bislang hatte der Cloud-Nutzer als verantwortliche Stelle größte Schwierigkeiten, die oben genannten Punkte klären zu können. Mit der DSGVO erhält er neue Instrumente zur Bewertung von Cloud-Anbietern. Nachweisen lassen sich technisch-organisatorische Maßnahmen des Cloud-Anbieters durch das Einhalten geeigneter und genehmigter Verhaltensregeln (Code of Conduct) oder aber durch Zertifizierung nach DSGVO.

WAS SOLLTEN CLOUD-NUTZER JETZT TUN?

Unternehmen, die auf Cloud Computing setzen, können sich schon jetzt auf die EU-DSGVO vorbereiten, indem sie die folgenden Punkte abarbeiten:

- Überblick verschaffen: Zunächst ist ein Überblick über die Unternehmensdaten notwendig. Rechtskonform funktioniert dies mit einem Verfahrensverzeichnis, in dem sämtliche Verarbeitungsprozesse aller Daten dokumentiert werden.
- Abstimmen: Anschließend wird die eigene Datenverarbeitung mit der des Cloud-Anbieters verglichen. Stimmen die Verarbeitungsarten sowie die Sicherheitsstandards überein oder existieren große Lücken?
- Schulen: Datensicherheit geht mit Awareness einher. Mitarbeiter sind zu schulen, außerdem sind Verhaltensregeln festzulegen. Das beginnt bei den Zugriffsrechten, die gewissenhaft verwaltet sein wollen, und schließt auch das Sensibilisieren der Mitarbeiter und das Festlegen von Verhaltensregeln ein.

Beliebige Cloud-Zertifizierungen oder Verhaltensregeln kommen hier nicht in Frage. Die Aufsichtsbehörde bzw. der Europäische Datenschutzausschuss genehmigen und veröffentlichen solche Verhaltensregeln. Ein Register erlaubt den Einblick in eben diese vorgeschriebenen Verhaltensregeln. Verarbeitungsvorgänge hingegen lassen sich über einen Nachweis zur datenschutzkonformen Verarbeitung zertifizieren. Neben den Aufsichtsbehörden sind dafür akkreditierte Stellen verantwortlich. Nicht jede Zertifizierung garantiert jedoch die gewünschte rechtliche Wirkung, denn die Akkreditierung muss gemäß Art. 43 DSGVO erfolgen.

Anbieter tragen Mitverantwortung

Kommt es zu Datenpannen, die der Cloud-Anbieter zu verantworten hat, haftet er laut EU-Datenschutz ebenfalls. Dies ist beispielsweise dann so, wenn ein notwendiges Sicherheitsupdate verpasst wurde. Im Falle einer Datenschutzverletzung kann die Meldepflicht deshalb nicht nur beim Cloud-Nutzer liegen. Cloud-Anbieter müssen die Nutzer laut Gesetz „unverzüglich" benachrichtigen, wenn der Schutz der personenbezogenen Daten in Gefahr ist. Nutzer haben eine Meldefrist von 72 Stunden, der sie jedoch nur dann nachkommen können, wenn der Anbieter sie rechtzeitig informiert.

Der Cloud-Anbieter garantiert also für Datenschutz und -sicherheit, der Cloud-Nutzer hat dies zu überprüfen. Neben regelmäßigen Audits sind auch folgende vertragliche Zusicherungen relevant: Werden personenbezogene Daten verschlüsselt und pseudonymisiert? Sind Vertraulichkeit, Integrität und Verfügbarkeit der Daten genauso sichergestellt wie die Belastbarkeit von Systemen und Diensten? Sind personenbezogene Daten verfügbar und nach technischen oder physischen Zwischenfällen rasch wiederherstellbar? Werden Verfahren regelmäßig überprüft, bewertet und in der Wirksamkeit evaluiert, um die Sicherheit der Datenverarbeitung zu gewährleisten?

Datenmigration

Beim Cloud Computing besteht häufig ein Problem mit der zum Cloud-Anbieter entstehenden Abhängigkeit. Diese Anbieterabhängigkeit könnte mit der DSGVO gemindert werden: Mit dem neuen „Recht auf Datenübertragbarkeit“ können Nutzer ihren Anspruch geltend machen, ihre Daten in marktüblichem, maschinenlesbarem Format zu bekommen. Die DSGVO sieht also vor, dass es Cloud-Nutzern einfacher gemacht wird, eigene Daten zu einem anderen Anbieter mitzunehmen.

Auch die Frage nach der Datenübermittlung in Drittstaaten ist sehr wichtig. Die DSGVO stellt die Voraussetzung, dass ein „angemessenes Schutzniveau“ bestehen muss. Alternativ übermittelt ein Verantwortlicher die personenbezogenen Daten nur dann, wenn wirksame Rechtsbefehle, durchsetzbare Rechte sowie geeignete Garantien vorgesehen sind. Dies können unternehmensinterne Datenschutzvorschriften (sogenannte „Binding Corporate Rules“) sein oder aber Standarddatenschutzklauseln, wie sie die Kommission oder die zuständige Aufsichtsbehörde annimmt.

Möchten ausländische Anbieter Cloud-Services innerhalb der EU anbieten, gilt das sogenannte Marktortprinzip. Dies besagt, dass EU-externe Serviceprovider die Vorgaben der DSGVO genauso beachten müssen wie Unternehmen aus der EU selbst. Wird diesem Prinzip nicht gefolgt, erhalten Nicht-EU-Anbieter keinen Zugang zum europäischen Markt. Neu ist im Übrigen der sogenannte One-Stop-Shop. Dieser Mechanismus klärt, welche Aufsichtsbehörde beim grenzüberschreitenden Datenverkehr überhaupt zuständig ist. Grundsätzlich gilt, dass die Aufsichtsbehörde am Hauptsitz eines Unternehmens zuständig ist, sodass es einen zentralen Ansprechpartner gibt.

Löschpflichten

Mit der EU-Datenschutz-Grundverordnung werden insbesondere Betroffenenrechte gestärkt. Aus dem „Recht auf Vergessenwerden“ gestalten sich komplexe Löschpflichten: Neben dem Löschen der personenbezogenen Daten selbst müssen auch die Links auf die entsprechenden Daten sowie Datenkopien entfernt werden. Im Übrigen ist der Cloud-Anbieter dazu verpflichtet, die Nutzerdaten umgehend zu löschen, wenn der Vertrag gekündigt wird.

Wettbewerbsvorteile sichern

Bis zur Einführung der DSGVO am 25.05.2018 gibt es noch viel zu tun. Etliche Unternehmen sehen zwar derzeit mehr Herausforderungen als Chancen, doch langfristig kann das Einhalten des Datenschutzes jedem Unternehmen einen Wettbewerbsvorteil verschaffen, indem man sich von der Konkurrenz abhebt. Auch wenn die DSGVO fürs Cloud Computing mehr Arbeit bedeutet, sollten Unternehmen rechtzeitig – nämlich spätestens jetzt – mit der Umsetzung der Neuregelungen beginnen. Dann steht einem rechtssicheren Beginn der neuen Datenschutz-Ära nichts mehr im Wege.

Patrycja Tulinska
Leitung Marketing und Training, PSW GROUP

Impressum
Themenbeilage Sicherheit & Datenschutz

Redaktion just 4 business GmbH
Telefon: 08061 34811100, Fax: 08061 34811109,
E-Mail: tj@just4business.de

Verantwortliche Redakteure:
Thomas Jannot (v.i.S.d.P.), Ralph Novak, Martin Fuhrmann (Redaktion), Rudolph Schuster (Lektorat)

Autoren dieser Ausgabe:
Stefan Cink, Sascha Dubbel, Detlef Hühnlein, Dr. Holger Mühlbauer, Siegfried Müller, Patrycja Tulinska, Ellen Wüpper

DTP-Produktion:
Madlen Grunert, Matthias Timm, Hinstorff Media, Rostock

Korrektorat:
Sylvia Raschke-Eckerle, Hinstorff Media, Rostock

Titelbild:
© shutterstock, Sentavio

Verlag
Heise Medien GmbH & Co. KG,
Postfach 61 04 07, 30604 Hannover; Karl-Wiechert-Allee 10, 30625 Hannover;
Telefon: 0511 5352-0, Telefax: 0511 5352-129

Geschäftsführer:
Ansgar Heise, Dr. Alfons Schräder

Mitglieder der Geschäftsleitung:
Beate Gerold, Jörg Mühle

Verlagsleiter:
Dr. Alfons Schräder

Anzeigenleitung (verantwortlich für den Anzeigenteil):
Michael Hanke (-167), E-Mail: michael.hanke@heise.de, www.heise.de/mediadaten/ix

Leiter Vetrieb und Marketing:
André Lux

Druck:
Dierichs Druck + Media GmbH & Co. KG, Frankfurter Straße 168, 34121 Kassel

Die Inserenten

Die hier abgedruckten Seitenzahlen sind nicht verbindlich.
Redaktionelle Gründe können Änderungen erforderlich machen.

WIR TRINKEN DEN KAFFEE #000000.

iX. WIR VERSTEHEN UNS.

Jetzt Mini-Abo testen:
3 Hefte + iX-Kaffeebecher nur 13,50 €
www.iX.de/test

Sie mögen Ihren Kaffee wie Ihr IT-Magazin: stark, gehaltvoll und schwarz auf weiß!
Die iX liefert Ihnen die Informationen, die Sie brauchen: fundiert, praxisnah und unabhängig.
Testen Sie 3 Ausgaben iX im Mini-Abo + iX-Kaffeebecher für 13,50 Euro und erfahren Sie, wie es ist, der Entwicklung einen Schritt voraus zu sein.
Bestellen Sie online oder telefonisch unter +49 (0)541 800 09 120.