Cybersecurity Trends 2018

Cybersecurity in einer zunehmend digitalen Welt.

www.tuv.com/informationssicherheit

TÜVRheinland®
Genau. Richtig.

Inhalt

Liebe Leserinnen, liebe Leser,

in den vergangenen Monaten ist ein dramatischer Anstieg des Volumens, der Komplexität und der Raffinesse von Cyber-Angriffen zu verzeichnen. Es war ein Jahr, in dem nichts sicher schien und in dem Cyber-Attacken auch die Verwundbarkeit unserer persönlichen Daten deutlich machten. Eine Entwicklung, auf die wir in unseren Cybersecurity Trends 2017 bereits aufmerksam machten.

Im April tauchten über die bisher anonyme Gruppe „Shadow Brokers" eine Reihe von Hacking-Tools auf, die im Verdacht stehen, der US National Security Agency zu gehören. Im Juli stahlen Angreifer die persönlichen Daten von 145 Millionen Menschen von Equifax. WannaCry und NotPetya Ransomware folgten und verbreiteten sich in über 150 Ländern, was zu empfohlenen Lösegeldzahlungen von mehr als 2 Milliarden US-Dollar im Jahr 2017 führte. FedEx schrieb allein dem NotPetya-Angriff einen Verlust von 300 Millionen US-Dollar zu. Diese beiden, inzwischen berüchtigten, Ransomware Angriffe nutzten die von Shadow Brokers durchgesickerte Schwachstelle aus.

In jüngster Zeit hat die Enthüllung von Nutzerprofilen von Facebook die weitreichenden Risiken aufgezeigt, die sich aus dem Missbrauch unserer persönlichsten Informationen ergeben. Es scheint inzwischen einfacher denn je, Malware oder Ransomware zu erstellen und damit auch Zugang zu persönlichen Daten zu erhalten. Während Unternehmen ihre digitale Transformation fortsetzen und wir „intelligente" Geräte in unser tägliches Leben integrieren, stellt Cyber-Kriminalität zunehmend eine große Bedrohung für Wirtschaft und Gesellschaft dar.

In den Cybersecurity Trends 2018 stellen wir Ihnen vor, wo wir Bedrohungen aber auch Chancen der digitalen Transformation sehen. Wir diskutieren die Auswirkungen unserer zunehmend vernetzten Welt – welchen Einfluss globale Regulierungen nehmen und die Notwendigkeit, Vertrauen in Cybersecurity zu schaffen. Erfahren Sie, wie Sie sich vor „intelligenten" Cyber-Angriffen schützen und was Sie tun können, um die Lücke zwischen dem Fachkräftemangel an Cybersecurity-Experten und der Fülle an schützenswerten Daten zu schließen.

Wir freuen uns, den Dialog mit Ihnen über die spannenden und unumgänglichen Themen in der IT-Sicherheit fortzusetzen.

BJÖRN HAAN, GESCHÄFTSFÜHRER IM GESCHÄFTSFELD CYBERSECURITY DEUTSCHLAND, TÜV RHEINLAND

Zusammenfassung

Cybersecurity in einer zunehmend digitalen Welt.

Mit welchen Herausforderungen müssen Unternehmen in den nächsten Monaten umgehen, auf welche Bedrohungen sollten sie vorbereitet sein?

TREND 1: DURCH DIE WACHSENDE ANZAHL AN GLOBALEN REGULIERUNGEN IM CYBER-UMFELD STEIGT DER PREIS UM DIE PRIVATSPHÄRE ZU SCHÜTZEN

Datenschutz ist ein kritischer Aspekt in einer immer digitaler werdenden Welt. Der 25. Mai 2018 stellt einen entscheidenden Wendepunkt für den Datenschutz in Europa dar. Dieses Datum markiert das Ende des Übergangszeitraums für die Datenschutz-Grundverordnung (DSGVO) der EU, da diese ab diesem Tag rechtsverbindlich gilt. Sie bedeutet einen grundlegenden Wandel bei der Daten-Governance und der Art, wie Informationen von Unternehmen geschützt werden, die personenbezogene Daten von EU-Bürgern verarbeiten. Die Verordnung ist der Beginn einer wachsenden weltweiten Regulierung im Bereich Datenschutz. Verstöße gegen diese können mit Strafen in Höhe von bis zu 4% des globalen Umsatzes belegt werden – eine enorme Summe, die nicht außer Acht gelassen werden darf. Stellen Sie sich darauf ein, dass die EU-Kommission Verstöße gegen die DSGVO durch große globale Unternehmen konsequent verfolgen wird.

TREND 2: DAS INTERNET OF THINGS TREIBT DAS ZUSAMMENSPIEL VON SICHERHEIT, CYBERSECURITY UND DATENSCHUTZ VORAN

Im Jahr 2016 hat die Verwendung der Malware Mirai gezeigt, dass IoT-Geräte ein schlagkräftiges und gefährliches Botnet bilden können. Die Time-to-Market-Anforderungen bei der Produktentwicklung und die eingeschränkte technische Performance von IoT-Geräten sorgen heute dafür, dass diese Geräte kritische Schwachstellen aufweisen, die einfach ausgenutzt werden können. Die Auswirkungen von Datenverletzungen gehen heute weit über eine einfache Datenmonetarisierung hinaus und umfassen auch physische Bedrohungen für Gesundheit und Sicherheit, da Geräte und Systeme direkt mit offenen Netzwerken verbunden sind. Es ist ein offenes Geheimnis, dass es um die IoT-Sicherheit nicht gut bestellt ist. Und wenn man bedenkt, dass wir bis 2022 laut Schätzungen unsere Wohnungen und Häuser mit über 500 solcher Geräte teilen, wird klar, dass sich die Risiken für Sicherheit, Cybersecurity und Datenschutz stark erhöhen werden.

TREND 3: OPERATIONAL TECHNOLOGY ALS ANGRIFFSPUNKT FÜR CYBER-ATTACKEN

Das Industrial Internet sorgt bereits für eine Transformation der globalen Industrie und Infrastruktur und verspricht mehr Effizienz, Produktivität und Sicherheit. Um im Wettbewerb zu bestehen, werden Prozessleittechnikgeräte mit der Online-Welt verbunden, wodurch oftmals unbeabsichtigt Komponenten, die Schwachstellen aufweisen, Cyber-Angriffen ausgesetzt werden. Fertigungsanlagen sind ebenfalls ein Angriffsziel, um an geistiges Eigentum, Geschäftsgeheimnisse und technische Informationen zu gelangen. Hinter Angriffen auf die öffentliche Infrastruktur stehen dagegen finanzielle Gründe, Hacktivismus und die Unzufriedenheit mit staatlichen Stellen. Die Angst vor einem „Worst-Case-Szenario", bei dem Angreifer einen Zusammenbruch von Systemen auslösen, die das Fundament der Gesellschaft bilden, war ein Thema beim diesjährigen Weltwirtschaftsforum. Industrielle Systeme sind besonders anfällig gegen Angriffe auf die Lieferkette. Das haben auch kriminelle Angreifer erkannt und begonnen, diese Systeme ins Visier zu nehmen.

TREND 4: WENN ABWEHRMECHANISMEN FÜR CYBER-ANGRIFFE VORHANDEN SIND, VERLAGERT SICH DIE FOKUSSIERUNG AUF DIE ERKENNUNG VON BEDROHUNGEN UND ANGEMESSENE REAKTIONEN

Angriffe der letzten Zeit zeigen, dass im Kampf gegen erfahrene und beharrliche Cyber-Kriminelle Verhinderungsmechanismen allein nicht ausreichen. Heute dauert es im Schnitt 191 Tage, bis ein Unternehmen ein Datenleck erkennt. Und je länger es dauert, eine Bedrohung zu erkennen und darauf zu reagieren, umso größer sind der finanzielle Schaden und der Reputationsverlust, den das Unternehmen durch den Vorfall erleidet. Durch den enormen Anstieg erfasster sicherheitsrelevanter Daten, die Einschränkungen von aktuellen Technologien, die ineffiziente Nutzung von vorhandenen Bedrohungsinformationen (Threat Intelligence), die fehlende Überwachung von IoT-Geräten und den Fachkräftemangel an Cybersecurity-Experten entstehen in den Unternehmen teure Verweildauern.

TREND 5: ZUNEHMENDE NUTZUNG VON KÜNSTLICHER INTELLIGENZ FÜR CYBER-ATTACKEN UND -ABWEHR

Auf ihrem Weg der digitalen Transformation werden Unternehmen in steigendem Maße zum Ziel für komplexe und hartnäckige Cyber-Attacken. Malware wird immer smarter. Sie kann sich „intelligent" anpassen und traditionelle Erkennungs- und Beseitigungsroutinen umgehen.

Angesichts des globalen Mangels an Cybersecurity-Spezialisten sind die Unternehmen dabei, das Cyber-Wettrüsten zu verlieren. Die Menge an Sicherheitsdaten überschreitet bei weitem die Kapazitäten für ihre effiziente Nutzung. Das führt zu einer steigenden Anzahl von KI-fähigen Cybersecurity-Anwendungsfällen: Beschleunigung der Erkennung und Bekämpfung von Sicherheitsvorfällen, bessere Identifizierung und Vermittlung von Risiken gegenüber den Fachabteilungen und die Bereitstellung einer einheitlichen Sicht auf den Sicherheitsstatus innerhalb der gesamten Organisation.

TREND 6: ZERTIFIZIERUNGEN WERDEN WICHTIG, UM DAS VERTRAUEN IN CYBERSECURITY ZU STÄRKEN

Es herrscht weitgehend Einigkeit darüber, dass Cybersecurity und Datenschutz integrale Bestandteile einer digitalen und vernetzten Welt sind. Aber: Wie lässt sich das Schutzniveau eines Unternehmens objektiv einschätzen? Die Bedenken, ob und inwieweit Cybersecurity tatsächlich umgesetzt wird, nehmen zu. Dies führt dazu, dass bestehende und neue Standards, die Cybersecurity-Strategien international vergleichbar machen, immer stärker an Relevanz gewinnen. Für CISOs und Produkthersteller sind Zertifizierungen wichtig, um nachzuweisen, dass sie getan haben, was sie versprochen haben. Die Zertifizierungsverfahren für die Bestätigung der IT-Sicherheit von Produkten konzentrieren sich heute jedoch vor allem auf kritische Infrastrukturen und öffentliche Hand. Wo bleiben die Hersteller von Verbraucherprodukten?

TREND 7: ABLÖSUNG DER KENNWÖRTER DURCH BIOMETRISCHE AUTHENTIFIZIERUNG

Unser digitales Leben wird durch ein komplexes Netz aus Online-Apps bestimmt, unsere digitale Identität durch Benutzernamen und Passwörter geschützt. Um den Schutz hinter diesen Apps zu steigern, wird empfohlen, schwer zu erratende und komplexe Kennwörter zu verwenden und diese regelmäßig zu ändern. In der Praxis geschieht das aber nur selten. Mit der exponentiellen Zunahme der Rechenleistung und dem einfachen Zugang über die Cloud können Kennwörter in einer immer kürzeren Zeit geknackt werden. Was 2000 noch fast 4 Jahre gedauert hat, ist heute in 2 Monaten erledigt. Wenn man bedenkt, dass Kennwörter häufig gestohlen, gehackt und gehandelt werden, wird klar, dass sie noch nie offener verfügbar waren als heute. Aus diesem Grund begegnen wir heute bei Mobiltelefonen, Tablets und Laptops und auch bei physischen sowie Online-Services vermehrt der biometrischen Authentifizierung (Gesicht, Fingerabdruck, Iris und Sprache).

TREND 8: AUSGEWÄHLTE BRANCHEN IM VISIER DER ANGREIFER: GESUNDHEITSWESEN, FINANZDIENSTLEISTUNGEN UND ENERGIEVERSORGUNG

Der Großteil der Cyberangriffe wird von Kriminellen aus finanziellen Motiven begangen. Der Wert von Daten im Darknet richtet sich nach der Nachfrage, ihrer Verfügbarkeit, ihrer Vollständigkeit und den Möglichkeiten für deren Nutzung. Daher sind persönliche Informationen aus dem Gesundheits- und Finanzsektor besonders gefragt. Krankenakten kosten, je nachdem, wie vollständig sie sind, zwischen 1 bis 1000 US-Dollar. Kreditkartendaten werden für 5 bis 30 US-Dollar verkauft, wenn die benötigten Informationen für ihre Nutzung mitgeliefert werden. Andere Cyber-Angriffe haben eher politische oder nationalstaatliche Motive. Im Jahr 2018 besteht hier ein erhöhtes Risiko für Störungen von kritischen Services durch Angriffe auf den Energiesektor. Beleg dafür sind die Berichte der jüngsten Zeit über die von Russland initiierten Cyber-Attacken auf das US-Stromnetz, die vermutlich bereits seit einem oder mehreren Jahren ausgeführt werden.

Trend 1: Durch die wachsende Anzahl an globalen Regulierungen im Cyber-Umfeld steigt der Preis um die Privatsphäre zu schützen

Datenschutz ist ein kritischer Aspekt in einer immer digitaler werdenden Welt. Der 25. Mai 2018 stellt einen entscheidenden Wendepunkt für den Datenschutz in Europa dar.
Dieses Datum markiert das Ende des Übergangszeitraums für die Datenschutz-Grundverordnung (DSGVO) der EU, da diese ab diesem Tag rechtsverbindlich gilt. Sie bedeutet einen grundlegenden Wandel bei der Daten-Governance und der Art, wie Informationen von Unternehmen geschützt werden, die personenbezogene Daten von EU-Bürgern verarbeiten. Die Verordnung ist der Beginn einer wachsenden weltweiten Regulierung im Bereich Datenschutz. Verstöße gegen diese können mit Strafen in Höhe von bis zu 4% des globalen Umsatzes belegt werden[1] — eine enorme Summe, die nicht außer Acht gelassen werden darf. Stellen Sie sich darauf ein, dass die EU-Kommission Verstöße gegen die DSGVO durch große globale Unternehmen konsequent verfolgen wird.

1 Europäische Komission, Mai 2017

„Die DSGVO ist eine Herausforderung für Unternehmen, gleichzeitig aber auch eine Chance, die Daten-Governance und zugehörige Schutzmaßnahmen zu optimieren, um das Risiko von Datenschutzpannen zu reduzieren."

MICHAEL SILVAN,
Chief Technology Officer (CTO), Center of Excellence Risk & Compliance, TÜV Rheinland

DATENSCHUTZ IST EIN KRITISCHER ASPEKT IN EINER IMMER DIGITALER WERDENDEN WELT

Parallel zur fortschreitenden digitalen Transformation und Vernetzung in den Unternehmen häufen sich Cyber-Angriffe und werden immer ausgeklügelter. Cyber-Angriffe der jüngsten Vergangenheit haben die Anfälligkeit von Unternehmen deutlich offengelegt. Die Ransomware WannaCry infizierte innerhalb von weniger als 48 Stunden über 300.000 Computer in zahlreichen Organisationen in verschiedenen Ländern und auf unterschiedlichen Kontinenten. 87 Millionen Facebook-Profile wurden von der Analysefirma Cambridge Analytica abgegriffen. Damit zählt dieser Vorfall zu den folgenschwersten Datenverletzungen in der Geschichte und steht auf einer Stufe mit dem Diebstahl der Finanzdaten von Equifax. Diese Angriffe lassen eine dunkle Zukunft für den Datenschutz erahnen.

DIE DSGVO BEDEUTET EINEN GRUNDLEGENDEN WANDEL BEI DER DATEN-GOVERNANCE UND DER ART, WIE INFORMATIONEN GESCHÜTZT WERDEN SOLLEN

Unternehmen müssen in zunehmendem Maße nachweisen können, dass sie personenbezogene Daten in Übereinstimmung mit den rechtlichen Bestimmungen in diesem neuen Regulierungsumfeld verarbeiten. Mit der DSGVO werden verschiedene Schlüsselkomponenten eingeführt, wie z.B.: Extraterritorialer Anwendungsbereich für EU-Datenschutzrecht, Betroffenenrechte, Pflicht zur Bestellung eines Datenschutzbeauftragten, Transparenzpflichten und Einwilligung, Einschränkungen für Subauftragnehmer, Datenschutz-Folgenabschätzung und Anzeigepflicht bei Verstößen gegen die Datensicherheit. Diese Anforderungen zwingen Unternehmen, ihre Daten-Governance, ihre Systemarchitektur, ihre Dokumentation und ihren Schutz vor Datenverlust zu überdenken.

VERSTÖSSE GEGEN DIE VERORDNUNG KÖNNEN MIT STRAFEN IN HÖHE VON BIS ZU 4% DES GLOBALEN UMSATZES BELEGT WERDEN

Die damit verbundenen geschäftlichen Risiken sind enorm. Bei einem Verstoß sieht die EU Sanktionen in Höhe von bis zu 4 Prozent des Vorjahresumsatzes oder 20 Millionen Euro vor, je nachdem, welche Summe höher ist. Mängel bei der technischen und organisatorischen Datensicherheit, wie beispielsweise veraltete Verschlüsselungsstandards, erhöhen die Wahrscheinlichkeit, dass ein Unternehmen von diesen Strafzahlungen betroffen ist.

VIELE UNTERNEHMEN UNTERSCHÄTZEN DAS AUSMASS SOLCHER ANFORDERUNGEN

Nur wenige Unternehmen werden zum bevorstehenden Stichtag vollständig vorbereitet sein. Die meisten haben das Ausmaß der Anforderungen unterschätzt und sind noch immer mit der Entwicklung eines Plans beschäftigt, um die DSGVO umzusetzen. Manche haben beschlossen, gar keinen Plan auszuarbeiten und die fehlende Konformität einfach als ein weiteres operatives Risiko hinzunehmen. Wahrscheinlich gehen diese Unternehmen davon aus, dass die EU-Kommission die Verordnung nicht wirklich konsequent umsetzen wird. Andere Unternehmen wiederum sind sich nicht sicher, ob die Verordnung überhaupt auf sie zutrifft. Im Ergebnis lässt sich sagen, dass die Mehrzahl der Unternehmen die Implementierung viel zu spät angeht.

EINE WACHSENDE LISTE VON WELTWEITEN DATENSCHUTZBESTIMMUNGEN

Die DSGVO ist ein führender globaler Trend, da nicht nur die europäischen Regulierungsstellen eine größere Rechenschaftspflicht auf der Management-Ebene fordern. Auch in den USA, in Argentinien, in Brasilien, in der Schweiz, in Afrika, in Indien und in China werden die geltenden Datenschutzbestimmungen überarbeitet. Viele bauen auf ähnliche Konzepte, wie beispielsweise Einwilligungserklärungen von Benutzern und Anzeigepflicht bei Verstößen gegen die Datensicherheit, die Unternehmen verpflichtet, bei Datenschutzverletzungen die zuständigen Behörden und alle betroffenen Datensubjekte zu informieren – ein oftmals kostspieliger Vorgang. Das führt auch zu einer Fragmentierung und zu neuen Marktbarrieren, bedingt durch territoriale Anforderungen für den Datenschutz und grenzüberschreitende Datenflüsse. Für globale Unternehmen wird damit das internationale Geschäft zu einer immer kostspieligeren und komplexeren Herausforderung.

www.tuv.com/datenschutzmanagement

Trend 2: Das Internet of Things treibt das Zusammenspiel von Sicherheit, Cybersecurity und Datenschutz voran

Im Jahr 2016 hat die Verwendung der Malware Mirai gezeigt, dass IoT-Geräte ein schlagkräftiges und gefährliches Botnet bilden können. Die Time-to-Market-Anforderungen bei der Produktentwicklung und die eingeschränkte technische Performance von IoT-Geräten sorgen heute dafür, dass diese Geräte kritische Schwachstellen aufweisen, die einfach ausgenutzt werden können. Die Auswirkungen von Datenverletzungen gehen heute weit über eine einfache Datenmonetarisierung hinaus und umfassen auch physische Bedrohungen für Gesundheit und Sicherheit, da Geräte und Systeme direkt mit offenen Netzwerken verbunden sind. Es ist ein offenes Geheimnis, dass es um die IoT-Sicherheit nicht gut bestellt ist. Und wenn man bedenkt, dass wir bis 2022 laut Schätzungen unsere Wohnungen und Häuser mit über 500 solcher Geräte teilen, wird klar, dass sich die Risiken für Sicherheit, Cybersecurity und Datenschutz stark erhöhen werden.

MIRAI HAT GEZEIGT, DASS IOT-GERÄTE EIN GEFÄHRLICHES BOTNET BILDEN KÖNNEN

Am Freitag, den 21. Oktober 2016 erfolgte um 7 Uhr Ortszeit ein massiver DDoS-Angriff (Distributed Denial of Service) auf Dyn Inc., in dessen Folge große Teile des Internets an der Ostküste der USA ausfielen. Davon betroffen waren Unternehmen wie Twitter, Spotify, Amazon, Netflix, Reddit, The Guardian, CNN und die New York Times. Das Mirai-Botnet bestand vorwiegend aus gehackten IoT-Geräten. Der Angriff war ein Weckruf, der die Anfälligkeit von internetfähigen Geräten gegenüber Cyber-Angriffen deutlich machte.

KOMMERZIELLE UND TECHNISCHE BESCHRÄNKUNGEN MACHEN IOT-GERÄTE ANFÄLLIG FÜR CYBER-ANGRIFFE

Viele IoT-Geräte sind extrem unsicher und setzen Produkthersteller und Kunden dem Risiko einer Cyber-Attacke aus. Das sollte kaum überraschen, da die Hersteller nicht im Cybersecurity-Geschäft tätig sind. Vielmehr stehen sie unter dem steigenden Druck, mit ständigen Innovationen der Konkurrenz voraus zu sein und die eigenen Margen zu schützen. Die Gewährleistung, dass die Geräte leicht produziert werden können, funktional, vernetzt und sicher sind – und gleichzeitig einen niedrigen Stromverbrauch bieten, um so die Akkulaufzeiten zu verlängern – ist eine komplexe technische Herausforderung, die nur mit schwierigen Zugeständnissen bewältigt werden kann.

SCHWACHSTELLEN SIND OFTMALS TIEF IN DER SOFTWARE DES PRODUKTS VERANKERT

Um Zeit und Geld zu sparen, verwenden Software-Entwickler offene Quellcode-Bibliotheken; anstatt das Rad für Basisfunktionen neu zu erfinden. Diese externen Bibliotheken von Drittanbietern können eine Quelle für kritische Sicherheitslücken sein. Ein gutes Beispiel dafür ist die Schwachstelle Devil's Ivy, die kürzlich im gSOAP-Toolkit gefunden wurde, das häufig von Herstellern für die Anbindung ihrer Geräte an das Internet genutzt wird. Es existieren schätzungsweise über eine Millionen Geräte, die anfällig für eine Ausnutzung eines Stapelüberlaufs durch Devil's Ivy sind.

„Erst wenn sich die Hersteller der Bedrohungen und Risiken, die in ihren Geräten lauern, voll und ganz bewusst sind und die entsprechenden Konsequenzen im Hinblick auf ‚Cybersecurity by Design' ziehen, können sie sich auf ihre Produktinnovationen konzentrieren."

UDO SCALLA,
Leiter, Competence Center IoT Privacy, TÜV Rheinland

DIE AUSWIRKUNGEN VON DATENVERLETZUNGEN GEHEN HEUTE WEIT ÜBER EINE EINFACHE DATEN-MONETARISIERUNG HINAUS

Wir leben zunehmend in einem integrierten digitalen System, das unsere Lebensqualität verbessern soll. Die Verbraucher besitzen jedoch häufig nicht das nötige Wissen, um sich vor diesen anfälligen IoT-Ökosystemen zu schützen. Produkthersteller, die Cybersecurity- und Datenschutzaspekte vernachlässigen, liefern ihre Kunden Cyber-Kriminellen aus. In einer Welt der cyber-physischen Dinge ist dies nicht nur eine Bedrohung für die persönlichen Daten, sondern auch für die persönliche Gesundheit und Sicherheit.

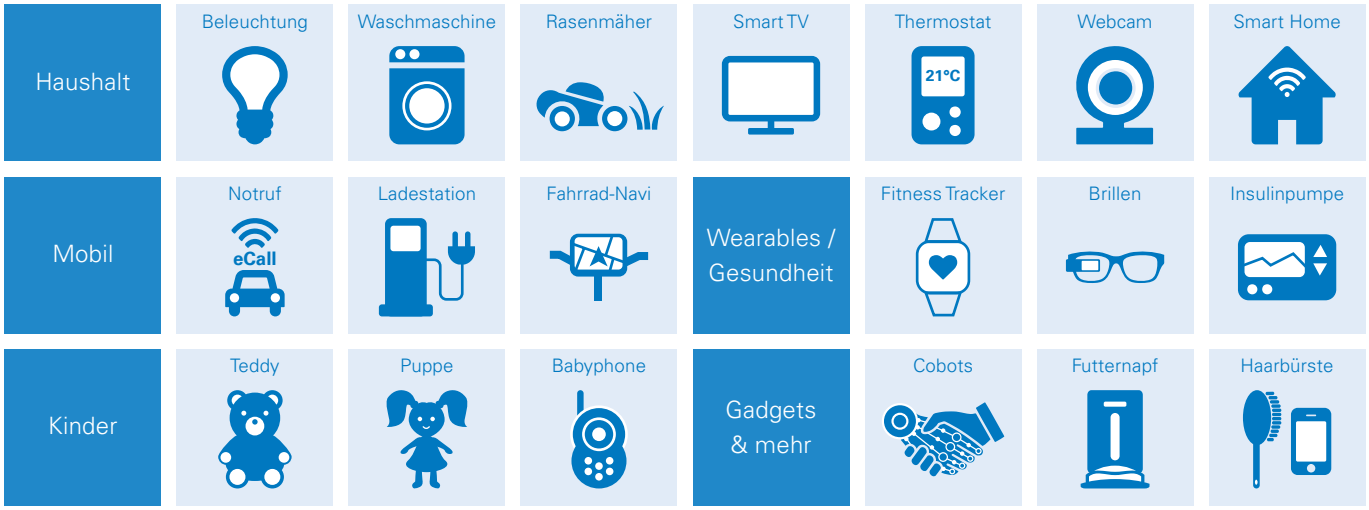
HACKING-ANFÄLLIGE MEDIZINISCHE GERÄTE GEFÄHRDEN DAS LEBEN VON PATIENTEN

Im letzten Jahr hat die US-amerikanische Lebens- und Arzneimittelbehörde FDA bestätigt, dass die implantierbaren Herzgeräte von St. Jude Medical, einschließlich Herzschrittmacher und Defibrillatoren, anfällig gegen Cyber-Angriffe sind. Demnach können Angreifer die Kontrolle über die Geräte übernehmen, indem sie auf den Transmitter zugreifen, der die Gerätedaten ausliest und an die Ärzte sendet. Ein anderes Beispiel ist ein Herzmonitor für Babys, bei dem ein unverschlüsseltes Wi-Fi-Netz zwischen dem Monitor und dem Sensor ein Einfallstor für eine Cyber-Attacke öffnet. Angreifer können die Kontrolle über das System übernehmen, ein fremdes Baby überwachen und alle Alarme unterbinden, die an die Eltern gesendet werden sollen.[2]

HACKING-ANFÄLLIGE AUTOS ÜBERLASSEN DAS SCHICKSAL DER INSASSEN POTENZIELLEN ANGREIFERN

Im Jahr 2015 gelang es einem Forscherteam, die vollständige Kontrolle über einen Jeep-SUV zu erhalten. Dabei wurde eine Schwachstelle der Firmware-Update-Funktion genutzt, um den CAN-Bus des Fahrzeugs über eine Mobilfunkverbindung zu kapern. Die Forscher konnten das Fahrzeug per Fernzugriff beschleunigen, abbremsen und sogar von der Straße lenken. Und erst kürzlich wurde über eine neue Schwachstelle im CAN-Protokoll berichtet, die nicht nur universal ist, sondern auch unter Umgehung der Anti-Hacking-Mechanismen der Autoindustrie ausgenutzt werden kann.[3] Angreifer können so kritische Sicherheits- und Schutzsysteme wie Airbags, ABS und die Türverriegelung abschalten. Diese Schwachstelle hat ihren Ursprung im Design des CAN-Standard selbst.

Alltägliche Produkte gehen online und werden Teil des Internet of Things



www.tuv.com/iot-privacy

2 The Register, Wi-Fi baby heart monitor may have the worst IoT security of 2016, Oktober 2016
3 Wired, Car hack shut down safety features, August 2017

Trend 3: Operational Technology als Angriffspunkt für Cyber-Attacken

Das Industrial Internet sorgt bereits für eine Transformation der globalen Industrie und Infrastruktur und verspricht mehr Effizienz, Produktivität und Sicherheit. Um im Wettbewerb zu bestehen, werden Prozessleittechnikgeräte mit der Online-Welt verbunden, wodurch oftmals unbeabsichtigt Komponenten, die Schwachstellen aufweisen, Cyber-Angriffen ausgesetzt werden. Fertigungsanlagen sind ebenfalls ein Angriffsziel, um an geistiges Eigentum, Geschäftsgeheimnisse und technische Informationen zu gelangen. Hinter Angriffen auf die öffentliche Infrastruktur stehen dagegen finanzielle Gründe, Hacktivismus und die Unzufriedenheit mit staatlichen Stellen.
Die Angst vor einem „Worst-Case-Szenario", bei dem Angreifer einen Zusammenbruch von Systemen auslösen, die das Fundament der Gesellschaft bilden, war ein Thema beim diesjährigen Weltwirtschaftsforum. Industrielle Systeme sind besonders anfällig gegen Angriffe auf die Lieferkette. Das haben auch kriminelle Angreifer erkannt und begonnen, diese Systeme ins Visier zu nehmen.

DAS INDUSTRIAL INTERNET TRANSFORMIERT DIE GLOBALE INDUSTRIE UND INFRASTRUKTUR

In den letzten 15 Jahren hat das Internet die Geschäftswelt hin zu einer engeren Verbraucherbeziehung gewandelt und informationsbasierte Branchen wie Medien, Einzelhandel und Finanzdienstleistungen demokratisiert. In den kommenden 10 Jahren wird es die physischen Branchen Fertigung, Energieversorgung, Transport und Landwirtschaft umkrempeln. Unter der Bezeichnung „Industrial Internet" wird der Trend zur Integration von Informationsnetzwerken und operativen Technologienetzwerken nie dagewesene Möglichkeiten, aber auch neue Risiken mit sich bringen.

„Risikobewertungen durchzuführen, um sich einen Überblick über die aktuellen Schwachstellen und den Stand der Cybersecurity zu verschaffen – das ist das A und O für Operational Technology."

URMEZ RUSI DAVER,
Leiter, Center of Excellence Industrial Security,
TÜV Rheinland

UM IM WETTBEWERB ZU BESTEHEN, WERDEN GERÄTE MIT DEM INTERNET VERBUNDEN

Seit Jahrzehnten werden in den industriellen Sektoren Messdaten genutzt, um die Produktivität und Wettbewerbsfähigkeit zu verbessern und Energie zu sparen.
Auf der elementarsten Ebene werden aktuelle Daten mit historischen Daten verglichen um zu bestimmen, wie Prozesse ausgeführt werden sollten. Analysen liefern Empfehlungen, Verbesserungen und Warnungen als Unterstützung für die Entscheidungsfindung.[4] Der nächste große Schritt in der industriellen Evolution ist die Erfassung von Messdaten außerhalb der Einrichtung und deren Migration in die Cloud. Auf diese Weise können Informationen von Verarbeitungsgeräten rund um den Globus kombiniert werden, was zu neuen Möglichkeiten und damit zu neuen Wettbewerbsvorteilen führt.

ANGST VOR EINEM „WORST-CASE-SZENARIO" ALS THEMA BEIM WELTWIRTSCHAFTSFORUM

Die Häufigkeit und Komplexität von Cyber-Angriffen steigt rasant an und hat sich in den vergangenen fünf Jahren nahezu verdoppelt. In der Vergangenheit waren industrielle Systeme autonom und nicht mit Unternehmensnetzwerken oder dem Internet verbunden. Doch in einer zunehmend vernetzten industriellen Welt steht Cyber-Kriminellen eine deutlich höhere Anzahl von potenziellen Zielen zur Verfügung. Damit werden auch immer häufiger kritische und strategische Infrastrukturen auf der Welt angegriffen, wie z.B. Regierungsministerien, Bahnbetriebe, Banken, Telekommunikationsunternehmen, Energieversorger, Fertigungsbetriebe und Krankenhäuser. Das schürt die Angst vor einem „Worst-Case-Szenario", bei dem Angreifer die Systeme zum Zusammenbruch bringen, die für das Funktionieren der Gesellschaft essentiell sind.

FERTIGUNGSANLAGEN WERDEN ANGEGRIFFEN, UM AN GESCHÄFTSGEHEIMNISSE ZU GELANGEN

Die Anzahl von Cyber-Attacken steigt und die Fertigungsindustrie gehört zu den am häufigsten angegriffenen Zielen. Etwas mehr als ein Drittel der dokumentierten Cyber-Attacken entfallen auf die Fertigung. Fertigungsunternehmen zählen in fünf von sechs geografischen Regionen zu den drei häufigsten Zielen.[5] Grund dafür ist der harte Wettbewerb in diesem Sektor, in dem geistiges Eigentum Gold wert ist, es aber an Investitionen in Cybersecurity mangelt, da der Fokus mehr auf Produktivität und Effizienz liegt.

ANGRIFFE AUF DIE ÖFFENTLICHE INFRASTRUKTUR HABEN ZERSTÖRERISCHE MOTIVE

Oftmals im Schatten des schieren Ausmaßes der personengebundenen Informationen, die von Cyber-Kriminellen im Unternehmenssektor gestohlen werden, forcieren Cyber-Spionagegruppen ihre Angriffe auf die öffentlichen Infrastrukturen rund um den Globus.[6] Im vergangenen Jahrzehnt haben sich zerstörerische Angriffe auf Organisationen und kritische Infrastrukturen gehäuft. Doch die letzten 18 Monate markierten den bisherigen Höhepunkt dieser Entwicklung. Die Malware „Crash Override" wurde für einen Angriff auf das ukrainische Stromnetz genutzt. Den Angreifern gelang es dabei, die Kontrolle über Leistungs- und Schutzschalter zu erhalten. Bei jüngeren Angriffen gelang ein Eindringen in Atomkraftwerke, um Informationen über Computernetzwerke und Prozessleitsysteme für künftige Attacken zu sammeln.

4 ABB, The Internet of Things, Services and People – A new age of industrial production, 2016
5 Computerweekly, Manufacturing a key target for cyber attacks, August 2017
6 Business Insider Germany, Destructive cyberattacks are only going to get worse, September 2017

Globale Cyber-Bedrohungen für Operational Technology

Cyber-Kriminellen steht eine exponentiell zunehmende Zahl von potenziellen Zielen zur Verfügung, da die Nutzung von Cloud-Diensten nach wie vor Fahrt aufnimmt

2016
Mehr als 4 Milliarden Datensätze geknackt

2016
Zahl der DDoS-Angriffe mit über 100 GBPS um 140% angestiegen

2017
Über 300.000 Computer mit Ransomware befallen

2017
Jedes DDoS-Ziel durchschnittlich 32 Mal innerhalb von drei Monaten getroffen

Systeme des staatlich geregelten Transportsektors sind im Schnitt 1.000 Angriffen im Monat ausgesetzt

2017
Kosten für die Reaktion auf Cyber-Angriffe $ 15 Mio. pro Unternehmen (27,4% mehr als im Vorjahr)

Anstieg von Threat Intelligence bei "Spear-Phishing"-E-Mails gegen Betreiber von Atomkraftwerken

2016
357 Mio. neue Malware-Varianten

ANGRIFFE AUF LIEFERKETTEN SIND EINE NEUE BEDROHUNG

Industrielle Prozesse sind von einer stabilen Ressourcenbereitstellung und logistischem Support abhängig. Angreifer haben die Bedeutung der Lieferkette erkannt und entsprechende Attacken mit Abhör-, Infiltrations-, Fälschungs- und Störmaßnahmen gestartet. Das kann anhand der Auswirkungen von Cyber-Angriffen auf die globale Logistikbranche demonstriert werden. Im letzten Jahr meldeten FedEx und AP Moller-Maersk geschäftliche Verluste in Höhe von fast 600 Mio. US-Dollar durch die Ransomware-Attacke und den Angriff des „Wiper"-Virus. Da Lieferketten immer globaler werden, steigen die Risiken durch die absichtliche Einpflanzung von Schadfunktionen.

ZUSÄTZLICHE FINANZMITTEL SIND ERFORDERLICH, UM DIE COMPLIANCE-ANFORDERUNGEN ZU ERFÜLLEN

In diesem Zusammenhang müssen Unternehmen Budgets für Erkennungstechnologien und für das Notfallmanagement aufbringen; Investitionen in Vermeidungstechnologien sind nicht genug. KI (Künstliche Intelligenz) und Vorhersageanalysen für das Management von Cyber-Risiken für OT werden eingeführt. Die Compliance-Anforderungen von Regulierungsstellen für den Schutz kritischer Infrastrukturen werden steigen, die Compliance-Kosten für die Betreiber werden sich erhöhen. Regionale und branchenspezifische Standards bringen Klarheit in das Compliance-Thema. Datenschutzbestimmungen wie die DSGVO werden Einzug in diese Domäne halten, in der die Betreiber vor einzigartigen Herausforderungen im Umfeld des Datenschutzes und der Datensicherheit speziell für das IIOT (Industrial Internet of Things) stehen.

www.tuv.com/de/industrial-sec

Erfahren Sie mehr über Industrial Security in unserer globalen Meinungsumfrage, verfügbar ab Juli 2018.

Bleiben Sie auf dem Laufenden unter: www.tuv.com/de/OT

Trend 4: Wenn Abwehrmechanismen für Cyber-Angriffe vorhanden sind, verlagert sich die Fokussierung auf die Erkennung von Bedrohungen und angemessene Reaktionen

Angriffe der letzten Zeit zeigen, dass im Kampf gegen erfahrene und beharrliche Cyber-Kriminelle Verhinderungsmechanismen allein nicht ausreichen. Heute dauert es im Schnitt 191 Tage, bis ein Unternehmen ein Datenleck erkennt. Und je länger es dauert, eine Bedrohung zu erkennen und darauf zu reagieren, umso größer sind der finanzielle Schaden und der Reputationsverlust, den das Unternehmen durch den Vorfall erleidet. Durch den enormen Anstieg sicherheitsrelevanter Daten, die Einschränkungen von aktuellen Technologien, die ineffiziente Nutzung von vorhandenen Bedrohungsinformationen (Threat Intelligence), die fehlende Überwachung von IoT-Geräten und den Fachkräftemangel an Cybersecurity-Experten entstehen in den Unternehmen teure Verweildauern.

ORGANISATIONEN BENÖTIGEN IMMER NOCH ZU VIEL ZEIT FÜR DIE ERKENNUNG EINER DATENSCHUTZVERLETZUNG

Je schneller ein Datenleck erkannt und eingedämmt werden kann, umso geringer sind die Kosten und die Auswirkungen auf das Ansehen und das Business. Ein Cyber-Krimineller braucht nur wenige Minuten oder Stunden, um ein Netzwerk zu knacken und Basisdaten zu extrahieren. Die Identifizierung und der Diebstahl von kritischen Daten dauert Tage oder Wochen. Unternehmen brauchen aber im Schnitt 191 Tage, um eine Verletzung zu erkennen und 66 Tage, um sie einzudämmen. Organisationen, die die Erkennungszeit auf unter 100 Tage drücken können, können über 1 Mio. US-Dollar sparen. Darüber hinaus fällt der Aktienwert beim Bekanntwerden einer Datenschutzverletzung sofort um durchschnittlich fünf Prozent, im Einklang mit dem Kundenvertrauen. Bei Unternehmen, die kurze Erkennungs- und Reaktionszeiten vorweisen können, erholt sich der Aktienwert schnell; doch für den Rest gilt, dass der alte Stand oftmals nie wieder erreicht wird.

TRADITIONELLE KONZEPTE FÜR DIE ERKENNUNG VON BEDROHUNGEN SIND KOMPLEX

Traditionelle Konzepte bauen auf SIEM-Lösungen (Security Information and Event Management) auf. Anders als eine Sicherheitskamera, die einfach montiert wird und sofort Bilder liefert, ist der Umgang mit SIEM-Lösungen alles andere als einfach. Umständliche Implementierung, eingeschränkte Skalierbarkeit, Schwierigkeiten bei der Einbindung von Datenquellen und unübersichtliche Reporting-Prozesse – für diese Lösungen ist quasi eine kleine Armee von Sicherheitsanalysten nötig, um sie effizient zu nutzen. Erschwert wird das durch die Tatsache, dass sich die Menge der von den Sicherheitsteams analysierten Daten jedes Jahr verdoppelt und dass es dabei vermehrt um unstrukturierte Daten geht; ein Datentyp, den traditionelle SIEM-Tools nicht analysieren können.

DIE GRÖSSTEN BEFÜRCHTUNGEN DER TÜV RHEINLAND-EXPERTEN:

- „... nicht abgesicherte IoT-Geräte, die niemand updatet und die in vollem Umfang mit dem Internet verbunden sind."
- „... die Absicherung von kritischen nationalen Infrastrukturen und damit verbundenen Risiken für die Öffentliche Sicherheit und die nationale Wirtschaft."
- „... der Mangel an proaktiven Investments. Zur Zeit wird Geld nur im Nachgang eines Sicherheitsvorfalls ausgegeben oder weil es regulatorische Auflagen gibt."
- „... inadäquates Cybersecurity-Bewußtsein bei Mitarbeitern und auf Management-Level."
- „... Ignoranz gegenüber Sicherheitsrisiken, die durch Datenschutzprobleme entstehen. Technologie-Lösungen, die Familien, ältere Menschen oder Kinder dem Risiko von Cyber-Angriffen aussetzen."
- „... mangelndes Budget für Cybersecurity-Initiativen."
- „... Kompetenzen im Bereich Cybersecurity und der Fachkräftemangel in der Branche."

DER MANGEL AN CYBERSECURITY-KOMPETENZEN VERSCHÄRFT SICH

IT-Organisationen führen Cybersecurity als den Bereich an, in dem der Fachkräftemangel am dramatischsten ist. Ein Blick auf die globale jährliche Studie von ESG zum Status der IT zeigt einen alarmierenden Anstieg dieses Problems und eine Verdoppelung von 23% der Unternehmen in 2014 auf 51% in 2018.[7] Laut den Erwartungen wird es bis 2021 rund 3,5 Millionen unbesetzte Cybersecurity-Stellen geben. Über eine halbe Million dieser Stellen entfallen dabei auf die USA. Der Fachkräftemangel im Cybersecurity-Umfeld verschärft sich und es gibt keine Anzeichen, dass sich an dieser Situation in absehbarer Zukunft etwas ändert.

DIE SCHNELLE ERKENNUNG VON CYBER-BEDROHUNGEN UND DIE PRÄZISE REAKTION VERLANGEN NACH EINEM NEUEN KONZEPT

Moderne Malware und komplexe Cyber-Bedrohungen verlangen nach einem proaktiven, agilen Konzept als Ersatz für traditionelle SIEM-Lösungen. Traditionelle Lösungen erkennen bekannte Bedrohungen innerhalb fester Unternehmensnetzwerkgrenzen und anhand von signaturbasierten Verfahren, die heute aber überwunden werden können. Um die Erkennungszeiten spürbar zu verkürzen und die Eindämmung zu beschleunigen, werden Organisationen vermehrt auf erweiterte Sicherheitsanalysen setzen. Dieses neue Konzept nutzt Maschinendaten für die Identifizierung von Anomalien basierend auf einem vorbestimmten Basis-Nutzungsverhalten innerhalb der dynamischen Landschaft des modernen digitalen Unternehmens.

BARRIEREN FÜR DIE EFFIZIENTE NUTZUNG VON THREAT INTELLIGENCE BLEIBEN BESTEHEN

In einem Umfeld von „Big Security Data" kann die Kombination aus erweiterten Bedrohungsinformationen (Threat Intelligence) und einem Team aus Sicherheitsanalysten fundierte Erkenntnisse liefern. Threat Intelligence ist keine Technologie. Es ist das Wissen über den Gegner und seine Mittel, Motive und Absichten. Diese Bedrohungsinformationen sollten so verbreitet werden, dass Cybersecurity-Teams und die Fachabteilungen optimal beim Schutz der kritischen Ressourcen des Unternehmens unterstützt werden. Doch selbst die besten Bedrohungsinformationen sind nutzlos, wenn Sie keine Spezialisten mit dem Wissen, den Fähigkeiten und der Erfahrung haben, um wirkungsvoll mit diesen Informationen umzugehen. Leider besteht innerhalb der Branche ein starkes Gefälle. Nur die attraktivsten Marken mit den größten Budgets, die an der Spitze des Markts agieren, sind in der Lage, die besten Talente zu finden und vor allem zu binden.

www.tuv.com/apt

7 CSO online, research suggests cybersecurity skills shortage is getting worse, Januar 2018

WOLFGANG KIENER,
Business Development Manager Cybersecurity, TÜV Rheinland

„2018 wird ein Schlüsseljahr für Unternehmen in Bezug auf die Einführung neuer Threat-Detection-Konzepte. Wir helfen unseren Kunden bei der Nutzung von neuen, cloud-nativen Technologien für Sicherheitsanalysen und Maschinenlernen. Dadurch sind sie in der Lage, die enormen Mengen an Sicherheitsprotokollen und -daten zu analysieren, Bedrohungsinformationen (Threat Intelligence) besser zu nutzen, IoT- und OT-Technologien zu überwachen und den Mangel an qualifizierten Cybersecurity-Mitarbeitern zu kompensieren."

Trend 5: Zunehmende Nutzung von Künstlicher Intelligenz für Cyber-Attacken und -Abwehr

Auf ihrem Weg der digitalen Transformation werden Unternehmen in steigendem Maße zum Ziel für komplexe und hartnäckige Cyber-Attacken. Malware wird immer smarter. Sie kann sich „intelligent" anpassen und traditionelle Erkennungs- und Beseitigungsroutinen umgehen. Angesichts des globalen Mangels an Cybersecurity-Spezialisten sind die Unternehmen dabei, das Cyber-Wettrüsten zu verlieren. Die Menge an Sicherheitsdaten überschreitet bei weitem die Kapazitäten für ihre effiziente Nutzung. Das führt zu einer steigenden Anzahl von KI-fähigen Cybersecurity-Anwendungsfällen: Beschleunigung der Erkennung und Bekämpfung von Sicherheitsvorfällen, bessere Identifizierung und Vermittlung von Risiken gegenüber den Fachabteilungen und die Bereitstellung einer einheitlichen Sicht auf den Sicherheitsstatus innerhalb der gesamten Organisation.

UNTERNEHMEN VERLIEREN DAS CYBER-WETTRÜSTEN

Vorbei sind die Tage, in denen Cyber-Angreifer nicht viel mehr waren als nervende „Script-Kiddies". Sie haben sich weiterentwickelt – zu organisierten und gut finanzierten Cyber-Kriminellen und nationalstaatlichen Akteuren. Sie sind eine ernsthafte und komplexe Bedrohung, die regelmäßig über Unternehmen und Regierungen herfällt. Cyber-Kriminalität ist sehr lukrativ, risikoarm und global. Die Cybersecurity-Branche steht natürlich nicht still, trotzdem haben die Angreifer meistens den längeren Arm; wenn Sie also Schwachstellen nicht ausräumen, machen Sie es ihnen zu einfach.

THOMAS MÖRWALD,
Practice Leader,
Security Consulting,
TÜV Rheinland

„Der Einsatz Künstlicher Intelligenz wird für Cyber-Attacken wie für die Cyber-Abwehr sehr schnell und erheblich an Bedeutung gewinnen. Die Methoden stehen weitestgehend zur Verfügung, auch die notwendige Rechen-Kapazitäten sind heute kein Hindernis mehr. Ist die ‚Lernaufgabe' klar definiert, ist der Erfolg nur eine Frage der Zeit."

EXPERTEN VON TÜV RHEINLAND BETRACHTEN THREAT INTELLIGENCE ALS EIN STRATEGISCHES BUSINESS-TO-BUSINESS COLLABORATION TOOL, UM WISSEN ZWISCHEN UNTERNEHMEN ZU TEILEN, ...

1. .... um Vorfälle effektiver zu erkennen.
2. .... um schneller und effizienter auf Vorfälle zu reagieren.
3. .... um die eigene strategische Rolle in der Reaktion auf Cybersecurity-Vorfällen zu stärken.

DIE MENGE AN SICHERHEITSDATEN ÜBERSCHREITET BEI WEITEM DIE KAPAZITÄTEN FÜR IHRE EFFIZIENTE NUTZUNG

Die meisten Unternehmen haben Dutzende Sicherheitstechnologien implementiert und unter Umständen auch integriert. Die digitale Wirtschaft vernetzt alles und jeden. Die Folge: Milliarden neuer Endgeräte. Dadurch generieren wir so viele Sicherheitsereignisprotokolle und Alarminformationen, dass wir am Ende den Wald vor lauter Bäumen nicht mehr sehen. Das erschwert den wirkungsvollen Schutz des Unternehmens ungemein und stellt möglicherweise sogar ein größeres Risiko als die steigende Komplexität der eigentlichen Cyber-Angriffe dar.

DAS ZEITALTER VON KI-FÄHIGEN CYBER-ANGRIFFEN IST ANGEBROCHEN

Mit KI besteht die Gefahr, dass sich die ohnehin schon große Herausforderung von Cybersecurity, vor denen Unternehmen in einer zunehmend digitalen Welt stehen, noch verschärfen. KI-basierte Cyber-Angriffe sind noch rar, aber es gibt sie bereits. Im letzten Jahr wurden wir Zeuge des ersten auf künstlicher Intelligenz basierenden Cyber-Angriffs, bei dem rudimentäres Maschinenlernen genutzt wurde, um normale Verhaltensmuster innerhalb der Netzwerke eines Unternehmens zu studieren.[8] Sobald ein Grundverständnis über die Muster vorhanden war, begann die Malware, normales Netzwerkverhalten nachzuahmen, um selbst nicht erkannt zu werden.

CYBERSECURITY-EXPERTEN WERDEN KI FÜR DIE ABWEHR VON KI-ANGRIFFEN NUTZEN

Die Cyber-Angriffe der nächsten Generation werden KI-basierte Malware nutzen, die in Echtzeit reagieren kann, um Cybersecurity-Kontrollen zu umgehen. Deren Bekämpfung wird neue Abwehrkonzepte erforderlich machen. Cybersecurity-Experten setzen auf erweiterte Cyber-Schutzmechanismen, die KI nutzen, um auf solche Angriffe zu reagieren. An einem guten Tag können humane Sicherheitsanalysten, die vor einer potenziellen Phishing-Attacke gewarnt werden, den Angriff innerhalb von einigen Stunden eindämmen. Mit einer KI-basierten Sicherheitsautomatisierung lässt sich derselbe Angriff in nur wenigen Minuten entdecken und eindämmen. KI gilt daher zunehmend als kritischer Baustein einer modernen Cybersecurity-Strategie.

KI FÄNGT DEN ZUNEHMENDEN MANGEL AN CYBER-SECURITY-EXPERTEN AB

Mit KI können Sicherheitsteams riesige Mengen an Sicherheitsdaten zügig verarbeiten und Alarminformationen und Ereignisprotokolle in einen viel größeren Kontext setzen. Diese Fähigkeit, die Bedrohungen mit dem größten Gefahrenpotenzial zu priorisieren und in den Mittelpunkt zu rücken, ist ein Segen für Unternehmen, die mit begrenzten Cybersecurity-Mitteln ihre kritischen Ressourcen schützen möchten. Das birgt jedoch die Gefahr, dass einige Sicherheitsspezialisten (Sicherheitsanalysten von Tier 1 und Tier 2 oder Analysten im Security Operations Centre [SOC]) in den kommenden 5 bis 10 Jahren durch KI ersetzt werden könnten.[9]

www.tuv.com/pentest

8 Wall Street Journal, The Morning Download: First AI-Powered Cyberattacks Are Detected, November 2017
9 Security Now, Ai is stealing these IT-Security-Jobs now, März 2018

Trend 6: Zertifizierungen werden wichtig, um das Vertrauen in Cybersecurity zu stärken

Es herrscht weitgehend Einigkeit darüber, dass Cybersecurity und Datenschutz integrale Bestandteile einer digitalen und vernetzten Welt sind. Aber: Wie lässt sich das Schutzniveau eines Unternehmens objektiv einschätzen? Die Bedenken, ob und inwieweit Cybersecurity tatsächlich umgesetzt wird, nehmen zu. Dies führt dazu, dass bestehende und neue Standards, die Cybersecurity-Strategien international vergleichbar machen, immer stärker an Relevanz gewinnen. Für CISOs und Produkthersteller sind Zertifizierungen wichtig, um nachzuweisen, dass sie getan haben, was sie versprochen haben. Die Zertifizierungsverfahren für die Bestätigung der IT-Sicherheit von Produkten konzentrieren sich heute jedoch vor allem auf kritische Infrastrukturen und öffentliche Hand. Wo bleiben die Hersteller von Verbraucherprodukten?

WIRKUNGSVOLLE CYBERSECURITY IST VORAUSSETZUNG FÜR EINE FUNKTIONSFÄHIGE, IOT-BASIERTE WIRTSCHAFT

Angesichts der Tatsache, dass immer mehr Services online bereitgestellt und immer mehr vernetzte Geräte eingesetzt werden, wird deutlich, dass Cybersecurity eine kritische Bedeutung für die Überlebensfähigkeit unserer digitalen Wirtschaft hat. Der Schutz unseres digitalen Ökosystems, von der kritischen Infrastruktur bis hin zu Verbrauchergeräten, muss eine elementare Voraussetzung für das digitale Geschäft sein. Das bedeutet, dass Cyber-Bedrohungen eine ernsthafte Gefahr für das moderne Gesellschaftsgefüge darstellen.[10]

DAS FÜHRT ZU WACHSENDEN BEDENKEN IM HINBLICK AUF DAS VERTRAUEN IN CYBERSECURITY

Der globale Risikobericht des diesjährigen Weltwirtschaftsforums legt dar, dass sich Cyber-Angriffe auf Unternehmen in den letzten fünf Jahren verdoppelt haben. Das hat in diesem Jahr die Angst vor Cyber-Angriffen und massiven Datendiebstählen enorm geschürt. In der allgemeinen Wahrnehmung zählen diese beiden Aspekte zu den fünf wahrscheinlichsten globalen Risiken.[11] Eine Umfrage des Pew Research Center hat ergeben, dass die Mehrheit (64%) der Amerikaner bereits Opfer einer größeren Datenschutzverletzung wurden und dass viele Verbraucher den Unternehmen nicht zutrauen, ihre persönlichen Daten ausreichend zu schützen.[12] In Europa hat die Europäische Kommission zwei Initiativen für die Zertifizierung und Kennzeichnung angekündigt: einen Sicherheitsrahmen für ICT-Produkte und ein IoT-Siegel für Vertrauenswürdigkeit („Trusted IoT Label"). Diese enthalten Informationen über die verschiedenen Stufen des Datenschutzes und der Sicherheit und demonstrieren, sofern zutreffend, die Compliance mit der Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie); die 2016 vom Europaparlament verabschiedet wurde.

AUSWIRKUNGEN AUF GESCHÄFTLICHE ÖKOSYSTEME UND LIEFERKETTEN

Die andauernde digitale Transformation des Geschäfts führt zu immer komplexeren und stärker vernetzten Ökosystemen und Lieferketten. Die Automobilindustrie ist dafür ein gutes Beispiel. In diesem Sektor gewinnt der TISAX-Audit (Trusted Information Security Assessment Exchange) zunehmend an Bedeutung. TISAX gibt akkreditierten Anbietern die Möglichkeit, gegenseitig anerkannte Bewertungen basierend auf dem Information Security Assessment des VDA (Verband der Automobilindustrie) anzubieten; welches wiederum auf einem Katalog von Kriterien für die Informationssicherheit basiert, der die Schlüsselaspekte der internationalen Normen ISO/IEC 27001 und 27002 umfasst.

10 DIGITALEUROPE's views on Cybersecurity Certification and Labelling Schemes, März 2017
11 World Economic Forum: The Global Risks Report 2018, 13th Edition
12 Pew Research Center, Americans and Cybersecurity, Januar 2017

DR. DANIEL HAMBURG,
Leiter, Center of Excellence Testing and Certification, TÜV Rheinland

„Eine Zertifizierung signalisiert ein entsprechendes Niveau der IT-Sicherheit gemäß nationaler oder internationaler Standards. Das schafft eine Vergleichsmöglichkeit auf dem Markt und Vertrauen – wenn der Zertifizierungsrahmen transparent und übersichtlich ist."

ZERTIFIZIERUNGEN BESTÄTIGEN, DASS SIE DAS GETAN HABEN, WAS SIE VERSPROCHEN HABEN

Mit der Einsicht, dass Cybersecurity von kritischer Bedeutung ist, stellt sich die Frage: Wie lässt sich das Schutzniveau eines Unternehmens objektiv einschätzen? Das Vorliegen einer entsprechenden Zertifizierung spielt etwa bei der DSGVO eine wichtige Rolle, so u.a. bei der Entscheidung über das Ob und die Höhe von Bußgeldern, falls das Unternehmen nicht alle Vorgaben erfüllt oder dagegen verstößt. Eine Zertifizierung kann belegen, dass sich das Unternehmen eingehend mit einer neuen Verordnung oder einem bereits bestehenden Standard auseinandergesetzt und diese gänzlich umgesetzt hat.

REGULIERTE ZERTIFIZIERUNGSSYSTEME HINKEN DER MARKTNACHFRAGE HINTERHER

Die Idee eines Rahmenwerks für die Sicherheitszertifizierung von Produkten und Dienstleistungen ist genau der richtige Ansatz. Es muss aber sichergestellt werden, dass die Zertifizierung nach Möglichkeit auf globaler Ebene erfolgt und kein trügerisches Sicherheitsgefühl schafft, denn 100-prozentige Sicherheit gibt es in der IT nicht. Zertifizierungsprogramme auf nationaler Ebene, die Standards und Evaluierungsmethoden definieren und nur Zertifizierungsstellen innerhalb der eigenen geografischen Region anerkennen, können Marktfragmentierung schaffen. Die jüngsten Erfahrungen mit allgemeinen Kriterien haben gezeigt, dass selbst bei einem länderübergreifenden Konzept globaler Support erforderlich ist, um zu verhindern, dass für ein Produkt mehrere regionale Zertifizierungen gelten. Letztendlich ist Cybersecurity eine globale Angelegenheit, für die internationale Lösungen gefragt sind.

VERBRAUCHER BENÖTIGEN VERSTÄNDLICHE, TRANSPARENTE INFORMATIONEN

Die unabhängige Produktevaluierung kann jedoch ein ressourcenintensiver Prozess sein und konzentriert sich daher auf risikoreiche Produkte und Dienstleistungen der Regierung oder der kritischen Infrastruktur. Das öffnet die Tür für prozessbasierte Konzepte wie ISO/IEC 27034 sowie für Zertifizierungen für spezifische Systemtypen wie ISA/IEC 62443. Doch mit dem steigenden Druck, noch schnellere und noch billigere Produktentwicklungszyklen zu realisieren, müssen agile Beurteilungsschemata, bei denen Umgebungen für die Testautomatisierung zum Einsatz kommen, erstellt und weiterentwickelt werden.

www.tuv.com/datenschutz-zertifizierung

Trend 7: Ablösung der Kennwörter durch biometrische Authentifizierung

Unser digitales Leben wird durch ein komplexes Netz aus Online-Apps bestimmt, unsere digitale Identität durch Benutzernamen und Passwörter geschützt. Um den Schutz der digitalen Identität hinter diesen Apps zu steigern, wird empfohlen, schwer zu erratende und komplexe Kennwörter zu verwenden und diese regelmäßig zu ändern. In der Praxis geschieht das aber nur selten. Mit der exponentiellen Zunahme der Rechenleistung und dem einfachen Zugang über die Cloud können Kennwörter in einer immer kürzeren Zeit geknackt werden. Was 2000 noch fast 4 Jahre gedauert hat, ist heute in 2 Monaten erledigt.[13] Wenn man bedenkt, dass Kennwörter häufig gestohlen, gehackt und gehandelt werden, wird klar, dass sie noch nie offener verfügbar waren als heute. Aus diesem Grund begegnen wir heute bei Mobiltelefonen, Tablets und Laptops und auch bei physischen sowie Online-Services vermehrt der biometrischen Authentifizierung (Gesicht, Fingerabdruck, Iris und Sprache).

BEWÄHRTE KENNWORTRICHTLINIEN SIND ALLSEITS BEKANNT, SORGEN ABER IN DER PRAXIS FÜR FRUSTRATION

Traditionelle Best-Practice-Konzepte für die Erstellung von Kennwörtern haben uns träge werden lassen. Der Zwang, Großschreibung, Sonderzeichen und Ziffern zu verwenden und das Kennwort alle 90 Tage zu ändern, hat zu Kennwörtern wie „P@ssW0rd123!" geführt. Das gegebene Passwort ist nicht leicht zu merken, aber relativ einfach zu erraten. Wer sich nach einem längeren Zeitraum wieder an einer Anwendung anmelden möchte, ist schnell frustriert, denn das Kennwort ist vergessen und muss deshalb zurückgesetzt werden. Das Problem ist, dass die meisten Menschen immer dasselbe Schema für die Erstellung von Kennwörtern verwenden. Dadurch sind diese vorhersagbar und besonders anfällig gegen Algorithmen zum Knacken von Kennwörtern, die sich die Physiognomie von Passwörtern zunutze machen.

DAS MOORESCHE GESETZ LÄSST KENNWÖRTER MIT DER ZEIT SCHWÄCHER WERDEN

Im Laufe der Zeit werden Kennwörter in bedrohlichem Maße schwächer, da sich die Rechenleistung ungefähr alle 18 Monate verdoppelt. Außerdem werden Cyber-Kriminelle immer versierter. Beispiel: War ein Kennwort im Jahr 2000 erst nach fast vier Jahren zu knacken, dauerte das 2004 nur noch etwas über ein Jahr und fünf Jahre später in 2009 nur noch 4 Monate. In der heutigen Zeit können Kennwörter einfach nicht mehr den komplexen Cyber-Bedrohungen standhalten. Ein Drittel der Cyber-Kriminalität entfällt auf gestohlene Kennwörter. Bisher wurden bereits über 1,5 Milliarden Kennwörter gestohlen.

MARK CODERRE,
Leiter, Center of Excellence Risk & Compliance, TÜV Rheinland

„Adaptive, risikobasierte Authentisierungslösungen werden häufiger. Doch die Zukunft der Authentisierung hat bereits begonnen."

13 Better Buys, Estimating password cracking times

DIE TÜV RHEINLAND-EXPERTEN SEHEN DIE ZUKUNFT DER NUTZER-IDENTIFIKATION IN NEUEN METHODEN:

- **Die zertifikatsbasierte Authentifizierung** bzw. die gegenseitige Authentifizierung (Mutual Authentication) beschreibt einen Prozess, bei dem sich zwei Parteien (meist Client und Server) gegenseitig authentifizieren. Durch den Einsatz eines digitalen Zertifikats wird der Benutzer, Computer oder das Gerät identifiziert, bevor diesem Zugang zu einer Ressource, einem Netzwerk, einer Anwendung usw. gewährt wird.
- **Biometrische Erkennung** wird von Geräte-Herstellern angeboten und weist eine Identität auf Basis menschlicher Charakteristika nach. Dies kann der Schlüssel sein für ein deutlich effektiveres System. Experten sagen eine „Fast-Gewissheit" voraus, dass innerhalb weniger Jahre drei biometrische Optionen in jedem Smartphone zu Standard-Features werden: der in den Bildschirm eingebaute Fingerabdruck-Scanner, Gesichtserkennung durch High-Definition-Kameras und Stimm-Erkennung auf Basis einer großen Sammlung menschlicher Stimmproben.
- **FIDO (Fast Identity Online)** umfasst eine Reihe plattformunabhängiger Sicherheitsspezifikationen, um eine starke Authentifizierung zu ermöglichen. Die Spezifikationen für FIDO unterstützen die Multi-Faktor-Authentifizierung (MFA) und Kryptographie mit einem öffentlichen Schlüssel. Ein wesentlicher Vorteil der FIDO-kompatiblen Authentifizierung ist die Tatsache, dass Benutzer ihre komplizierten Kennwörter nicht verwenden müssen. Sie müssen auch nicht mit komplexen Richtlinien für starke Passwörter fertig werden. Wenn ein Benutzer sein Passwort vergessen hat, ist kein Reset erforderlich. Im Gegensatz zu Datenbanken für Passwörter speichert FIDO personenbezogene Identifikationsinformationen (PII), z. B. biometrische Authentifizierung lokal, d. h. auf dem Gerät des Benutzers, um es angemessen zu schützen.

AKTUELLE DATENLECKS WEISEN GANZ KLAR IN RICHTUNG DER KENNWÖRTER

Bei vielen Datenlecks, die die Schlagzeilen in letzter Zeit bestimmten, war der Angriffsvektor ein mehrfach verwendetes Kennwort.[14] Das ist wenig überraschend, da viele Menschen ein Kennwort für verschiedene Konten nutzen. Beispielsweise konnte das Kennwort eines Auftragnehmers des Weißen Hauses nur deshalb geknackt werden, weil es mit dem Kennwort identisch war, das er für sein Gmail-Konto verwendete; welches wiederum beim Adobe-Sicherheitsvorfall im Jahr 2013 gestohlen wurde. Ganze zwei Drittel aller Fälle von Datenschutzverletzungen sind die Folge der Verwendung von schwachen oder Standardkennwörtern oder eines Kennwortdiebstahls. Und nahezu alle Phishing-Attacken zielen auf die Anmeldedaten von Benutzern ab.[15]

MIT DER BIOMETRISCHEN AUTHENTIFIZIERUNG LÄSST SICH EXAKT FESTSTELLEN, WER AUF EIN SYSTEM ZUGREIFT

Die biometrische Authentifizierung schafft Klarheit; jeder Zugriff oder Vorgang wird gemeinsam mit der damit verbundenen Person dokumentiert. Das reduziert das Risiko eines Missbrauchs, Betrugs oder Datenabflusses. Künftig werden drei biometrische Optionen zum Standardumfang jedes neuen Telefons gehören: ein im Bildschirm integrierter Fingerabdruck-Scanner, Gesichtserkennung mit hochauflösenden Kameras und Spracherkennung basierend auf einer großen Sammlung von menschlichen Stimmmustern. Die Anzahl der Geräte mit Fingerabdrucksensor hat die Marke von einer Milliarde bereits überschritten.[16] Anders als bei Kennwörtern ist es unmöglich, die biometrischen Anmeldedaten zu vergessen. Zudem können diese Informationen nur schwer gefälscht werden. Sollten andererseits biometrische Daten jemals kompromittiert werden, dürfte es schwierig werden, den Fingerabdruck eines Dritten zu fälschen oder dessen Aussehen zu verändern.

www.tuv.com/iam

14 CNBC, Passwords are the weakest link in cybersecurity today, Oktober 2016
15 IDAgent, 63% of Data Breaches Result From Weak or Stolen Passwords, 2016
16 Information Age, In the modern era biometrics should replace passwords, Februar 2017

Trend 8: Ausgewählte Branchen im Visier der Angreifer: Gesundheitswesen, Finanzdienstleistungen und Energieversorgung

Der Großteil der Cyberangriffe wird von Kriminellen aus finanziellen Motiven begangen. Der Wert von Daten im Darknet richtet sich nach der Nachfrage, ihrer Verfügbarkeit, ihrer Vollständigkeit und den Möglichkeiten für deren Nutzung. Daher sind persönliche Informationen aus dem Gesundheits- und Finanzsektor besonders gefragt. Krankenakten kosten, je nachdem, wie vollständig sie sind, zwischen 1 bis 1000 US-Dollar. Kreditkartendaten werden für 5 bis 30 US-Dollar verkauft, wenn die benötigten Informationen für ihre Nutzung mitgeliefert werden. Andere Cyber-Angriffe haben eher politische oder nationalstaatliche Motive. Im Jahr 2018 besteht hier ein erhöhtes Risiko für Störungen von kritischen Services durch Angriffe auf den Energiesektor. Beleg dafür sind die Berichte der jüngsten Zeit über die von Russland initiierten Cyber-Attacken auf das US-Stromnetz[17], die vermutlich bereits seit einem oder mehreren Jahren ausgeführt werden.

MEDIZINBRANCHE: VIELFÄLTIGE HERAUSFORDERUNGEN – STEIGENDE AUSGABEN

2017 hat sich die Zahl der Cyber-Angriffe auf Krankenhäuser und Gesundheitssysteme in einem alarmierenden Maß erhöht, Tendenz steigend.[18] Somit wächst auch der Bedarf nach Cybersecurity: Aufgrund der steigenden Digitalisierung und Nutzung von Gesundheitsinformationen, der Möglichkeit des Zugangs der Verbraucher zu privaten Gesundheitsdaten, der anhaltenden Innovation und Verfügbarkeit von verbraucherorientierten Health-Anwendungen und entsprechenden Geräten sowie der steigenden Anzahl von vernetzten medizinischen Geräten kommt es zu einem spürbaren Anstieg von potenziellen Cyber-Bedrohungen im Gesundheitssektor. Die Herausforderungen sind vielfältig. Ob Malware, die die Integrität von Systemen und die Daten von Patienten gefährdet, oder DDoS-Angriffe (Distributed Denial of Service), die die Patientenversorgung lahmlegen: Cyber-Angriffe können schwerwiegendere Folgen als finanzielle Verluste oder Datenschutzverletzungen haben – unmittelbare Auswirkungen auf das Leben der Patienten. Patientensicherheit, finanzielle Verluste, Störungen der Gesundheitsversorgung, Imageschäden und rechtliche Folgen durch Cyber-Angriffe – das sind im Jahr 2018 die Hauptrisiken für die Gesundheitsbranche. Die Folge: Organisationen geben mehr Geld für den Schutz ihrer Systeme und der Patientendaten aus. Cybersecurity Ventures prognostiziert für die nächsten fünf Jahre, von 2017 bis 2021, globale Cybersicherheitsausgaben von über 65 Milliarden US-Dollar.[19]

17 Reuters, In a first, U.S. blames Russia for cyber attacks on energy grid, März 2018
18 Health IT & CIO Report, 11 of the biggest healthcare cyberattacks of 2017, Dezember 2017
19 CSO online, Why healthcare cybersecurity spending will exceed $65B over the next 5 years, Februar 2018

FINANZSEKTOR: WACHSENDE ANZAHL UND KOMPLEXITÄT VON ANGRIFFEN

Der Bereich der Finanzdienstleistungen hat sich im Hinblick auf Cybersecurity relativ gut aufgestellt. Dies ist im Wesentlichen auch auf gesetzliche Regelungen, zum Beispiel im Hinblick auf das Risikomanagement, zurückzuführen. Dennoch war 2017 ein Wendepunkt: Wir erlebten eine wachsende Anzahl und Komplexität von Cyber-Angriffen ausgelöst durch eine Zunahme von Cyber-Kriminalitäts-Services, mit denen modernste Cyber-Angriffswaffen an weniger versierte Gegner verkauft und von ihnen eingesetzt wurden. Die gemeldeten Cyber-Attacken gegen Finanzdienstleister haben im letzten Jahr um 80 Prozent zugenommen. Das verdeutlicht den generellen Anstieg von Angriffen auf Organisationen.[20] Das Risiko von Cyber-Angriffen wird durch das verstärkte Outsourcing, das von Investment-Händler und Vermögensverwaltern betrieben wird, um ein Vielfaches erhöht.[21]

UNTERSCHIEDLICHE ANGRIFFSVEKTOREN — EIN ZIEL: GELD

Verschiedene cyberkriminelle Gruppen kompromittierten Bankeninfrastrukturen, E-Money-Systeme, Kryptowährungsbörsen, Kapitalverwaltungsfonds und sogar Casinos, um große Geldsummen abfließen zu lassen. In diesem Kontext hat das Abfangen von elektronischen Aktivitäten von Bankkunden durch die Umleitung von Bankendomänen für die Durchführung von Phishing-Attacken, die Installation von Schadcodes und die Übernahme von Transaktionen von Kunden, die gerade Online-Banking-Dienste in Anspruch nehmen, schon eher traditionelle Züge. Von den anhaltenden Cyber-Attacken auf Systeme, die SWIFT-Dienste ausführen[22], waren mehrere Banken in mehr als 10 Ländern weltweit betroffen. Neben den SWIFT-Angriffen beschäftigen sich Cyber-Kriminelle aber auch intensiv mit der Manipulation von Geldautomaten und greifen die Netzwerke und PoS[23]-Terminalnetze der Finanzinstitute an, um an das Geld der Kunden zu gelangen. Angriffe auf Geldautomaten wurden 2017 so populär, dass sogar der erste Malware-as-a-Service für Geldautomaten angeboten wurde.

NEUE UNBEKANNTE RISIKEN DURCH OFFENE BANKEN-ÖKOSYSTEME

In Zukunft wird der Finanzsektor weitere finanzielle Verluste hinnehmen müssen. Störungen von kritischen Services werden zunehmen – genau wie die Gefahr von Rechtsstreitigkeiten in Verbindung mit Cyber-Angriffen beispielweise durch DDoS- und Malware-Attacken. Durch die Notwendigkeit einer weiteren Öffnung der Ökosysteme der Banken werden neue, bis dato unbekannte Risiken entstehen.
Zudem droht Finanzorganisationen ein erheblicher Imageschaden, wenn Banken und Versicherungen im Rahmen der DSGVO gezwungen sind, alle aufgetretenen Datenschutzverletzungen zu kommunizieren. Dennoch ist das Vertrauen der Kunden in Banken und Versicherungen nach wie vor hoch: 82 Prozent der Kunden zählen sie zu den vertrauenswürdigsten Organisationen – vielleicht aufgrund der Praxis, dass Finanzinstitute nicht freiwillig Nachrichten über Datenschutzverletzungen austauschen.[24]
Für Finanzorganisationen ist es eine große Chance, sektorenübergreifend Kooperationen im Bereich Cybersecurity einzugehen, einschließlich Versicherungen, Banken und Sicherheitsfirmen. Solch konzertierte Aktionen weisen in die richtige Richtung, denn Cybersecurity im Kontext von kritischen Infrastrukturen gehen die gesamte Branche an und betreffen das Wohl der gesamten Gesellschaft.

20 Information age, Rise cyber attacks financial services firms, Januar 2018
21 Financial Post, Financial firm outsourcing increasing risk of cyberattacks: IIAC, Januar 2018
22 Financial Post, Financial firm outsourcing increasing risk of cyberattacks: IIAC, November 2017
23 Point of Sale-Terminalnetze
24 Computerweekly, Finance firms are vulnerable to cyber attacks, so why do customers think they are secure?, Februar 2017

ENERGIESEKTOR: ATTRAKTIVES ZIEL DANK SEINER NATIONALEN UND WIRTSCHAFTLICHEN BEDEUTUNG

Der Energiesektor wird zum Hauptziel von Cyber-Angriffen. Besonders betroffen sind Firmen, die sich mit der Entwicklung von alternativen Energien, dem Kohlebergbau, der Entwicklung von Kernenergien, der Verteilung von Erdgas, der Förderung und Produktion von Öl und Gas, der Herstellung von Equipment oder Bereitstellung von Services für Öl- und Gasfelder sowie der Erdölraffination beschäftigen. Diese Firmen sind aufgrund ihrer Bedeutung für die nationale und wirtschaftliche Sicherheit hochinteressante Ziele. Da ist es kaum verwunderlich, dass die Angst vor potenziellen Cyber-Angriffen auf die Energieinfrastruktur in den letzten Jahren stark zugenommen hat.

NEUE QUALITÄT VON ANGRIFFEN

Im Rampenlicht: „klassische" Daten, die Energieunternehmen gestohlen werden, sind Geschäftsprozessinformationen, Informationen über Vertragsverhandlungen, die Kommunikation der Führungsebene, Marktanalysen und proprietäre Technologien.[25] In 2017 waren Angreifer mit Dragonfly und einer neue Welle von Cyber-Attacken in der Lage, die Betriebsabläufe empfindlich zu stören.[26] Doch die Art der Angriffe wandelt sich: Laut Quellen der New York Times sind im August 2017 Hacker in die Computersysteme in einer Erdölanlage in Saudi-Arabien eingedrungen. Ihr Ziel war es nicht nur, Daten zu stehlen oder zu zerstören, sie wollten auch eine tödliche Explosion auslösen. Das ist eine völlig neue Qualität von Angriffen, die ohne weiteres auch in anderen Ländern auftreten können, da die betroffenen Systeme in Tausenden von industriellen Anlagen auf der ganzen Welt eingesetzt werden.[27] Und erst kürzlich, im April 2018, befand sich der Energiesektor in Großbritannien in erhöhter Alarmbereitschaft, da Cyber-Angriffe auf das Stromnetz des Landes befürchtet wurden.[28]
Vor diesem Hintergrund überlegen mehr und mehr Regierungen weltweit, wie sie den polizeilichen Schutz kritischer Infrastrukturen, wie z.B. kerntechnischer Anlagen, optimieren können. Ein Regulierungsrahmen für Cybersecurity in kritischen Sektoren steht im Mai 2018 in Großbritannien vor der Umsetzung.

ERNSTHAFTE AUSWIRKUNGEN AUF DIE ALLGEMEINE VERSORGUNGSSICHERHEIT

Die Cybersecurity-Risiken nehmen weiter zu: Eine dezentrale Energieversorgung erfordert ein Verteilnetz, das nicht mehr allein auf der herkömmlichen Perimetersicherheit basiert. Intelligente Netze stellen eine große Anzahl von Gateways für gezielte komplexe Angriffe und DDoS-Attacken dar. Das wachsende Pairing von mobilen privaten Geräten mit einer geringen Perimetersicherheit birgt erhebliche Malware-Risiken, wie etwa im Falle von WannaCry, die auch gravierende Auswirkungen auf das Gemeinwohl und die allgemeine Versorgungssicherheit haben können.

25 Intelligence Report, Cyber Threats to the Energy Industry, 2016
26 Symantec, Dragonfly: Western energy sector targeted by sophisticated attack group, Oktober 2017
27 Oilprice, Energy Sector Under Threat From Deadly Cyberattacks, März 2018
28 Financial Times, Energy sector on alert for cyber attacks on UK power network, April 2018

ANDREAS WALBRODT,
Director of Sales Cybersecurity,
TÜV Rheinland

„Die Erfahrung zeigt, dass gute Cybersecurity-Hygiene erlaubt den Großteil der Risiken zu beherrschen. Die Herausforderung, die wir täglich erleben, ist, die Grundlagen zu schaffen und darauf aufzubauen."

www.tuv.com/informationssicherheit

TÜV Rheinland
ICT & Business Solutions
Am Grauen Stein
51105 Köln
Tel. +49 221 806-0
cybersecurity@tuv.com

www.tuv.com/informationssicherheit

TÜVRheinland®
Genau. Richtig.