MANAGEMENTKOMPASS

02
2017

Cyber Security

TREND
Cyber Security
ist geschäftskritisch

THINK TANK
Mit SIEM for Business
Angriffe gezielt aufhalten

PRAXIS
Zahlungsverkehr: Betrugs-
prävention nicht nur Kür

F.A.Z.-INSTITUT

sopra steria
CONSULTING

Urs M. Krämer
CEO
Sopra Steria Consulting

„WannaCry hat einmal mehr gezeigt, wie verwundbar eine digitalisierte Gesellschaft ist. Die Bedrohungslage erfährt durch das Internet of Things einen neuen Schub. Spätestens jetzt gehört das Thema IT-Sicherheit ganz oben auf jede Management-Agenda – sie ist Pflichtdisziplin der digitalen Transformation. Ein rein technischer Ansatz greift jedoch zu kurz. Ohne die kontinuierliche Sensibilisierung der Mitarbeiter bleibt der Wirkungsgrad intelligentester Security-Lösungen eingeschränkt."

VORWORT

Jens Weidmann
Präsident der
Deutschen Bundesbank

„Cyber-Attacken können potenziell das Vertrauen der Öffentlichkeit in das Finanzsystem aushöhlen. Um die positiven Effekte einer digitalen Finanzwelt nicht zu gefährden, wird es entscheidend darauf ankommen, solche Cyber-Attacken ins Visier zu nehmen."

Torsten Jüngling
General Manager DACH,
Nordics and East Europe,
BT Security

„Cyber-Angriffe können unabsehbare Folgen für ein Unternehmen haben – von Geschäftsausfällen aufgrund einer DDoS-Attacke über Imageschäden durch den Verlust von Kundendaten bis hin zur persönlichen Haftung des Managements. Die IT-Sicherheit ist deshalb ein strategisches Unternehmensziel und muss Chefsache sein."

Mit der Digitalisierung steigt die unternehmerische Verletzlichkeit. Datendiebstahl, Spionage, Sabotage und Erpressung bedrohen alle Branchen, öffentliche Einrichtungen und Kritische Infrastrukturen. Doch viele Organisationen treiben die Digitalisierung ihrer Geschäfts-und Produktionsprozesse voran, ohne dabei dem Thema Security ausreichende Aufmerksamkeit zu widmen. Während kreative Hacker und andere Kriminelle ein beliebig vielschichtiges Arsenal für ihre Angriffe auf die Daten- und Betriebssicherheit einsetzen, beschränken sich der Schutz und die Abwehr unbefugten Eindringens vielerorts weiterhin auf altbekannte Security-Maßnahmen, die heute nicht mehr ausreichen.

Das Internet der Dinge bringt nicht nur neue Möglichkeiten, sondern auch unsichere Schnittstellen und Anwendungen mit sich. Zudem begünstigen systemische Schwachstellen und arglose Mitarbeiter die Cyber-Kriminalität und andere Angriffe auf den Motor des modernen wirtschaftlichen und gesellschaftlichen Lebens: die Daten. Um diese bestmöglich und gesetzeskonform zu schützen, müssen Unternehmen ihre IT-basierten Abläufe und Aktionen durchgängig überwachen. Ziel sollte sein, in den Datenströmen selbst kleinste Abweichungen zu erkennen, diese zu analysieren und flexibel reagieren zu können. Wichtig sind nicht nur technische Lösungen, sondern auch das Wissen um und das Bewusstsein für die Risiken.

Welche technischen, organisatorischen und mitarbeiterbezogenen Herausforderungen die aktuellen Spielarten des Cybercrime für Unternehmen mit sich bringen, beleuchtet dieser Managementkompass ebenso wie rechtliche Implikationen und wirksame Maßnahmen zur Prävention, Erkennung und Reaktion.

Sopra Steria Consulting

F.A.Z.-Institut

MEHR SCHUTZ DURCH CYBER SECURITY

In Zeiten fortschreitender Digitalisierung und Vernetzung hat die Reaktionsfähigkeit hinsichtlich Datendiebstahl und -missbrauch eine ebenso hohe Priorität wie die Prävention. Viel steht auf dem Spiel, wenn Cyber-Kriminelle Unternehmen erpressen, geistiges Eigentum abgreifen oder produktions- und geschäftskritische Abläufe lahmlegen. Unternehmensentscheider müssen sich fragen, ob ihre vorhandenen Systeme und Schutzmaßnahmen für den stetigen Wettlauf zwischen Cybercrime und Cyber Security ausreichend gerüstet sind und wo Handlungsbedarf besteht. Eine technische Lösung allein reicht jedoch nicht aus, denn Cyber-Kriminelle setzen oft gezielt bei der Schwachstelle Mensch an. Daher sollte jedes Unternehmen seine Mitarbeiter über die Risiken aufklären und regelmäßig schulen.

1 | » MANAGEMENTEMPFEHLUNG

Nehmen Sie zunächst die vorhandene IT und Anwendungslandschaft gründlich unter die Lupe, und spüren Sie unsauber aufgesetzte Prozesse auf. Betriebs- und Datensicherheit sind die Grundvoraussetzungen für die erfolgreiche Digitalisierung jedweder Produktions- und Geschäftsprozesse. Bevor Sie Entscheidungen zur Vernetzung (etwa zur Einbindung von Maschinen, Geräten und Abläufen in das Internet of Things, IoT) treffen, vergegenwärtigen Sie sich, dass die Modernisierung durch Digitalisierung auch neue Angriffsflächen schaffen kann.

Die Nachrüstung und Integration bestehender (Legacy-)Systeme mit modernen, Cloud-basierten Lösungen kann oft Sicherheitslücken entstehen lassen oder bereits vorhandene vergrößern, die für Datendiebstahl und -missbrauch dann ebenso zum Einfallstor werden wie für Sabotage oder Erpressung. Eine mangelnde Anwendungssicherheit, veraltete Betriebssysteme und unzureichend programmierte Schnittstellen zum IoT begünstigen IT-Ausfälle und damit Betriebsunterbrechungen. Viele Mankos im technischen Innenleben von Unternehmen machen Angriffe aus dem sogenannten Cyberspace erst möglich.

Wo Produktionsanlagen und Lieferketten immer stärker vernetzt sind und direkt miteinander agieren, können die Folgen eines technischen Fehlers oder menschlichen Versagens dramatischer denn je sein. Nicht korrekt verarbeitete, falsch formatierte oder missinterpretierte Daten können beispielsweise in Versorgungsnetzen, smarten Fabriken und anderen Industrie-4.0-Umgebungen zu schwerwiegenden Fehlleistungen, Ausfällen oder Stillstand führen.

Die eigene digitale Transformation sollte daher nicht im Hauruckverfahren erfolgen, sondern schrittweise, sorgsam und mit Blick auf eine umfassende Sicherheit. Dabei ist gut beraten, wer sich nicht allein auf die eigene IT-Abteilung verlässt, sondern bereits vor der unabdingbaren Schwachstellenanalyse ausgewiesene Modernisierungs- und Security-Experten hinzuzuzieht.

2 | » MANAGEMENTEMPFEHLUNG

Machen Sie Cyber Security zur Chefsache und die Widerstandsfähigkeit (Resilience) zum Schwerpunkt der Sicherheitsstrategie. Angriffe von innen und außen wird es immer geben, also sind Reaktionsbereitschaft und -fähigkeit das oberste Gebot. Die Kontinuität Ihres Geschäftsbetriebes muss auch bei schwerwiegenden Sicherheitsvorfällen gewährleistet bleiben.

Führungskräfte sollten sich fragen, wie es um das Risikomanagement, Notfallpläne und die Verantwortlichkeiten bestellt ist und sich zumindest einen Überblick über die aktuellen Grundvoraussetzungen verschaffen. Um Fehlinvestitionen zu vermeiden und zielführend auf die (Neu-)Gestaltung der unternehmensweiten Sicherheitsrichtli-

nien einzuwirken, gilt es, die Aussagen interner Mitarbeiter zur Sicherheitslage realistisch einschätzen zu können. Selbstüberschätzung in Sachen IT- und Cyber Security ist eine der größten Gefahren für die Betriebs- und Datensicherheit und noch immer weitverbreitet.

Etliche Studien belegen, dass gerade Geschäftsführer ihr Unternehmen häufig deutlich besser gegen interne Sicherheitsverstöße und externe Angriffe gerüstet sehen, als es tatsächlich ist. In vielen Unternehmen klafft eine breite Lücke zwischen der realen Widerstandsfähigkeit und einer Bedrohungslage, die immer ernster wird – sowohl mit Blick auf die Schwere der Angriffe als auch mit Blick auf die Art der Angreifer.

Abhilfe schaffen gezielte Investitionen in intelligente Bedrohungserkennung, prädiktive Datenanalysen und Incident-Response-Lösungen. 100-prozentige Sicherheit bieten zwar auch diese Ansätze nicht, aber sie tragen ganz wesentlich zu einer signifikanten Verringerung des Schadensrisikos und der Folgen gravierender Sicherheitsvorfälle bei.

3 | » MANAGEMENTEMPFEHLUNG

Stellen Sie sich auf strengere Datenschutzregeln ein. Zum 25. Mai 2018 wird die bereits heute geltende EU-Datenschutz-Grundverordnung (DSGVO) verbindlich. Nutzen Sie die Übergangsfrist bis zum Mai 2018, um Compliance mit den neuen EU-Richtlinien herzustellen, und bedenken Sie, dass eine Verletzung der Sorgfaltspflicht bei Datenschutz und Systemsicherheit nach deutschem Recht (Stichwort: Kontroll- und Transparenzgesetz, KonTraG) bereits heute als Straftatbestand geahndet werden kann.

Die EU-DSGVO schreibt das Grundrecht auf Datenschutz fest. Damit wächst nicht nur die Verantwortung, sondern auch das Haftungsrisiko – sowohl für das Unternehmen als auch für Geschäftsführer, IT-Verantwortliche und interne Datenschutzbeauftragte. Zudem drohen erhebliche Bußgeldforderungen. Die Höchstgrenze soll bei 20 Millionen Euro beziehungsweise 4 Prozent des Jahresumsatzes der betroffenen Unternehmen liegen.

Verschärfungen sieht die EU-DSGVO bei personenbezogenen Daten vor. Deren Definition ist deutlich strenger gefasst als bisher. Deshalb müssen Unternehmen letztlich nahezu alle Prozesse, Produkte, Dokumentationen und Verträge gründlich unter die Lupe nehmen und gegebenenfalls anpassen, um den gesetzlichen Anforderungen nach den Prinzipien „Privacy by Design“ und „Privacy by Default“ zu genügen. Besondere Aufmerksamkeit sollte hierbei auch den vertraglichen Vereinbarungen (Service Level Agreements/SLAs) zur Auftragsdatenverarbeitung gelten, die zwischen einem Unternehmen und dessen ITK- und Cloud-Dienstleistern bestehen.

4 | » MANAGEMENTEMPFEHLUNG

Sensibilisieren Sie sich und Ihre Mitarbeiter für wachsende Bedrohungen und Cyber Security. Als Führungskraft sollten Sie die Sicherheitsmankos der „Schwachstelle Mensch“ sowohl offensiv als auch methodisch angehen.

Laut der „Potenzialanalyse Digital Security 2017“ von Sopra Steria Consulting führen inzwischen fast alle Unternehmen mit mehr als 500 Mitarbeitern Maßnahmen zur Security Awareness für ihre Mitarbeiter durch. Aber nur knapp die Hälfte bietet dies regelmäßig allen Mitarbeitern an.

Schulungen zum Datenschutz und zur IT-Sicherheit sind wichtig: Denn neben Problemen in der vorhandenen IT-Basis und Anwendungslandschaft oder unsauber aufgesetzten Prozessen stellen nicht zuletzt die Arbeitsweisen und Gewohnheiten der Mitarbeiter ein Sicherheitsrisiko dar. Hier befinden sich in der Regel etliche Schwachstellen, die Cyber-Kriminelle aufspüren und nutzen, um ihr digitales Werkzeug in die (grundsätzlich recht gut abgesicherten) Netzwerke einzuschleusen.

Erpressungen mit Ransomware etwa, mit der Cyber-Kriminelle Daten und Anwendungen verschlüsseln und diese erst nach Zahlung eines Lösegeldes wieder freischalten, „funktionieren“ unter anderem deshalb so gut, weil viele Unternehmen kein systematisches Back-up betreiben. Für die Erpresser ist das ein lohnendes Geschäft. Eine Entschlüsselung der Blockade-Codes ist kaum möglich, der Geschäftsbetrieb muss weitergehen, und wer einmal für die „Freilassung“ seiner Daten zahlt, wird es wieder tun. Statistisch betrachtet, soll jedes vierte Unternehmen, das zum Erpressungsopfer wird, mindestens dreimal Lösegeld gezahlt haben. Ihren Weg in die Unternehmenssysteme nehmen solche und andere schädliche Codes häufig über Mitarbeiter, die E-Mail-Anhänge oder präparierte Links arglos öffnen. Die Herausforderung besteht darin, Sicherheitsbewusstsein und standardisierte Abläufe überall im Unternehmen zu verankern.

CYBER SECURITY IST GESCHÄFTSKRITISCH

Die fortschreitende Digitalisierung erfordert ganzheitliche Ansätze zur Sicherung der Unternehmensdaten, -systeme und der Schnittstellen zum IoT. Technische Sicherheitslücken und statische Abwehrkonzepte senken die Hürden für technisch versierte, flexibel agierende Hacker; mangelndes Sicherheitsbewusstsein der Mitarbeiter ermöglicht Erpressung und Betrug. Abhilfe schaffen dynamische Lösungen, die den internen und externen Datenfluss ganzheitlich überwachen und permanent auf Abweichungen hin untersuchen. Unternehmen begegnen ihren Angreifern zunehmend mit Hilfe selbstlernender Security-Technologie für die Prävention, Detektion und Reaktion.

» Nichts treibt Unternehmen weltweit mehr um als die Angst vor Betriebsunterbrechungen, wie das aktuelle Allianz Risk Barometer 2017 zeigt. Zu den gefürchtetsten Auslösern gehören nach Bränden, Naturkatastrophen und Lieferantenausfällen auch Cyber-Vorfälle. Deutsche Unternehmen halten Cyber-Vorfälle mittlerweile sogar für das größte Geschäftsrisiko. Sie sorgen sich um Angriffe von Cyber-Kriminellen, Systemausfälle oder Datenschutzverletzungen, die zu großen Verlusten führen, ohne direkte physische Schäden zu verursachen.

Im Jahr 2016 waren 42 Prozent der IT-Sicherheitsvorfälle „schwerwiegend". Zu diesem Ergebnis kommt eine aktuelle Untersuchung von PAC (Pierre Audoin Consultants). Schwerwiegend heißt, dass sich Unternehmen mit ernsthaften Störungen ihres Geschäftsbetriebes auseinandersetzen müssen, deren Beseitigung recht kostenintensiv und zeitaufwendig sein kann. Verursacher sind durchorchestrierte und gezielte Angriffe wie APT (Advanced Persistent Threats) oder „Distributed Denial of Service (DDoS)"-Attacken, immer häufiger aber auch der Einsatz marktüblicher Ransomware, die betriebswichtige Daten verschlüsselt und blockiert.

Großangriffe auf Netzbetreiber, Service Provider und Cloud-Plattformen mehren sich ebenso wie individuelle Attacken auf Kritische Infrastrukturen. Die Vermeidung von IT-Ausfällen und die Absicherung der Netze betreffen also nicht nur einzelne Unternehmen, sondern werden zu einer Frage der nationalen Sicherheit. Die aktuelle Cyber-Sicherheitsstrategie der Bundesregierung enthält über 30 strategische Ziele und Maßnahmen, die die Sicherheit erhöhen und das Risiko von Cyber-Kriminalität, -Spionage und -Terrorismus verringern sollen.

Erpressung und Betrug durch Cyber-Kriminelle nehmen zu

Nach Angaben des Cyber-Allianz-Zentrums Bayern (CAZ) im Bayerischen Landesamt für Verfassungsschutz dauert es durchschnittlich 260 Tage, bis ein diskreter Angriff entdeckt wird. Mindestens so lange also werden Unternehmen unsichere Schnittstellen zum Internet betreiben, selbst wenn es sich um eigentlich bekannte Schwachstellen handelt. Dazu gehören etwa SCADA-Systeme in der Industrie, wenn sie mit einem fehlerhaft implementierten Internetprotokoll (TCP/IP) arbeiten. Bis 2020 werden mehr als 25 Prozent der Cyber-Angriffe auf Unternehmen in Zusammenhang mit dem Internet der Dinge (Internet of Things, IoT) stehen. Diese Prognose der Analysten bei Gartner wird sich aller Voraussicht nach als deutlich zu niedrig erweisen. Für viele Experten steht fest, dass Angriffe mit IoT-Botnetzen und Ransomware zunehmen und das „Geschäftsmodell Erpressung" lukrativ bleiben wird.

Anbieter von Security-Software wie Bitdefender und Kaspersky schätzen, dass Kriminelle künftig verstärkt auf automatisiertes Targeting setzen, um noch gezielter anzugreifen und höhere Lösegelder zu erpressen. Mehr Umsatz verspricht auch die Betrugsmasche des falschen Chefs, auch bekannt als Fake President, CEO Fraud oder BEC Fraud. Für Kriminelle ist diese Betrugsmethode sehr attraktiv, auch weil sie kaum technisches Know-how erfordert. Es genügen Recherchen (Wer arbeitet in der Buchhaltung? Wer darf oder könnte Überweisungen tätigen?) und Social Engineering (Ausspähen der Zielpersonen und ihrer Verhaltensweisen in sozialen Medien und eine entsprechend angepasste Ansprache). Weder müssen Codes programmiert noch Sicherheitsvorkehrungen der Unternehmen umgangen noch Angriffswellen administriert werden. Meist reicht eine E-Mail mit vorgetäuschtem Absender und der dringenden Bitte, eine Zahlungsanweisung vorzunehmen. Ist all dies in einem Tonfall formuliert, der Mitarbeiter als Vertrauens- und Geheimnisträger adressiert, fallen gerade in traditionell hierarchisch organisierten Unternehmen die Misstrauensschranken. Schätzungen gehen davon aus, dass Cyber-Kriminelle mit dieser Vorgehensweise im laufenden Jahr noch mehr Schaden für Unternehmen anrichten werden als mit Ransomware.

Umfassende Bedrohungslage

Politisch und ideologisch motivierte Angriffe mit APT-Techniken werden weiter zunehmen. Darin sind sich Bundesbehörden wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) und Experten der IT-Security-Branche einig. Konsens besteht auch darüber, dass der Hauptantrieb durchschnittlicher Cyber-Krimineller reine Geldgier ist. Sie führt zu immer neuen Techniken, flexibler Taktik und richtet sich an aktuell besonders erfolgversprechenden (sprich: angreifbaren) Zielgruppen aus.

Zwar waren zuletzt verstärkt Krankenhäuser und andere medizinische Einrichtungen betroffen. Doch nach wie vor steht die Finanzbranche im Fokus krimineller Hacker. „Neben den etablierten Angriffsmethoden wie Ransomware werden auch unstrukturierte Daten zunehmend attraktiv", beobachtet Christian Nern, Head of Security

Software DACH bei IBM Deutschland. „E-Mail-Archive, Geschäftsdokumente, gestohlenes geistiges Eigentum oder Quellcodes eröffnen Kriminellen neue Möglichkeiten, etwa für den Insiderhandel, und setzen Unternehmen weiter unter Druck."

Professionelle Hackergruppen gehen immer raffinierter, komplexer und immer flexibler vor, wenn es darum geht, Spuren zu verwischen. Zudem steigt die Zahl von Erpressungen durch Kleinkriminelle, die Schadsoftware einfach im mittlerweile gut organisierten Markt erwerben. „Die Bedrohungslandschaft gezielter Attacken verändert sich laufend, und die Angreifer sind immer besser vorbereitet, um neue Lücken und Gelegenheiten aufzuspüren und auszunutzen", erläutert Juan Andres Guerrero-Saade, Senior Security Researcher bei Kaspersky Lab. Wie er beobachten viele Experten aktuell einen erhöhten Bedarf an Speicherforensik und an Vorfallreaktionen (Incident Response) gegen dateilose Malware-Attacken, bei denen Angreifer keine Spuren, etwa in Form von Trojaner-Dateien auf dem PC, hinterlassen und auch keine Tools zum Abgreifen von Daten oder Kommunikation nutzen. Stattdessen erfolgt der Einbruch über Skripte in der Registry, das heißt über Einträge in der Datenbank, in der die Einstellungen und andere Konfigurationsdaten des Betriebssystems gespeichert sind. Antiviren-Software und auch viele Forensik-Tools setzen aber vor allem auf die Analyse von Dateien und greifen daher in solchen Fällen nicht.

Technik allein reicht nicht zur Abwehr

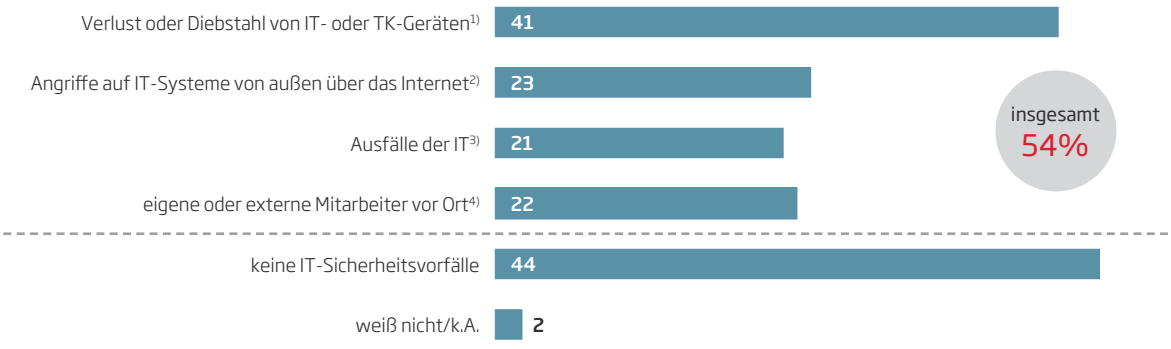
Doch die Erkennung und die Analyse von Sicherheitsvorfällen werden immer zuverlässiger. Das zeigt etwa der IBM X-Force Report 2017. Demnach ist die Anzahl von IT-Sicherheitsvorfällen, die intensive Untersuchungen im Nachgang erfordern, im Jahr 2016 um 48 Prozent gesunken. So wachse das Bewusstsein für Cyber-Bedrohungen, und damit stiegen auch die Aufwendungen für kognitive Analysen und selbstlernende Vorsorgesysteme sowie für Incident-Response-Pläne.

Laut PAC wollen Unternehmen in diesem Jahr größere Teile ihres Security-Budgets in den Bereich Incidence Response verschieben, um nach Angriffen nicht länger nur zu improvisieren. Konkrete Investitionspläne gibt es auch für leistungsstarke Frühwarn- und Erkennungssysteme und das Risiko- beziehungsweise Notfallmanagement. Experten sprechen in diesem Zusammenhang von einem Dreiklang aus Prävention, Detektion und Reaktion.

Mit technischen Mitteln allein werden sich Unternehmen jedoch nicht nachhaltig gegen die Energie der Cyber-Kriminellen schützen können. Je symbiotischer die Verbindung zwischen Menschen und ITK-Technologie wird und je mehr die Vernetzung von Maschinen und Prozessen zu wechselseitigen Abhängigkeiten führt,

MEHR ALS DIE HÄLFTE DER UNTERNEHMEN VERZEICHNET IT-VORFÄLLE

Ursachen für IT-Sicherheitsvorfälle in den vergangenen 24 Monaten, in Prozent der Befragten

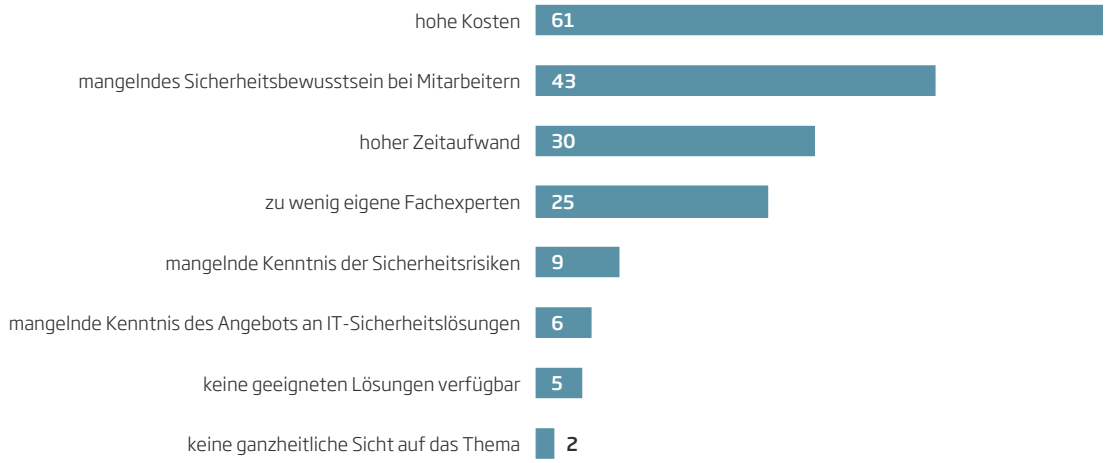


1) z.B. Datenträger, PC, Laptop, Handy, Smartphone oder Tablet
2) z.B. gezielter Online-Einbruch in die IT-Systeme, DDoS-Attacken
3) z.B. durch höhere Gewalt wie Stromausfälle oder durch Sabotage
4) z.B. Einschleusen eines Virus über USB-Stick
n = 556 (Mehrfachnennungen)

Quelle: Bundesdruckerei/Bitkom

HOHE KOSTEN STEHEN VERBESSERTER IT-SICHERHEIT ENTGEGEN

Hürden bei der Gewährleistung bzw. Verbesserung der IT-Sicherheit, in Prozent der Befragten



n = 556 (Mehrfachnennungen)

Quelle: Bundesdruckerei/Bitkom

desto zahlreicher werden die Angriffsflächen. Dabei ist der Mensch eine der größten Gefahrenquellen.

Striktes Identitäts- und Zugriffsmanagement hilft dabei, dass sensible Daten nicht in unbefugte Hände gelangen. Mitarbeiter, die sorglos mit Zugriffsprivilegien umgehen oder arglos digital kommunizieren, sind ein Sicherheitsrisiko, das sich künftig kein Unternehmen mehr leisten kann. Die Sensibilisierung für Cyber-Gefahren und gezielte Sicherheitsschulungen stehen daher 2017 weit oben auf der Prioritätenliste der Unternehmensentscheider, berichten der Bitkom und die Allianz für Cyber-Sicherheit.

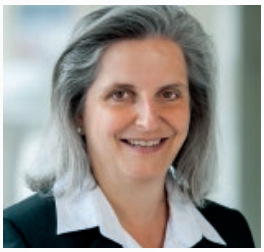
Managed Security Services sind gefragt

Unternehmen sollten schnellstmöglich dazu übergehen, Sicherheitslösungen einzusetzen, die Anomalien im Netzwerk über alle Ebenen und Instanzen aufspüren können. Die Herausforderung besteht darin, Strukturen für die Früherkennung, Risikominimierung und Abwehr zu etablieren und wirksam auszurichten. Dem stehen oftmals nicht nur hohe Kosten entgegen, sondern auch der anhaltende Mangel an qualifiziertem Fachpersonal.

Mit der Einsicht in den eigenen Nachholbedarf steigt in den Unternehmen das Interesse an externer Unterstützung. Sogenannte Managed Security Services (MSS) bieten zahlreiche Vorteile:

- Monitoring und Analyse rund um die Uhr (24/7)
- zeitnahe Angriffsabwehr mit den jeweils fortschrittlichsten Methoden und Tools
- dynamische Lösungen, auch für System-Logging und Datenforensik
- skalierbarer Leistungsumfang nach Bedarf
- keine Kapitalbindung durch Investitionen
- planbare Kosten bei gleichzeitiger Flexibilität
- Entlastung der eigenen IT

Zudem können spezialisierte Dienstleister bei Bedarf das gesamte IT-Sicherheitsmanagement übernehmen. Vertrauen und umfassende, rechtskonforme Serviceverträge (Service Level Agreements, SLAs) vorausgesetzt, sehen nicht nur kleinere Unternehmen ohne eigene IT-Abteilung die MSS als sinnvollen Weg zu einer höheren Cyber Security. «



Jacqueline Preußer
ist Redakteurin im F.A.Z.-Institut.

IT-SECURITY: STRATEGIEN GEFRAGT

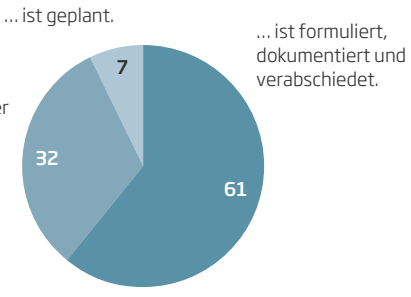
Sopra Steria Consulting hat im Rahmen der „Potenzialanalyse Digital Security 2017" IT-Entscheider aus Unternehmen ab 500 Mitarbeitern zu ihren digitalen Sicherheitsstrategien und konkreten Maßnahmen befragt. Hier präsentieren wir Ihnen einige zentrale Ergebnisse.

» Mit der fortlaufenden Digitalisierung der Wirtschaft gehen umfangreiche neue Herausforderungen für die digitale Sicherheit der Unternehmen einher. Die hohe Relevanz strategischer Überlegungen hinsichtlich IT-Sicherheit ist angekommen: Kein befragtes Unternehmen sagt: „Wir haben keine IT-Sicherheitsstrategie und planen auch keine." Zu diesem Ergebnis kommt die Studie „Potenzialanalyse Digital Security 2017", für die Sopra Steria Consulting im April 2017 in einer Online-Erhebung 205 IT-Entscheider befragen ließ. Sechs von zehn Unternehmen folgen heute schon einer aktuellen IT-Sicherheitsstrategie (61 Prozent). Weitere 32 Prozent arbeiten derzeit an einer eigenen IT-Sicherheitsstrategie, bei 7 Prozent der Unternehmen befindet sie sich zumindest in der Planung. Trotzdem sind immerhin 73 Prozent der befragten IT-Entscheider der Meinung, dass viele Unternehmen beim Schutz gegen Cyber-Angriffe noch zu wenig Initiative zeigten – digitale Sorglosigkeit sei weitverbreitet. Vor allem Vorstände und Geschäftsführer verharmlosen aus ihrer Sicht die Gefahr von Cyber-Angriffen.

IT-SICHERHEITSSTRATEGIEN FINDEN SICH BEREITS IN SECHS VON ZEHN UNTERNEHMEN

Verbreitung von eigenständigen IT-Sicherheitsstrategien in Unternehmen; in Prozent der befragten IT-Entscheider

Eine IT-Sicherheitsstrategie ...



Basis: alle Befragten, n = 205 (Einfachnennung)

Quelle: Potenzialanalyse Digital Security 2017 (Sopra Steria Consulting)

Einfallstor digitale Plattformen

Unternehmen sind heute weitreichend elektronisch vernetzt. Knapp 70 Prozent der befragten Unternehmen sind mit ihren Lieferanten und Dienstleistern über digitale Plattformen oder Softwarelösungen verbunden. Bereits mehr als die Hälfte der Unternehmen pflegt auch mit Kunden einen direkten elektronischen Austausch.

Insbesondere im elektronischen Austausch mit Lieferanten und Dienstleistern sind besondere IT-Sicherheitsvorkehrungen wichtig. Wichtige Informationen werden transferiert, ein Zugang zum unternehmenseigenen Netzwerk ist abzusichern.

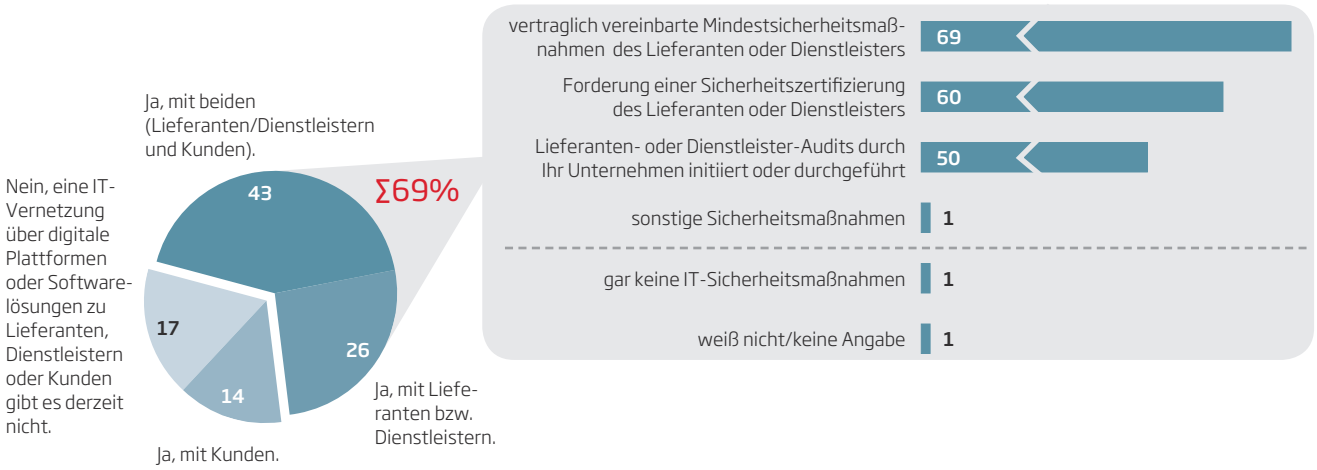
Zahlreiche Unternehmen sorgen entsprechend vor. Sieben von zehn befragten Unternehmen vereinbaren per Vertrag Mindestsicherheitsmaßnahmen des Lieferanten oder Dienstleisters, sechs von zehn fordern eine Sicherheitszertifizierung des Partners. Die Hälfte der Unternehmen initiiert Lieferanten- und Dienstleister-Audits, die sie dann auch durchführen. Vor allem Finanzdienstleister wählen diesen Weg überdurchschnittlich oft.

Mitarbeiter mitnehmen

Eine Schwachstelle in der IT-Sicherheit in allen Unternehmen sind die Mitarbeiter. Wenn der korrekte, sicher-

UNTERNEHMEN SIND HEUTE VIELFÄLTIG ELEKTRONISCH VERNETZT

Vernetzung mit Kunden und Lieferanten sowie IT-Sicherheitsmaßnahmen im Rahmen der IT-Vernetzung mit Lieferanten und Dienstleistern, in Prozent der Befragten



Basis: alle Befragten, n = 205 (Mehrfachnennungen)

Quelle: Potenzialanalyse Digital Security 2017 (Sopra Steria Consulting)

heitsorientierte Umgang mit digitalen Kanälen nicht vermittelt wird, nützen die sichersten Systeme nichts. Bei jedem einzelnen Mitarbeiter ist ein Mindestmaß an Security Awareness – also ein Bewusstsein für Informationssicherheitsaspekte – notwendig.

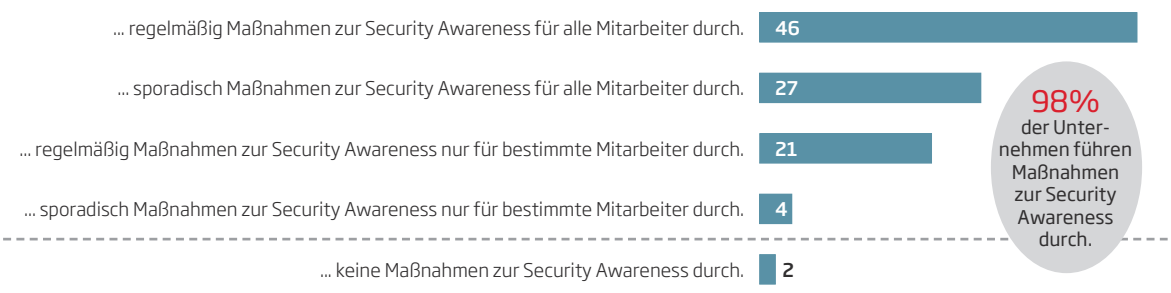
Mittlerweile führen fast alle Unternehmen Maßnahmen zur Security Awareness durch (98 Prozent). Allerdings sind es weniger als die Hälfte der Unternehmen, die dies tatsächlich regelmäßig für alle Mitarbeiter tun. Etwas mehr als ein Viertel hingegen schult nur sporadisch. 21 Prozent hingegen schulen zwar regelmäßig, aber nur bestimmte Mitarbeiter.

Gut die Hälfte der Unternehmen, die ihre Mitarbeiter schulen, hat sich dafür entschieden, die Maßnahmen auf die unterschiedlichen Rollen und Aufgaben der Mitarbeiter zuzuschneiden und entsprechend differenzierte Angebote zu machen. «

MITARBEITER WERDEN NICHT IMMER AUSREICHEND GESCHULT

Form der Security Awareness; im Prozent der befragten IT-Entscheider

Wir führen ...



Basis: alle Befragten, n = 205 (Mehrfachnennungen)

Quelle: Potenzialanalyse Digital Security 2017 (Sopra Steria Consulting)

DIGITALE SCHATTENWIRTSCHAFT: VON SPIONAGE BIS ZU DATENKLAU

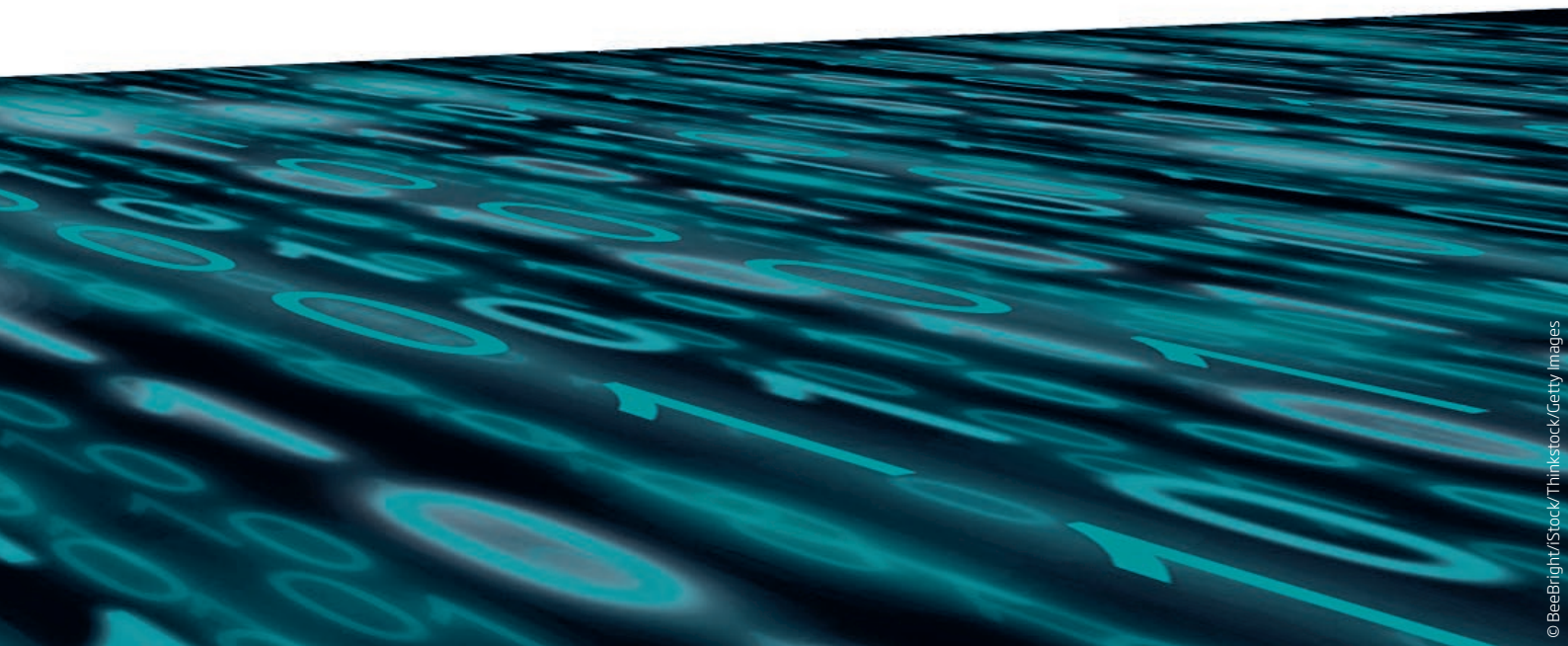
Die Cyber-Kriminalität hat sich in den vergangenen Jahren professionalisiert. Waren es anfangs einzelne Hacker, handelt es sich mittlerweile um ein globales Phänomen, das sich auf eine weitverzweigte Infrastruktur stützt und arbeitsteilig organisiert ist. Die finanziellen Interessen und die damit verbundene Wertschöpfung sind enorm. Dem Gefühl der Machtlosigkeit gilt es mit Wissen und mehr Prävention beizukommen.

» Die Cyber-Kriminalität umgibt in der öffentlichen Diskussion stets eine Aura des Geheimnisvollen und Konspirativen. Immer wieder ist von „Hackern" die Rede, die in „rechtsfreien Räumen" agierten. Die wahre Bedrohungslage ist jedoch diffus und trotz – oder vielleicht wegen – der Dauerberichterstattung schwer einzuschätzen. Doch wo liegen die wirklichen Probleme? Bei der Antwort auf diese Frage liegt der Fokus im Folgenden speziell auf Kriminalität, die gegen Computersysteme gerichtet ist und von der vor allem Unternehmen und Behörden betroffen sind.

Die Entwicklung der Cyber-Kriminalität ist eng verbunden mit der Entwicklung vernetzter Computersysteme, insbesondere des Internets, das als Netzwerk von Forschern und Freaks entstand. Spätestens seit Mitte der 1990er Jahre haben im Internet jedoch finanzielle und kommerzielle Interessen zunehmend an Bedeutung gewonnen. Infolgedessen bleibt auch der Cyberspace nicht verschont von Kriminalität. Waren es anfangs nur vereinzelte und eher „ethisch motivierte" Hacker, dominiert heute eine finanziell motivierte, arbeitsteilige und professionelle Kriminalität den Cyberspace.

Arbeitsteilung und hoher Organisationsgrad

In der Literatur sind der hohe Grad an Organisation und eine ausdifferenzierte Arbeitsteilung der Schattenwirtschaft sehr gut dokumentiert. Die Arbeitsteilung manifestiert sich in einem raffinierten Organisationskreislauf, an dessen Ausgangspunkt die Arbeit von technischen



Experten (den „Hackern") steht, die fremde Systeme erfolgreich angreifen können.

Die Vorgehensweise der Szene hat sich in den vergangenen beiden Jahrzehnten grundlegend verändert: Während bis zur Jahrtausendwende das Angreifen von Systemen häufig noch händisch erfolgte, sind die meisten Vorgänge heute mittels Software hochgradig automatisiert. Im Ergebnis können bei Vorliegen einer entsprechenden Schwachstelle deutlich mehr Systeme erfolgreich angegriffen werden als früher.

Aufgrund der Komplexität der Aufgabenstellung ist die Arbeitsteilung in diesem Bereich besonders weit fortgeschritten. So gibt es Spezialisten, die sich ausschließlich mit der Suche nach Schwachstellen in bestimmten Systemen (Betriebssystemen, Anwendungssoftware, Smartphones etc.) beschäftigen. Das Ergebnis ist dann meist ein sogenannter Exploit, also eine Beschreibung der Schwachstelle mitsamt einem kleinen Programm, das den Angriff ausführt und damit dessen Erfolg dokumentiert. Exploits sind daher der eigentliche „Rohstoff" der digitalen Schattenwirtschaft.

Botnetze sind universelle Plattformen für nahezu jede Art bösartiger Aktivitäten im Internet.

Exploits werden anschließend zur eigentlichen Schadsoftware (engl. Malware) weiterverarbeitet. Dies geschieht auf verschiedene Arten. In der Regel muss ein Exploit verfeinert werden, damit er mit höherer Wahrscheinlichkeit und auf einer größeren Menge von IT-Systemen funktioniert. Anschließend bauen andere Spezialisten den Exploit in Werkzeuge ein, die damit beispielsweise automatisiert und großflächig Systeme angreifen können. Andere Spezialisten wiederum setzen den Exploit ein, um zielgerichtet eine bestimmte, sehr kleine Anzahl von Systemen anzugreifen (gezielte Angriffe).

Weiter gibt es Akteure, die für den Vertrieb von Schadsoftware zuständig sind. Diese bieten die Schadsoftware selbst sowie dazugehörige Dienstleistungen auf entsprechenden Internetforen zum Kauf an. Zu den Diensten gehören etwa die Erstellung von Schadsoftware für bestimmte Zwecke (Spionage, Erpressung etc.) oder deren Härtung gegen bekannte Antivirenprodukte. Im Preis inbegriffen ist meist ein professioneller „Support" mit einer 24-stündigen Erreichbarkeit via Internet.

Botnetze ermöglichen die Verbreitung

Die massive Verbreitung von Schadsoftware mit einer einheitlichen Möglichkeit der Fernsteuerung führt wiederum zu neuen Geschäftsformen. Die Infrastruktur liefern dabei die sogenannten Botnetze. Ein Botnetz besteht aus einer Menge von aktiven Schadsoftware-Exemplaren (den Bots), die über das Internet überwacht und ferngesteuert werden können. Botnetze sind daher universelle Plattformen für nahezu jede Art bösartiger Aktivitäten im Internet. Mit ihnen kann man den Effekt der Schadfunktion von einem infizierten Rechner auf Tausende Rechner ausdehnen. Dies führt zu einer neuen Qualität der durchgeführten Aktivitäten, etwa dem Spam-Versand oder dem massenhaften Keylogging. Erst durch Botnetze werden auch verteilte Überlastungsangriffe auf einzelne Rechner oder die Internetinfrastruktur als Ganzes möglich.

Neue Formen der Wertschöpfung

Wertschöpfung erfolgt immer dann, wenn illegale Aktivitäten im Cyberspace zu einem wirtschaftlichen Vorteil in der realen Welt führen. Da ein Großteil der heutigen Cyber-Kriminalität von finanziellen Interessen getrieben zu sein scheint – ob nun in Form von Spionage, Datenklau oder Erpressungsversuchen –, ist die Frage der Wertschöpfung von ganz entscheidender Bedeutung.

Bei den Wertschöpfungsprozessen kann man unterscheiden zwischen Aktivitäten, die eine direkte Analogie in der realen Welt haben, und neuartigen Geschäftsideen, die ohne vernetzte Informationstechnik nicht denkbar sind. Hierzu zählen etwa der Versand von „klassischem" Spam, also Werbebotschaften für online bestellbare Produkte, aber auch neue Erpressungsmaschen, wie elektronische Schutzgelderpressungen. Dies sind Geldforderungen gegen Online-Dienste (wie Online-Wettanbieter) bei gleichzeitiger Drohung, deren Webpräsenz durch einen Überlastungsangriff massiv zu stören. Zuletzt sind auch viele Unternehmen, Behörden und Privatleute Opfer von sogenannten Erpressungstrojanern geworden, die Daten auf infizierten Systemen verschlüsseln und nur gegen die Zahlung eines Geldbetrages wieder zugänglich machen.

Die Monetarisierung von Informationen aus gezielten Angriffen wird zudem immer perfider. Wo vor Jahren noch Geld verdient wurde mit dem Verkauf von Geschäftsgeheimnissen im Rahmen von Spionageaktivitäten, versucht man heute, unter einem Vorwand

durch die gezielte Beeinflussung einzelner Personen hohe Geldbeträge ins Ausland überweisen zu lassen Mit dem „CEO Fraud" ist der klassische Enkeltrick im 21. Jahrhundert angekommen.

Im Rahmen von Botnetzen sind jedoch auch andere und neuartige Wertschöpfungsprozesse möglich, die bis vor kurzem nur schwer vorstellbar waren. Sie zielen auf die Monetarisierung von Daten, die in großer Menge durch Keylogger gesammelt werden. Wertvoll sind beispielsweise Kreditkartendaten und Zugangsinformationen (Kennung und Passwort) zu diversen Online-Diensten oder Zugangsdaten zu Online-Rollenspielen.

Weitverzweigte Infrastruktur

Im Hintergrund steht eine Infrastruktur, die den Kreislauf der digitalen Schattenwirtschaft duldet oder sich mit ihm arrangiert hat. Entgegen einer häufig geäußerten Meinung gibt es keinerlei wissenschaftliche Belege dafür, dass es engere Verbindungen zwischen der traditionellen organisierten Kriminalität (etwa im Bereich Drogen- oder Menschenhandel) und den Infrastrukturanbietern für die digitale Schattenwirtschaft gibt.

Zur Infrastruktur gehören erstens Staaten, die Cyber-Kriminalität rechtlich oder faktisch nur unzureichend verfolgen und hieraus durchaus auch kurzfristige wirtschaftliche Vorteile ziehen können. Zweitens sind hierzu die bereits genannten anonymen Zahlungsdienste zu zählen, die eine Nachverfolgung der wirtschaftlichen Ströme zumindest deutlich erschweren.

Schließlich und drittens benötigt man aber auch immer eine Reihe willfähriger Internet-Service-Provider, die die Strafverfolgungsbehörden nicht unterstützen und denen das Benehmen ihrer Kunden egal ist, sofern diese nur pünktlich ihre Rechnungen bezahlen. Sie sind somit direkte Nutznießer der digitalen Schattenwirtschaft.

Zu den Angeboten derartiger Provider zählen auch schnelle Änderungen bei der Namensauflösung durch den Namensdienst DNS. Diese werden für sogenannte Fast-Flux-Netzwerke benötigt, eine besonders raffinierte Verschleierungstechnik von Botnetzen. Hierbei wird das Botnetz selbst als eine Art Anonymisierungsdienst genutzt, indem Kommunikationsverbindungen zwischen dem Angreifer und den Bots über mehrere Zwischenstationen innerhalb des Botnetzes weitergeleitet werden.

Das Fehlen verlässlicher Zahlen

Zur politischen Einschätzung des Risikos von Cyber-Kriminalität ist es notwendig, zwischen potenziellen Schäden und wirklichen Schäden zu unterscheiden. Werden die potenziellen Schäden mit den wirklichen Schäden verwechselt, verlangt die öffentliche Meinung schnell nach einer Kontrolle und Überwachung durch den Staat und entscheidet sich damit gegen grundlegende Freiheitsrechte der Bürger. Helfen können hier nur verlässliche empirische Daten. Solche Daten fehlen aber leider weitestgehend.

Aus der Unsicherheit gegenüber Cyber-Kriminalität heraus entsteht eine individuell, politisch und gesellschaftlich gefühlte Machtlosigkeit. Das drängendste Problem ist die unzureichende Kenntnis, die unzureichende kriminologische Erforschung der Cyber-Kriminalität. Dieses Dunkelfeld gilt es aufzuhellen, denn anekdotisches Wissen über Cyber-Kriminalität und über mutmaßliche Erfolge einzelner Ermittlungsmethoden reicht nicht aus, um angemessen auf Cyber-Kriminalität zu reagieren.

Zusammenfassung: Mit Macht gegen die Ohnmacht

Erste Studien zeigen, dass unsere moderne Gesellschaft extrem ineffizient in der Bekämpfung von Cyber-Kriminalität ist: Cyber-Kriminelle bürden der Gesellschaft mit geringem eigenem Aufwand unverhältnismäßig hohe Kosten auf. Die Gründe dafür sind teilweise bekannt, etwa die Tatsache, dass Cyber-Kriminalität inhärent global agiert. Die gesellschaftlichen Kosten entstehen aber auch durch hohe Investitionen in Sicherheitstechnologien (wie Antivirenprogramme oder Firewalls), die sich zunehmend als unwirksam erweisen.

Eine Schlussfolgerung ist demnach, dass wir stärker in die nichttechnische Prävention (Schulung von Mitarbeitern; professionelle Computer Emergency Response Teams, sogenannte CERTs) und die konkrete Strafverfolgung investieren sollten, um das Ergreifungsrisiko zu erhöhen. Denn weder ist Cyber-Kriminalität ein rein technisches Problem, noch sind wir machtlos bei ihrer Bekämpfung. «

Prof. Dr.-Ing. Felix Freiling
ist Inhaber des Lehrstuhls für IT-Sicherheitsinfrastrukturen an der Friedrich-Alexander-Universität Erlangen-Nürnberg.

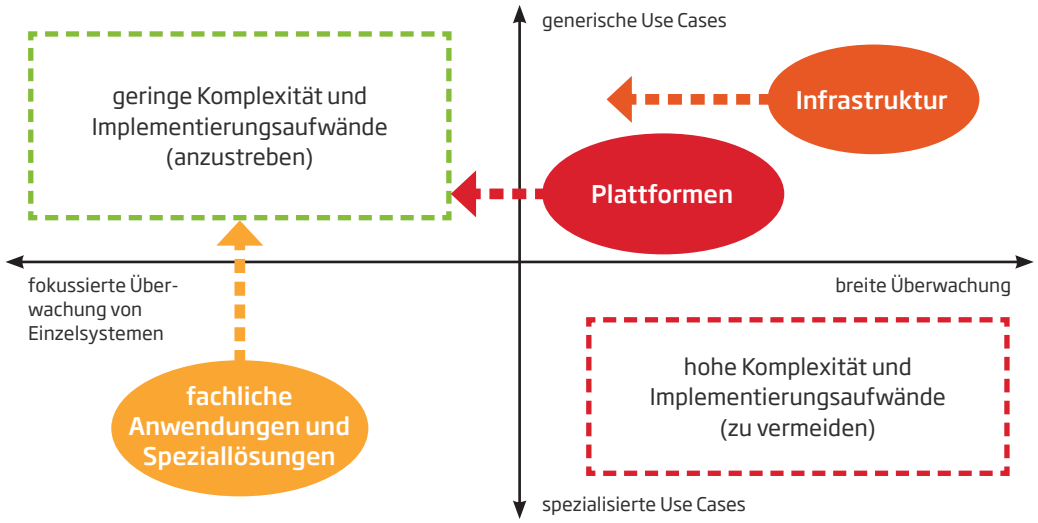
MIT SIEM FOR BUSINESS
ANGRIFFE GEZIELT AUFHALTEN

Mit einem Security Information and Event Management (SIEM) haben Unternehmen ihre IT-Sicherheit im Blick. Doch ein solches SIEM muss sorgfältig ausgestaltet sein, damit Risiken angemessen adressiert werden und sich gleichzeitig Komplexität und Investitionskosten im Rahmen halten.

» Vertrauliche Informationen und die Funktionalitäten von Anwendungen der Unternehmens-IT stellen für Angreifer attraktive Ziele dar. Spionage und Sabotage erfolgen immer häufiger über IT-Systeme. Und der tägliche Blick in die Nachrichten verrät: Unternehmen haben dringenden Handlungsbedarf! Da inzwischen praktisch alle Prozesse IT-gestützt ablaufen und oft eine Kommunikation mit Kunden, externen Partnern und deren Infrastruktur erfordern, sind Anwendungen und IT-Systeme zwangsläufig mit öffentlichen Netzen verbunden. Ebenso kann bei noch so stringenter Vergabe von Berechtigungen ein Missbrauch durch Innentäter nie vollständig ausgeschlossen werden. Daher müssen IT-Systeme und deren Daten gegenüber böswilligen, oft kriminellen Handlungen wirksam geschützt werden. Die Schutzmaßnahmen gliedern sich in:

» **Prävention:** Verminderung oder Vermeidung der Risiken durch Angriffe
» **Detektion:** zuverlässige und zeitnahe Identifikation von Angriffen

ZIEL: VERMEIDUNG VON KOMPLEXITÄTS- UND AUFWANDSTREIBERN



Quelle: Sopra Steria Consulting

» **Reaktion:** Maßnahmen, die Schäden durch Angriffe begrenzen oder beseitigen

Eine besondere Bedeutung erhält vor allem die automatisierte Detektion von Angriffen, basierend auf Protokolldaten von Anwendungen, Infrastruktur und Netzwerkkomponenten – auch bezeichnet als Security Information and Event Management (SIEM).

Schadenspotenzial ermitteln

Die Analyse der unternehmensspezifischen Risikolage ist die Grundlage für praktisch jedes SIEM-Vorhaben. Daneben ist die Definition des Überwachungsbereichs und des Detektionsgegenstands (das heißt der zu überwachenden Ereignisse) eine wesentliche Voraussetzung für ein wirkungsvolles SIEM. Zum einen müssen alle IT-Systeme hinsichtlich der Möglichkeit, dass sie als Tatwaffe oder Ziel eines Cyber-Angriffs dienen können, bewertet werden. Zum anderen sind Angriffsszenarien möglichst vollständig zu erheben und daraus Methoden abzuleiten, wie diese mit zur Verfügung stehenden (Protokoll-)Daten erkannt werden können.

Zum Überwachungsbereich gehören alle Systeme mit einem großen Schadenspotenzial für das Unternehmen. In der Praxis erfordert dies eine Bewertung des Schutzbedarfs verfügbarer Informationen, der Kritikalität des Systems für das Unternehmen sowie der vorhandenen Kompetenzspielräume, die durch betrügerische Handlungen ausgenutzt werden können. Risiken sind in einer Risikoanalyse zu dokumentieren. Schützenswerte und für Angreifer attraktive Ziele sind regelmäßig Sicherheitssysteme, Datenbanken, wie zum Beispiel (Kunden-)Stammdatensysteme, interne Netzwerke oder kritische Anwendungen.

Zur Bestimmung des Detektionsgegenstands müssen mögliche Angriffsszenarien umfassend erhoben werden. Aus diesem Inventar sind die einzelnen Handlungen eines Angriffsszenarios abzuleiten und in Form eines Use-Case-Katalogs zu dokumentieren. Folgende drei Kategorien sind üblich:

» generische Use Cases (zum Beispiel Brute-Force-Angriff)
» komponentenspezifische Use Cases (zum Beispiel Verbindung von Datenbanken in nichtvertrauenswürdige Netzwerkbereiche)
» systemindividuelle Use Cases (zum Beispiel Manipulation des Zahlungsverkehrssystems, wie 2016 bei der Bangladesh Bank)

Überwachung priorisieren und fokussieren

Mit dem zunehmend spezialisierten Einsatz eines Systems ist der Detektionsgegenstand genauer an das überwachte System anzupassen, wobei eine Basisüberwachung durch eher generische Komponenten (zum Beispiel Infrastruktursysteme) hergestellt wird. Je breiter der Überwachungsbereich und je spezialisierter der Detektionsgegenstand, desto mehr Aufwand entsteht. Um die Projekte wirklich umsetzen und die Risiken wie angestrebt reduzieren zu können, ist daher eine breite Überwachung sehr spezialisierter Use Cases zu vermeiden (siehe Abbildung Seite 16).

Der Angriff auf die SWIFT-Software der Zentralbank von Bangladesch 2016 zeigt deutlich, dass durch eine Über-

wachung fachlicher Anwendungen und Infrastrukturkomponenten Schäden hätten begrenzt werden können. Die Herausforderung für Unternehmen liegt darin, aus häufig Tausenden Systemen – vom Speiseplan über Firewalls bis hin zur Finanzbuchhaltung – einen Überwachungsbereich zu selektieren, der ein risikobasiertes Monitoring ermöglicht.

Für diese Selektion sind im Unternehmen bestehende Gefahrenkataloge und Risikobewertungen heranzuziehen und deren Relevanz für die IT zu bewerten. Neben systemspezifischen Sicherheitsbetrachtungen bieten sich daher insbesondere OpRisk-Kataloge, Compliance-Gefährdungsanalysen, Betrugsfalldatenbanken oder das Business Continuity Management an. Im Ergebnis muss ein Kriterienkatalog ermöglichen, jedes System – inklusive seiner Komponenten, Umgebungen und Instanzen – hinsichtlich der Aufnahme in den Überwachungsbereich zu bewerten.

Auch die Ableitung geeigneter Use Cases muss zwingend aus einer Risikosicht erfolgen. Für alle Anwendungen im Überwachungsbereich sind daher mittels Risikoanalysen die relevanten Bedrohungen zu bewerten. Ebenso gilt hier, dass mit zunehmend spezialisiertem Einsatz eines Systems die Risikoanalyse spezifischer auf einzelne Systeme abgestimmt werden muss.

Um einen hinreichenden Abdeckungsgrad zu erreichen, sollte ein möglichst passgenauer Bedrohungskatalog erstellt werden. Zusätzlich zu den genannten Quellen können die IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder Sicherheitsdokumentationen der Softwarehersteller genutzt werden.

In der Praxis zeigt sich, dass bereits in dieser Konzeptionsphase eine sehr spezifische und konkrete Beschreibung von Überwachungsmaßnahmen als Use Cases eine hohe Ergebnisqualität impliziert. Ausgelöste SIEM-Regeln können daher deutliche Hinweise auf Betrug aufzeigen. Neben langfristig signifikant niedrigeren Aufwänden in der Bearbeitung von Prüfergebnissen (insbesondere durch die Reduktion von False Positives) erhält ein SIEM dadurch einen präventiven Charakter, um Schäden zu verhindern.

Stufenweises Vorgehen unabdingbar

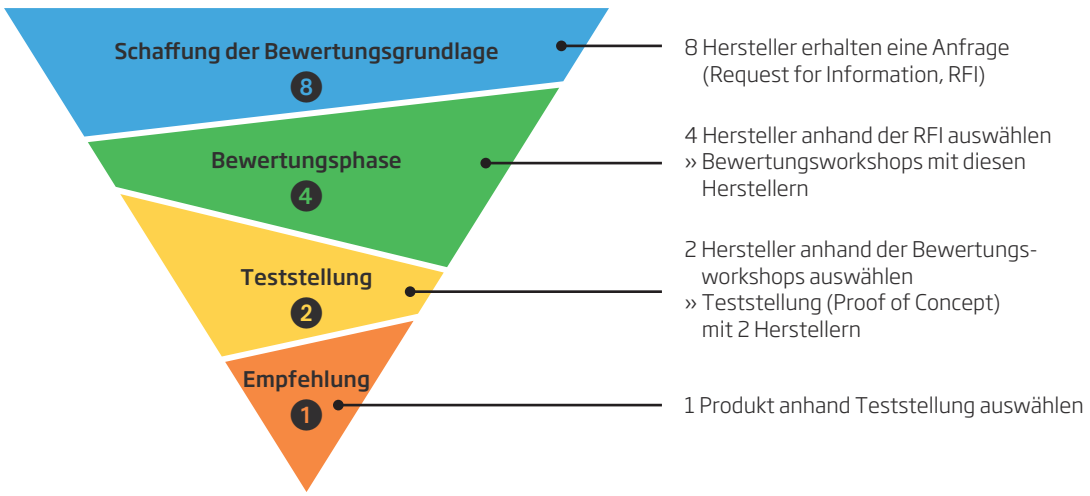
Ein SIEM-Projekt ist aufgrund der Schnittstellen zu praktisch allen Organisationsbereichen ein aufwendiges Vorhaben und kann nur phasenweise implementiert werden. Die einzelnen Phasen sollten sich am Überwachungsbereich der in das SIEM zu integrierenden Systeme orientieren:

Phase 1: Vorprojekt und Marktanfrage

Zunächst müssen die Ausgangslage und Anforderungen für die nachfolgenden Phasen bestimmt werden. Eine Ist-Analyse stellt folgende Informationen zusammen:

» externe Anforderungen hinsichtlich der Kontrolle und der Entdeckung des Missbrauchs von IT-Systemen

8-4-2-1-METHODE ZUR PRODUKT- ODER DIENSTLEISTERAUSWAHL



Quelle: Sopra Steria Consulting

» Sicherheitsleitlinien, Bedrohungsanalysen oder bekannte Schwachstellen
» (Security) Incident Management und Eskalationsprozesse

Eine Marktanfrage ermittelt mögliche Dienstleister oder Tool-Anbieter. Die Beurteilungskriterien dafür ergeben sich aus der Ist-Analyse und dem Anforderungskatalog, so dass nach dieser Phase eine „Make or Buy"-Entscheidung getroffen werden kann.

Phase 2: Produkt- oder Dienstleisterauswahl

In dieser Phase werden je nach der Entscheidung aus Phase 1 ein Produktanbieter und/oder ein Dienstleister ausgewählt. Bewährt hat sich die 8-4-2-1-Methodik (siehe Abbildung Seite 18).

Da die Funktionalitäten der im Markt etablierten Produkte und die Angebote der Dienstleister sehr ähnlich und die Unterschiede oft nur auf Nachfrage zu finden sind, sind die „richtigen" Fragen in den Bewertungsworkshops ein kritischer Erfolgsfaktor.

Phase 3: Perimeter-Monitoring

Diese Phase fokussiert auf die Etablierung einer Angriffserkennung von Systemen mit Internetanbindung, weitverbreiteten Komponenten bekannter Hersteller, breitflächiger Malware zur Ausnutzung von Schwachstellen und zielgerichteten Angriffen (DoS-Angriffe oder Advanced Persistent Threats) für Spionage oder größere Betrugsdelikte. Die Entwicklung von Bedrohungsszenarien sollte sich am von Lockheed Martin entwickelten Modell der „Cyber Kill Chain" ausrichten.

Phase 4: Überwachung privilegierter Benutzer

Privilegierte Benutzer sind vor allem Administratoren und Mitarbeiter von Service Desks. Kritische Berechtigungen erlauben Tätigkeiten, mit denen hohe Schäden verursacht werden können:
» Umgehen von Kontrollen
» Verschaffen weiterer Berechtigungen
» Ändern oder Löschen von System- oder Anwendungsprotokollen

Da oft erst in der Kombination mehrerer administrativer Tätigkeiten eine betrügerische Handlung erkennbar wird, kann nur ein SIEM durch die Korrelation von Ereignissen diese Absichten frühzeitig zutage bringen.

Phase 5: Überwachung von Fachanwendungen

Viele Anwender erhalten im Rahmen ihrer Aufgaben nur die dafür notwendigen Berechtigungen und unterliegen damit grundsätzlich Einschränkungen. Dennoch gibt es auch bei Fachanwendungen kritische Berechtigungen, deren Kennzeichen sind:
» umfangreiche Freigabekompetenzen
» Zugang zu hochvertraulichen Daten, zum Beispiel Finanz- oder Personaldaten
» Möglichkeit zur Veränderung von Begrenzungen (zum Beispiel Freigabe-Limits) oder Kontrollen (zum Beispiel Freigabemechanismen)
» Möglichkeit zur Änderung von Daten mit hohen Integritätsanforderungen

Eine Vielzahl von Tätigkeiten in Unternehmen benötigt solche kritischen Berechtigungen. Das SIEM-Projekt hilft, eine Übersicht zu schaffen, die dadurch erzeugte Komplexität wird jedoch erst durch eine stringente Methodik und Priorisierung beherrschbar. In dieser letzten Projektphase sind daher die zuvor gesammelten Erfahrungen bestmöglich zu nutzen.

Informationssicherheit von morgen

Die Überwachung von IT-Systemen und Anwendungen durch die Auswertungen von Protokolldateien ist ein unverzichtbares Instrument des internen Kontrollsystems (IKS). Zusätzlich geben Rückkanäle zu den operativen Systemen und die Verzahnung mit anderen Maßnahmen (zum Beispiel einem Intrusion Detection System) dem SIEM einen präventiven Charakter, um Schäden nachhaltig zu verhindern. Dies erzeugt messbaren Mehrwert für das Unternehmen.

Zukünftig wird die Entwicklung von Use-Cases- und SIEM-Regeln durch Systeme mit Künstlicher Intelligenz übernommen (zum Beispiel IBM Watson), so dass Cyber-Angriffen unverzüglich, hochgradig volatil und fokussiert begegnet werden kann.

Das volle Potenzial eines SIEM eröffnet sich jedoch erst, wenn es nicht nur auf das Sicherheits-Monitoring beschränkt wird. Mit Hilfe eines SIEM lassen sich auch Ineffizienzen in Prozessen oder unnötige Kosten durch Überlizenzierung aufdecken. Durch neue Services könnte dadurch dem Vorurteil begegnet werden, dass Informationssicherheit ein reiner Kostentreiber sei. «

Dr. Gerald Spiegel
ist Senior Manager Information Security Solutions bei Sopra Steria Consulting.

Benjamin Rische
ist Manager Banking/Compliance bei Sopra Steria Consulting.

SECURITY INTELLIGENCE: REAKTIONSSTARK UND SCHNELL SEIN

Eine umfassende Digitalisierung der Cyber Security ist heutzutage dringend notwendig, um alle Arten von Angriffsvektoren zu erkennen und zunehmend automatisch abzuwehren. Gefragt sind ein intelligentes Echtzeit-Reporting sowie der Einsatz von Business Intelligence und Business Analytics.

» Die Digitalisierung der Leistungsangebote von Firmen und Behörden ist in vollem Gange. Die damit verfolgten Ziele sind vielfältig. Ihnen ist jedoch eines gemeinsam: Prozesse sollen vereinfacht oder überhaupt erst ermöglicht werden. Damit steigt aber zugleich die Attraktivität für Cyber-Angriffe und das resultierende Schadenspotenzial. Cyber Security wird daher von immer mehr Entscheidern und Führungskräften als wichtig angesehen – auch weil Angriffe immer raffinierter werden und sich ihr Spektrum erweitert hat. So erfolgen Angriffe aus dem Cyber-Raum mittlerweile nicht nur auf technischem Wege, sondern zum Beispiel auch dadurch, dass Angreifer unerkannt Falschinformationen in sozialen Netzwerken verbreiten.

Statische Cyber Security – ein Kampf auf verlorenem Posten

Die Reaktion auf Bedrohungen und Angriffe aus dem Cyber-Raum erfolgt in der Praxis meist noch zu statisch und zu langsam. Einem wirksamen IT-Sicherheitsmanagement wird eine solche Herangehensweise nicht gerecht.

Dies soll beispielhaft an der Erstellung von IT-Sicherheitskonzepten verdeutlicht werden, da hier ein Großteil der Vorgaben für den Schutz des jeweiligen Geschäftsprozesses beziehungsweise Verfahrens vor Gefahren aus dem Cyber-Raum dokumentiert wird. Die Erstellung ist in der Regel Handarbeit und erfolgt aufgrund fehlender Ressourcen oft rudimentär. Beliebte Arbeitsmittel sind Office-Programme. Je nach Vorgabe kommen auch Tools zum Einsatz, wie das (inzwischen eingestellte) GSTOOL des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder ähnliche, teils weiterentwickelte Lösungen. Diese Tools dienen ebenfalls nur der Dokumentation und einem einfachen Reporting, jedoch in strukturierterer und skalierbarer Form.

Ist ein IT-Sicherheitskonzept fertiggestellt, müssen die darin enthaltenen Maßnahmen umgesetzt werden. Da sie eine Vielzahl von Bereichen betreffen, müssen die verschiedensten Ansprechpartner informiert werden. Dies erfolgt in der Regel erneut händisch, da das IT-Sicherheitskonzept mit keinem weiterführenden System kompatibel ist und Vorgaben nicht automatisiert weiterverarbeitet werden können. Die Umsetzungsverantwortlichen planen die Vorgaben anschließend in ihren Arbeitsablauf ein – ein mitunter wieder zeitintensives Unterfangen, bei dem Maßnahmen schnell, langsam oder gar nicht umgesetzt werden.

Das Resultat ist, dass einige Vorgaben zum Zeitpunkt ihrer Umsetzung bereits wieder veraltet sind. Denn in der Zwischenzeit sind bereits neue Angriffsvektoren entstanden, gegen die die erstellten Sicherheitsmaßnahmen wirkungslos sind. Auch die anschließende Überprüfung der Umsetzung der Vorgaben durch händische oder teilweise automatisierte technische Tests ist in Teilen nicht mehr aussagekräftig. Diese überprüfen die Umsetzung teils veralteter Vorgaben, und auch die anschließende Nachbesserung basiert auf veralteten Erkenntnissen. Ein Teufelskreis.

Dynamisierung des IT-Sicherheitsmanagements

Dieses einfache Beispiel zeigt auf, dass das IT-Sicherheitsmanagement den Bedrohungen aus dem Cyber-Raum ohne eine Dynamisierung niemals schnell genug entgegentreten kann. Das Ziel muss ein so weit wie möglich vollständig digitalisiertes und dynamisches IT-Sicherheitsmanagement sein, das einer Institution jederzeit eine angemessene Cyber Security garantiert, indem es Vorgaben selber ermittelt, umsetzt und kontrolliert. Die Verantwortlichen müssen in Echtzeit, zum Beispiel durch Security Dashboards, über die tatsächliche Sicherheitslage informiert werden und (sofern notwendig) Entscheidungsvorlagen erhalten. Die Realisierung eines solchen Vorhabens ist komplex.

Um bei dem Beispiel zu bleiben: Ein IT-Sicherheitskonzept beruht zum großen Teil auf Bedrohungen und dagegen wirkenden Maßnahmen, deren Auswahl auf logischen Mustern basiert. Liegt beides in entsprechender Qualität und Umfang katalogisiert vor, kann eine Auswahl durch den Einsatz entsprechender Analysemethoden automatisiert werden. Dies kann bis zu einem gewissen Grad unter Zuhilfenahme klassischer Automatisierung erfolgen. Um die Erstellung eines IT-Sicherheitskonzepts weiter zu dynamisieren, sind jedoch weitere Techniken, zum Beispiel aus dem Bereich Business Intelligence, denkbar. Bedrohungen und Maßnahmen sowie ihr Zusammenspiel beruhen in vielen Bereichen nur auf einer intelligenten Auswahl und Verknüpfung von Daten, basierend auf vorgegebenen Parametern. Genau hier können Analytics-Lösungen behilflich sein, um aus einer großen Menge von Informationen die relevanten Datensätze auszuwählen und weiterzuverarbeiten. Im Idealfall werden manuell der Scope eines abzusichernden Bereichs definiert und Informationen bereitgestellt, die anschließend automatisch zu Sicherheitsvorgaben verarbeitet werden.

> *Ziel muss es sein, Überprüfungen zunehmend zu automatisieren und ohne menschliches Zutun vorzunehmen.*

Die intelligente Erstellung eines IT-Sicherheitskonzepts stellt bei der Dynamisierung des IT-Sicherheitsmanagements als Ganzes natürlich nur einen Schritt dar. Darüber hinaus müssen die enthaltenen Vorgaben so bereitgestellt werden, dass sie im Idealfall automatisch von Nachfolgesystemen weiterverarbeitet werden können. Dies ist zum Beispiel wichtig, um eine Server-Konfiguration automatisch anzupassen. Zudem muss es das Ziel sein, Überprüfungen zunehmend zu automatisieren und ohne menschliches Zutun vorzunehmen, gefolgt von einem intelligenten Echtzeit-Reporting. Auch hier kann der Einsatz von Business-Intelligence- und Business-Analytics-Lösungen hilfreich sein, zum Beispiel um ein Matching der Ergebnisse automatisierter Prüfungen von Security-Operation-Centern mit den Vorgaben des IT-Sicherheitskonzepts zu ermöglichen. Und letztendlich geht es um eine Zusammenführung aller relevanten Informationen, um Verantwortlichen jederzeit das aktuelle Lagebild und Handlungsbedarfe aufzeigen zu können. «

Jochen Zerhusen
ist Manager Information Security Solutions bei Sopra Steria Consulting.

CHECKLISTE

Angesichts des direkten Zusammenhangs zwischen steigender Digitalisierung und Angreifbarkeit müssen Entscheider die Sicherheitslage des eigenen Unternehmens selbstkritisch hinterfragen. Dazu gehört, die bestehende ITK-Landschaft ebenso unter die Lupe zu nehmen wie die Geschäfts- und Produktionsprozesse, die betriebliche Organisation und die Arbeits- und Verhaltensweisen der Mitarbeiter.

POSITIONSBESTIMMUNG:

- ☐ Gibt es im Rahmen Ihrer Digitalisierungsstrategie ein ganzheitliches Sicherheitskonzept?
- ☐ Sind darin alle Unternehmensbereiche und deren Schnittstellen zum internetbasierten Datenverkehr erfasst?
- ☐ Auf welcher Unternehmensebene ist Cyber Security verankert?
- ☐ Hat Ihr Unternehmen Security beziehungsweise Privacy by Design zur Hauptmaßgabe aller Digitalisierungsmaßnahmen gemacht?
- ☐ Wie viel Ihres Digitalisierungsbudgets ist für die IT-Sicherheit beziehungsweise Cyber Security vorgesehen?
- ☐ Welche internen und übergreifenden Prozesse (etwa mit Lieferanten, Partnern, Kunden) steuert Ihr Unternehmen bereits digital?

AUSSTATTUNG:

- ☐ Wie alt sind IT-Infrastrukturen und Steuerungssysteme, die beim operativen Betrieb im Einsatz sind?
- ☐ Werden diese IT-Infrastrukturen und Steuerungssysteme geregelt überprüft und (so vorhanden) mit Patches der Hersteller auf dem höchstmöglichen Sicherheitsstand gehalten?
- ☐ Wie zentralisiert wird Ihre ITK betrieben, verwaltet und gewartet?
- ☐ Gibt es Unternehmens- oder einzelne Fachbereiche, die unabhängig mit neuerer/schnellerer Technologie (wie Rechnerleistung, Datenspeicher und Anwendungen aus der Cloud) als andere arbeiten (müssen)?

SENSIBILISIERUNG:

- ☐ Ist sich Ihr Unternehmen im Klaren darüber, dass überalterte Hardware, Software und vor allem Betriebssysteme etliche Sicherheitslücken aufweisen, die Cyber-Kriminelle nutzen können (beispielsweise für Betriebsunterbrechungen mit oder ohne Lösegeldforderung)?

- ☐ Ist Ihr Unternehmen auf das Inkrafttreten der EU-DSGVO (Europäische Datenschutz-Grundverordnung) im Mai 2018 vorbereitet?
- ☐ Ist im Unternehmen bekannt, dass Versäumnisse oder Nachlässigkeiten beim Schutz personenbezogener Daten bald mit strengen Sanktionen und Bußgeldern geahndet werden?
- ☐ Verfügen Management und Mitarbeiter über ausreichende Sensibilität gegenüber Cyber-Bedrohungen, und stellen sie ihr Verhalten darauf ab?
- ☐ Sind Management und Mitarbeiter ausreichend geschult, um niederschwellige Risiken (etwa beim Öffnen von Mails und Dateianhängen, beim Nutzen von USB-Sticks) zu erkennen und zu vermeiden?

SICHERHEITSSTATUS UND -STRATEGIE:

- ☐ Wie sind die Sicherheitsvorkehrungen für Produktions- und Office-Prozesse geregelt?
- ☐ Sind die Sicherheitsvorkehrungen integriert, oder gibt es noch systemische Mauern zwischen dem Security- und dem operativen Bereich?
- ☐ Werden Remote-Zugänge (beispielsweise in der Fernsteuerung/Fernwartung oder beim Zugriff auf geschäftskritische Daten mit mobilen Endgeräten wie Tablets oder Smartphones) regelmäßig auf den neuesten sicherheitstechnischen Stand gebracht?
- ☐ Setzen Sie Access und Identity Management und Mehrfaktorauthentifizierung ein, um unautorisierte Zugriffe und Identitätsdiebstahl zu vermeiden?
- ☐ Wie interaktiv sind Ihre Datenbanken?
- ☐ Wie werden Ihre Datenbanken gepflegt und geschützt?
- ☐ Können Sie und autorisierte Mitarbeiter bereits Berichte, Analysen und Prognosen in Echtzeit erstellen?

Prävention

- ☐ Steht die Identifikation und Beseitigung von Schwachstellen auf Ihrer Prioritätenliste?
- ☐ Werden bekannte Risiken systematisch neutralisiert?
- ☐ Welche Maßnahmen zur Prävention, Erkennung und Reaktion auf Sicherheitsvorfälle hat Ihr Unternehmen bereits implementiert?
- ☐ Wie sieht das aktuelle Risikomanagement aus?
- ☐ Gibt es Risiko- und Bedrohungsanalysen? Wie häufig finden diese statt?
- ☐ Nutzen Sie Threat Intelligence?

Erkennung

- ☐ Betreibt Ihr Unternehmen ein systematisches Monitoring, das die gesamten Datenströme permanent auf Anomalien hin untersucht?
- ☐ Erfasst Ihr Unternehmen auch unstrukturierte Daten (etwa aus Sensoren oder E-Mails)?
- ☐ Betreiben Sie „Big Data Security Analytics", gegebenenfalls auch mit Hilfe intelligenter, selbstlernender Algorithmen, die automatisch Gegenmaßnahmen einleiten können?

Reaktion

- ☐ Gibt es unternehmensweite Notfallpläne, sogenannte Disaster-Recovery-Lösungen, die den Geschäftsbetrieb und die Datensicherheit nach Sicherheitsvorfällen wiederherstellen können?
- ☐ Sind zeitgemäße Lösungen und Pläne zur Vorfallreaktion (Incident Response) im Einsatz?

KRITISCHE INFRASTRUKTUREN: MEHR SECURITY STATT NUR SAFETY

Betreiber Kritischer Infrastrukturen – seien es Strom-, Gas- oder Wasserversorger, Kliniken oder auch Verkehrsbetriebe – sind per Gesetz gefordert, Angriffen vorzubeugen und bestimmte Standards einzuhalten, um die Versorgungs- und damit die öffentliche Sicherheit zu gewährleisten. Um die abstrakten Anforderungen des Gesetzgebers in die Praxis umzusetzen, müssen die Betreiber ihre Systeme gründlich analysieren, Schwachstellen erkennen und Maßnahmen definieren.

» Wie sichert man 600 separate und vernetzte Standorte (zum Beispiel Umschaltanlagen, Relaisstationen und Trafohäuschen), von denen aus man quasi direkt auf das Leitsystem zugreifen kann, mit einem Team von zehn Personen? Diese oder vergleichbare Fragen stellen sich momentan Betreiber von Energienetzen, denn das IT-Sicherheitsgesetz und spezifische Fachvorgaben verpflichten sie dazu, ihre Leit- und Steuersysteme gegen (Cyber-)Angriffe zu schützen. Aber was heißen diese Forderungen konkret? Wie lassen sie sich in die Praxis umsetzen? Ein Stadtwerke-Verbund, der in einer lokal begrenzten Region allein für die Infrastruktur und die Grundversorgung der Bevölkerung zuständig ist, hat sich mit den Regelungen auseinandergesetzt.

ABGRENZUNG ZWISCHEN SECURITY UND SAFETY

Im Gegensatz zur deutschen Sprache findet sich im Englischen eine Unterscheidung zwischen den Begriffen „Safety" und „Security", die zwei verschiedene Aspekte von „Sicherheit" bezeichnen.

Der Begriff **Safety** bezieht sich dabei auf die Zuverlässigkeit, das heißt die Ablauf- und Ausfallsicherheit eines Systems („Betriebssicherheit"). Im Sinne von Safety soll die Umgebung vor einem unvorhersehbaren Fehlverhalten eines Objektes/Systems geschützt werden.

Der Begriff **Security** umfasst dagegen den Schutz eines Objektes oder Systems vor vorsätzlichen Angriffen aus der Umgebung („Angriffssicherheit"). IT-Security zielt also auf den Schutz der IT-Systeme und der gespeicherten Daten vor unerwünschten Einwirkungen von außen.

Im IT-Bereich verschwimmen die Grenzen zwischen beiden Begriffen beziehungsweise beeinflussen sich Safety und Security gegenseitig.

Sicherheit der Leitsysteme vernachlässigt

Zweifellos ist das Thema IT-Sicherheit auch für die Betreiber Kritischer Infrastrukturen (KRITIS) – genauso wie für andere Unternehmen – nichts Neues. Um die Büro-IT der Unternehmen, zu der auch die „klassische" IT (Server, Clients, Mailsysteme) gehört, ist es meist recht gut bestellt; die Systeme und Netzwerke entsprechen hier oft schon dem aktuellen Stand der IT-Sicherheit und -Technik. Deutlich anders sieht es dagegen in vielen Fällen in Teilen des sogenannten OT-Netzwerks („Operational Technology") aus, also dem Fernwirk- und Leitsystem, das für den Betrieb der realen Versorgung (mit Strom, Wasser, Gas, Wärme) zuständig ist.

Die OT war und ist oft immer noch vor allem eine Domäne der Ingenieure, die diesen Bereich sehr erfolgreich auf Funktion, Versorgungssicherheit und Safety (nicht Security) getrimmt haben. Doch dass die Systeme und Netze der OT ein Teil der IT sind, den es zu pflegen und zu warten gilt, haben sowohl die Betreiber der OT-Netzwerke als auch die IT-Abteilung der Unternehmen lange Zeit vernachlässigt – und damit die Security. Oft sind sehr grundsätzliche Vorgaben, die in der IT schon lange Standard sind, in der OT nur rudimentär vorhanden oder fehlen ganz. Angesichts der zum Teil langen Gerätelaufzeiten von bis zu 20 Jahren – in der IT sind eher fünf bis acht Jahre üblich – hat die OT also einen deutlich höheren Bedarf an IT-Sicherheitsmaßnahmen.

So existiert zum Beispiel relativ selten ein strukturiertes Nutzer- und Passwortmanagement, was nicht nur den fehlenden Prozessen des Betreibers, sondern auch den stark limitierenden Möglichkeiten seitens der Hersteller der Leit- und Steuertechnik geschuldet ist. Systeme, die nur einen Nutzer mit einem Passwort von maximal vier bis sechs Zeichen zulassen, sind momentan noch eher die Regel als die Ausnahme. Zudem ist ein geregelter

Patch-Zyklus, wie er in der IT seit Jahren üblich ist, oft gar nicht oder nur rudimentär vorhanden, häufig ebenfalls bedingt durch den fehlenden Support der Hersteller, die die Funktion eines Leit- oder Steuersystems nur im Originalzustand, also ohne Patches, garantieren – ein Punkt, der im Bereich der Versorgungssicherheit als kritisch anzusehen ist.

Aber nicht nur die Hersteller, auch die Betreiber sind beim Thema IT-Sicherheit oft nicht auf dem aktuellen Stand der Technik. Bei vielen der Leit- und Steuersysteme wird auf eine Antivirenlösung verzichtet, da Virenscanner schon oft die sehr hardwarenahe Steuersoftware fälschlicherweise als Schadsoftware identifiziert und geblockt haben – was einen sehr zeitnahen Versorgungsausfall zur Folge haben kann. Ebenso sind die in der IT gängigen Intrusion-Detection- oder Intrusion-Prevention-Systeme in solchen industriellen Netzwerken nur selten anzutreffen, da nur sehr wenige dieser Geräte die industriellen Spezialprotokolle ausreichend beherrschen.

Neue Sichtweise gefragt

All dies macht deutlich, vor welcher großen Aufgabe der Stadtwerke-Verbund stand, als es darum ging, die abstrakten Forderungen des IT-Sicherheitsgesetzes zu erfüllen. Am Anfang standen viele Fragen: Welche der Prozesse und Systeme sind „kritisch" im Sinne des Gesetzes? Wo und wie kann ein Angreifer mit Fachkenntnissen gezielt auf Schwachstellen in den Systemen und der Architektur zugreifen, um die Prozesse zu manipulieren oder gar zu sabotieren? Welche Risiken existieren für die eigene Kritische Infrastruktur, und mit welchen konkreten Maßnahmen können sie eingegrenzt oder beseitigt werden?

Um diese Fragen beantworten zu können, wurden zunächst alle vernetzten Systeme mit allen aus IT-Sicht relevanten Informationen erfasst, beginnend bei den prozessnahen speicherprogrammierbaren Steuerungen (SPS). Das Ziel war, einen geregelten und strukturierten Betrieb zu gewährleisten, bei dem die IT-Sicherheit ein elementarer Bestandteil aller Prozesse und Entscheidungen ist. Dazu wurden unter anderem Konzepte, Betriebshandbücher und Leitlinien erstellt, wobei besonders die Spezifika des Leit- und Steuersystems berücksichtigt werden mussten. Neben Standortbesichtigungen wurden auch Gespräche mit Mitarbeitern geführt, um deren Erfahrungen und Meinungen einzuholen. Auf diese Weise entstand eine globale und vollständige Sicht auf das komplette Leit- und Steuersystem des Stadtwerke-Verbunds unter dem Aspekt der IT-Sicherheit – und damit ein neuer Blick auf das Thema OT-Sicherheit.

Das Gesetz in der Praxis leben

Diesen Wandel vollzieht der Verbund seit Anfang 2016. Es konnten bereits viele der notwendigen Prozesse erfolgreich implementiert werden. Auch die Mitarbeiter haben erkannt, dass die Betrachtung, Regulierung und Standardisierung von prozessualer und gelebter IT-Sicherheit nicht nur ein „Papiertiger" ist, sondern dass das Gesetz den Mitarbeitern und Vorgesetzten bei der täglichen Arbeit eine verlässliche Grundlage liefert und ihre Arbeit in vielen Fällen sogar erleichtert. Dies ist ein entscheidender Punkt: Nur wenn die Mitarbeiter von sich aus erkennen, welche Konsequenzen ihr Tun für die IT-Sicherheit ihrer kritischen Prozesse hat, und wenn sie IT-Sicherheit in ihrer täglichen Arbeit „leben", kann das IT-Sicherheitsniveau erreicht werden, das das IT-Sicherheitsgesetz von KRITIS-Betreibern bis 2018 bzw. 2019 fordert.

Mit der zunehmenden Digitalisierung in allen KRITIS-Sektoren bietet das IT-Sicherheitsgesetz eine Grundlage, damit eben diese Digitalisierung nicht nur den Vorgaben der Versorgungssicherheit und Safety entspricht, sondern gerade auch denen der (IT-)Security. Das Ziel ist, die Kritische Infrastruktur hierzulande so zu schützen, dass es keinem Angreifer – seien es Einzelpersonen, terroristische Gruppen oder auch Staaten – leichtfällt, diese effektiv anzugreifen oder auszuschalten. Um dieses Ziel zu erreichen, sieht das IT-Sicherheitsgesetz im Notfall auch finanzielle Sanktionen für die Betreiber vor. «

KRITIS-REGELN DES IT-SICHERHEITSGESETZES

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, in Kraft seit Juli 2015

Betroffene Branchen:

- **Betreiber Kritischer Infrastrukturen (KRITIS):** Einrichtungen oder Anlagen der Bereiche Energie, IT und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanzen und Versicherungen, deren Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe bedeuten oder die öffentliche Sicherheit gefährden würde
- **Bemessungsgrundlage:** sogenannte 500.000er-Regel, das heißt, wenn 500.000 oder mehr Bürger von einer Versorgungsleistung abhängig sind
- **zwei KRITIS-Rechtsverordnungen** mit Vorgaben für die Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation (in Kraft seit Mai 2016) sowie für Finanzen, Gesundheit, Transport und Verkehr (in Kraft seit Juni 2017)

Pflichten und Fristen:

- **binnen sechs Monaten:** Kontaktstelle zur Kommunikation mit dem BSI einrichten, um IT-Sicherheitsvorfälle zu melden, das heißt erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit, die zu einem Ausfall geführt haben oder hätten führen können
- **binnen zwei Jahren:** organisatorische und technische Vorkehrungen zur Vermeidung von IT-Sicherheitsvorfällen gemäß dem Stand der Technik
- **mindestens alle zwei Jahre:** geeignete Nachweise (zum Beispiel Sicherheits-Audits, Prüfungen oder Zertifizierungen)

Torben Klagge
ist Senior Consultant Information Security Solutions bei Sopra Steria Consulting.

IM ZAHLUNGSVERKEHR IST BETRUGSPRÄVENTION NICHT NUR KÜR

Unkomplizierte digitale Bezahlsysteme sind bei den Verbrauchern zunehmend gefragt und akzeptiert. Das veränderte Zahlungsverhalten und damit einhergehende regulatorische Anforderungen bringen eine neue Dynamik in den Markt. Zahlungsdienstleister müssen darauf reagieren: mit Angeboten, die dem veränderten Kundenverhalten gerecht werden, und mit Mechanismen, die Schutz vor immer neuen Angriffsmustern bieten.

» An einem Wochenende im November 2016 griffen Hacker auf rund 20.000 Konten der britischen Tesco-Bank zu. Am darauffolgenden Montag entschied die Bank, das Online-Banking für ca. 140.000 Kunden vorläufig einzustellen. Auch wenn die Bank Erstattungen an die Kunden leistete, der Reputationsschaden als Folge des Angriffs dürfte enorm sein – ebenso wie die Zahl der nicht entdeckten unautorisierten Zugriffe auf die IT-Infrastruktur von Kreditinstituten.

Investitionen in Betrugsprävention schützen vor Schäden und stärken zugleich das Vertrauen und das Sicherheitsgefühl bei den Kunden.

Die Angreifer setzen nicht nur direkt bei den Kreditinstituten an; auch der Kunde steht im Fokus. Eine Investition in Betrugspräventionsmaßnahmen schützt Zahlungsdienstleister und ihre Kunden daher nicht nur vor wirtschaftlichen Schäden, sondern stärkt auch das Vertrauen und das Sicherheitsempfinden der Kunden – und damit die Reputation. Aktuell ist das Sicherheitsempfinden insbesondere bei Bankgeschäften im Internet noch vergleichsweise gering. Laut DsiN-Sicherheitsindex 2016 schätzen rund 20 Prozent der befragten Verbraucher Online-Shopping als „gefährlich" oder „sehr gefährlich" ein; bei Bankgeschäften im Internet sind es indes fast 40 Prozent.

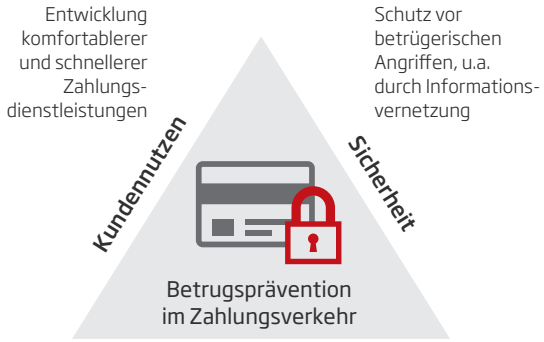
Anforderungen an Prüfungsverfahren und Sicherungsmaßnahmen steigen

Ohne hinreichenden Schutz birgt jedes neue Zahlverfahren und jede weitere Schnittstelle zusätzliche Risiken. Schon seit Einführung der Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI) im Jahr 2015 müssen Finanzinstitute Betrugserkennungssysteme verwenden, um verdächtige Transaktionen vor der Freigabe zu identifizieren. Durch die Einführung von Instant Payment (Echtzeit-Zahlungen) wird sich der Überweisungsvorgang beschleunigen; Kartenumsätze könnten sich dann auf schnelle überweisungsbasierte Bezahlverfahren verlagern. Die überarbeitete EU-Zahlungsdiensterichtlinie (Payment Service Directive, kurz PSD II) dürfte ab 2018 eine weitere Diversifizierung des Angebots an Zahlungsdienstleistungen mit sich bringen. Kunden können dann dritte Zahlungsdienstleister (zum Beispiel Zahlungsauslösedienste wie Sofort-Überweisung oder Kontoinformationsdienste wie figo) beauftragen, in ihrem Namen Transaktionen auszulösen. Kreditinstitute müssen hierzu standardisierte Schnittstellen bereitstellen.

Die Anforderungen an die Prüfungsmechanismen und die Komplexität der zu analysierenden Informationen steigen. Zur Risikominimierung sind der Aufbau und die regelmäßige Aktualisierung von Betrugspräventions- und -managementsystemen unerlässlich.

Ein wirksames Betrugspräventionssystem kombiniert verschiedene Ansätze und Methoden (siehe Tabelle Seite 28). Zunächst erfolgt die sichere Identifikation des Kunden durch Authentifizierungsverfahren, wie zum

BETRUGSPRÄVENTION: ZAHLUNGSDIENSTLEISTER IM SPANNUNGSFELD



Datenschutz
u.a. Transparenz, Datenminimierung und Zweckbindung, erweiterte Auskunftspflichten, höhere Sanktionen

Quelle: Sopra Steria Consulting

AUSGEWÄHLTE METHODEN ZUR GANZHEITLICHEN BETRUGSPRÄVENTION

AUTHENTIFIZIERUNG	REGELBASIERT	MUSTERERKENNUNG	ADAPTIVE METHODEN
• Wissen, z.B. der Online-Banking-PIN • Besitz, z.B. eines Mobilfunkgeräts beim mobilen mTAN-Verfahren • Inhärenz, z.B. eines biometrischen Charakteristikums wie des Fingerabdrucks	regelbasierte Prüfung aufgrund ausgewählter Merkmale, z.B.: • Transaktionshöhe • Transaktionsfrequenz • Zielländer • Sicherungsverfahren • Endgerät • Zahlverfahren	• Identifikation von Mustern und wesentlichen Abweichungen von diesen, z.B. auf Kundenbasis • Abweichungen von der gewohnten Vorgehensweise bei der Nutzung des Online-Bankings	• automatisiertes „Training" auf Basis von historischen Datenbeständen sowie fortlaufende Adaption • prädiktive Elemente zur Verbesserung der Ex-ante-Autorisierungsprüfung des Instituts/Dienstleisters

Quelle: Sopra Steria Consulting

Beispiel die Nutzung von Bankkarte und PIN. Ist die Authentifizierung erfolgreich, wird die Transaktion in Echtzeit geprüft. Dies geschieht auf Basis stetig weiterzuentwickelnder Regelwerke oder durch einen Abgleich des erwarteten mit dem tatsächlichen Kundenverhalten mittels Profilen oder Mustererkennung. Ein weiteres Element sind Risiko-Scores aus dem Einsatz adaptiver Methoden, zum Beispiel sogenannte neuronale Netze. Ein iterativer Schätzalgorithmus erstellt auf Basis eines historischen Datenbestands ein möglichst optimales Prognosemodell, woraufhin das System Transaktionen in Bezug auf ihre Betrugswahrscheinlichkeit bewerten kann. Das Besondere beim Einsatz eines neuronalen Netzes ist, dass nicht direkt ersichtlich ist, warum einer bestimmten Transaktion eine hohe Betrugswahrscheinlichkeit zugeordnet wird, da sich aus den im Prozess erlernten Schätzfaktoren keine Kausalitäten ableiten lassen.

Gezielte Nutzung von Informationen

Erfolgt die Transaktionsanalyse durch auf den jeweiligen Zugangskanal spezialisierte Anwendungen, ohne dass die Informationen zusammengeführt werden, erschwert dies den ganzheitlichen Blick auf den Kunden. Nur die gezielte Auswertung von Informationen aus aufeinander abgestimmten Systemen erlaubt, Auffälligkeiten zu erkennen und Kunden und Kreditinstitute wirksamer vor Schaden zu schützen. Neben internen Informationen können auch extern verfügbare Informationen genutzt werden. So könnten beispielsweise die GPS-Daten des Kunden-Smartphones oder der Banking-App zum Zeitpunkt eines Einkaufs mit den IP-Daten des Ortes der letzten Kartenzahlung abgeglichen werden.

Eine Herausforderung bei der Informationsverwertung zu Präventionszwecken ist es, ein abgestimmtes Datenmanagement zu etablieren und aufrechtzuerhalten. Dabei geht es zum einen um das Zusammenführen von Daten aus unterschiedlichen Bereichen und zum anderen um die Verwertung von Kundendaten unter Berücksichtigung geltender Datenschutzanforderungen. Die ab Mai 2018 geltende EU-Datenschutz-Grundverordnung erhöht den Handlungsdruck, da die informationelle Selbstbestimmung des Kunden gestärkt wird. So muss der Widerruf gespeicherter Daten für den Kunden genauso einfach sein wie die Abgabe. Ändert sich der Datenverarbeitungszweck, so muss der Kunde informiert werden. Im Zusammenspiel mit der erhöhten Vernetzung von Informationen wird die Gestaltung der Datenmanagementprozesse und -infrastrukturen deutlich komplexer.

Strategische Positionierung erforderlich

Mit Blick auf ein ganzheitliches Betrugspräventionssystem ist aufgrund der hohen Komplexität der zu analysierenden Daten eine gründliche Planung erforderlich. Sind grundsätzliche strategische Erwägungen zur Marktbegehung und zu unterschiedlichen regulatorischen Anforderungen geklärt, stehen harte Faktoren wie die IT-Infrastruktur sowie interne Organisationsprozesse auf dem Prüfstand. Es gilt zu klären, welche Anwendungen und Prüfprozesse aufeinander abgestimmt und wie Daten zentral verwertet werden können, um den erforderlichen Schutz zu gewährleisten. Eine frühzeitige Investition in eine übergreifende Betrugsprävention ist erforderlich, um zukünftigen Angriffsszenarien effektiv begegnen zu können. «

Christiane Ginsel
ist Senior Consultant Banking/Compliance bei Sopra Steria Consulting.

Ocke Rörden
ist Senior Consultant Cards & Digital Payments bei Sopra Steria Consulting.

BEI EINEM DIGITALANGRIFF SIND UNTERNEHMEN IN DER PFLICHT

Hackerangriffe, Datenklau und Wirtschaftsspionage sind nur einige Beispiele für digitale Bedrohungen, die in den vergangenen Jahren vermehrt aufgetreten sind. Zahlreiche Gesetze regeln mittlerweile die Meldepflichten der betroffenen Unternehmen gegenüber Behörden, Kunden, Lieferanten und der Allgemeinheit. Und auch in Sachen Prävention und Sorgfalt sind die Unternehmen in der Pflicht.

» Nach Angaben des Bitkom sind zwischen 2014 und 2016 mehr als zwei Drittel der für eine Studie befragten Unternehmen Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden. Den Schaden beziffert der Verband (konservativ) auf rund 45 Milliarden Euro. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schätzt, dass täglich ca. 380.000 neue Schadprogramme beziehungsweise Varianten entdeckt werden. Im August 2016 waren mehr als 560 Millionen Schadprogramme bekannt.

Angesichts solcher Entwicklungen müssen sich auch die Unternehmen immer besser gegen die Bedrohungen aus dem Netz rüsten. Doch was ist, wenn tatsächlich einmal ein Angriff stattfindet oder gar erfolgreich ist? Was sind die Pflichten eines Unternehmens, das Opfer eines digitalen Angriffes geworden ist?

Melde- und Informationspflichten

Zunächst unterliegen Unternehmen einer Reihe von Melde- und Informationspflichten. Die hierfür relevanten Normen stammen aus unterschiedlichen Gesetzen. Regelmäßig gelten diese Melde- und Informationspflichten gegenüber den zuständigen Aufsichtsbehörden; sie können sich jedoch auch auf die einzelnen betroffenen Personen, zum Beispiel Kunden oder Lieferanten, erstrecken oder sogar die Allgemeinheit erfassen (Anzeige in einer überregionalen Zeitung). Sinn und Zweck dieser Regelungen ist es, durch die Meldung von Vorfällen an die Aufsichtsbehörden mögliche oder bereits existierende Bedrohungen festzustellen und diesen entgegenzuwirken beziehungsweise die Konsequenzen für die Betroffenen zu reduzieren.

„Unternehmen sind verpflichtet, vorbeugend Maßnahmen zu ergreifen, um Cyber-Security-Vorfälle und Datenpannen zu verhindern."

Welche Informationspflichten im Einzelfall greifen, hängt von der Art und Weise des Cyber-Security-Vorfalls ab. Bei einer „Datenpanne", also der unrechtmäßigen Erlangung von personenbezogenen Daten von Kunden, wird vorrangig auf datenschutzrechtliche Regelungen zurückgegriffen. Aktuell enthält das Bundesdatenschutzgesetz (BDSG), das wegen der ab dem 25. Mai 2018 geltenden EU-Datenschutz-Grundverordnung (EU-DSGVO) gerade reformiert wurde, in § 42a BDSG beziehungsweise §§ 66 und 67 BDSG-neu eine Meldepflicht, die immer dann greift, wenn besonders sensible Informationen unrechtmäßig einem Dritten zur Kenntnis gelangen und dadurch schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen.

Typisches Beispiel eines meldepflichtigen „Data Breach" ist das Hacken von

© iLexx/iStock/Thinkstock/Getty Images

(Kunden-)Datenbanken. In diesen Fällen müssen sowohl die zuständige Datenschutzaufsichtsbehörde als auch die Betroffenen, also die Personen, deren personenbezogene Daten unrechtmäßig zur Kenntnis gelangt sind, unverzüglich informiert werden. Der Aufsichtsbehörde ist zudem mitzuteilen, welche Maßnahmen in Zukunft zur Verhinderung solcher Vorfälle ergriffen werden.

Sonderregelungen für Betreiber Kritischer Infrastrukturen

Der Gesetzgeber hat 2015 das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (IT-Sicherheitsgesetz) erlassen, das bereits im Jahr 2017 an die europäische Richtlinie zur Netzwerk- und Informationssystemsicherheit (NIS-Richtlinie) angepasst werden musste. Dieses Gesetz richtet sich allerdings nur an die Betreiber Kritischer Infrastrukturen (KRITIS) – wie etwa Strom- und Wasserversorgung, Finanzen, Ernährung oder Gesundheitsversorgung – und auch nur an Betreiber ab einer gewissen Größe. Ziel des Gesetzes ist es, präventiv Schutzmaßnahmen nach dem Stand der Technik zu implementieren, um die Kritische Infrastruktur vor einem Cyber-Angriff zu schützen und dadurch die Versorgungssicherheit der Bevölkerung zu gewährleisten.

Wird ein Betreiber Kritischer Infrastruktur Opfer eines Cyber-Security-Vorfalles, treffen ihn besondere Meldepflichten – und zwar nicht erst dann, wenn dieser Angriff auch erfolgreich war, sondern auch bei versuchten Angriffen. Der Betreiber muss die Angriffe der zuständigen Aufsichtsbehörde, in der Regel dem BSI, melden.

Diese Meldungen müssen ausführlich sein, um eine Verfolgung der Attacken und die Entwicklung wirksamer Schutzmaßnahmen zu ermöglichen. Nach § 8b Abs. 4 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) müssen dann Angaben zur Störung, den technischen Rahmenbedingungen, der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur Branche des Betreibers enthalten sein. Atom-, Energiewirtschafts- und Telekommunikationsgesetz enthalten (beispielsweise im IT-Sicherheitskatalog der Bundesnetzagentur) ähnliche Pflichten.

Nachforschungspflichten

Natürlich kann sich das betroffene Unternehmen nicht darauf ausruhen, die zuständige Behörde lediglich über den Cyber-Security-Vorfall informiert zu haben. Viel-

mehr muss der Vorfall, insbesondere wenn er erfolgreich war, fachmännisch aufbereitet werden, um die Sicherheitslücke zu schließen und zukünftige Angriffe über denselben Angriffsvektor zu erschweren. Hierbei ist es aber wichtig, behutsam vorzugehen, um mögliche Spuren, die der Angreifer hinterlassen hat, nicht zu verwischen. Forensikspezialisten sollten hier eng mit der IT- und Rechtsabteilung zusammenarbeiten.

Da der Eingriff in fremde Systeme in den meisten Fällen auch Strafgesetze verletzt, kann auch die Staatsanwaltschaft eingebunden werden. So haben bereits einige Bundesländer (wie etwa Nordrhein-Westfalen) spezielle Anlaufstellen gegründet. Von Köln aus ermitteln etwa Staatsanwälte der „Zentral- und Ansprechstelle Cybercrime" (ZAC), die Unternehmen rund um die Uhr zur Verfügung stehen.

Mit der deutschen Umsetzung der NIS-Richtlinie wurde für Provider zudem die rechtliche Grundlage geschaffen, künftig auch sogenannte Steuer- und Protokolldaten zu analysieren und zu speichern, um damit Cyber-Angriffe durch Botnetze besser bekämpfen zu können. Außerdem wird Anbietern von Telekommunikationsdiensten erlaubt, den Datenverkehr bei einer Störung einzuschränken, auf Warnseiten umzuleiten oder zu unterbinden, das heißt, unter Umständen auch Netzsperren zu nutzen.

Präventionsmaßnahmen

Unternehmen sind zudem verpflichtet, vorbeugend Maßnahmen zu ergreifen, um Cyber-Security-Vorfälle und Datenpannen zu verhindern. Dies ergibt sich für alle Unternehmen aus den allgemeinen Sorgfaltspflichten, aber auch aus der neuen Datenschutz-Grundverordnung. Danach soll ab Mai 2018 die Verarbeitung personenbezogener Daten (zumindest bei „risikobehafteter" Datenverarbeitung) auch durch eine sogenannte Datenschutzfolgenabschätzung begleitet und durch technische und organisatorische Maßnahmen geschützt werden. Bei diesem „Privacy Impact Assessment" müssen die Auswirkungen der Datenverarbeitung für Betroffene evaluiert und effektive Maßnahmen der IT-Sicherheit etabliert werden. Betreiber von Kritischen Infrastrukturen müssen sogar präventive Schutzmaßnahmen nach dem Stand der Technik implementieren, um die Kritische Infrastruktur vor einem Cyber-Angriff zu schützen.

Dabei ist es auch besonders wichtig, dass sich Unternehmen verstärkt mit den Themen IT-Compliance und Datenschutz auseinandersetzen. IT-Compliance bedeutet auch, dass ein Unternehmen Schutzvorkehrungen für seine Daten und IT-Systeme trifft, die dem aktuellen Stand der Technik entsprechen. War eine Attacke erfolgreich und greift die Meldepflicht, muss das Unternehmen so gut organisiert sein, dass es die gesetzlichen Anforderungen an den Inhalt einer Meldung an die jeweilige Aufsichtsbehörde überhaupt erfüllen kann. Hierzu bedarf es organisatorischer Strukturen innerhalb des Unternehmens, die eine schnelle Ermittlung der Einzelheiten des Angriffs, seiner Folgen sowie etwaiger zukünftiger Gegenmaßnahmen erlauben. Die klare Benennung von einem oder mehreren Verantwortlichen (zum Beispiel Datenschutzbeauftragter, Security Officer), Schulungen der Mitarbeiter zur IT-Sicherheit sowie entsprechende interne Prozesse sind hierfür zwingend notwendig.

Inzwischen richten auch Unternehmen, die nicht unmittelbar zum Adressatenkreis des IT-Sicherheitsgesetzes gehören, das Management ihrer Informationssicherheit am Standard ISO 27001 aus. Die Orientierung an diesem international anerkannten Modell ist auch sinnvoll, denn häufig geben die regulierten Industrien auch den Weg für die übrigen Industrien vor. Für den Bereich IT-Security hat etwa die Bundesnetzagentur (BNetzA) für die Strom- und Gasnetzbetreiber einen IT-Sicherheitskatalog verabschiedet, der die Zertifizierung nach ISO 27001 bis 2018 anordnet. Auch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) verweist in ihren MaRisk (Mindestanforderungen an das Risikomanagement) auf gängige IT-Standards wie ISO 27001 oder die BSI-IT-Grundschutzkataloge.

Die aktuellen Frameworks zur Cyber Security können auch als „Ideengeber" für die Gestaltung der internen Prozesse verwendet werden. Aus diesen Quellen sollte sich ein Unternehmen risikoorientiert auf der passenden Implementierungsebene bedienen. Kleinen und mittleren Unternehmen sei etwa ein „ISMS-light-Ansatz" empfohlen, zum Beispiel nach der Richtlinie „VdS 3473", die Empfehlungen und einen Maßnahmenkatalog für ein Informationssicherheitsmanagementsystem (ISMS) enthält. Ein solcher Ansatz ist in der Regel eine Vorstufe für eine mögliche ISO/IEC-27001- und BSI-IT-Grundschutz-Zertifizierung. «

Christian Kuß
ist Rechtsanwalt und Senior Associate der Luther Rechtsanwaltsgesellschaft mbH.

Dr. Michael Rath
ist Rechtsanwalt, Fachanwalt für Informationstechnologie-Recht und Partner der Luther Rechtsanwaltsgesellschaft mbH.

BUCH & WEB

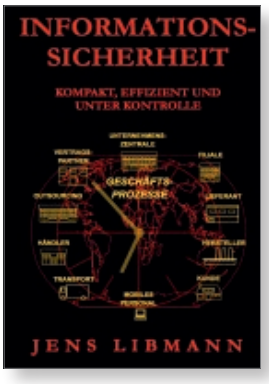
FACHLITERATUR

Ferri Abolhassan:
Security Einfach Machen: IT-Sicherheit als Sprungbrett für die Digitalisierung. Springer Gabler 2017

Autoren aus Politik, Wirtschaft und Forschung beleuchten in diesem Sammelband die Digitalisierung, insbesondere mit Blick auf die Sicherheit und die Konsequenzen für verschiedene Bereiche: Sicherheitspolitik, Management, IT-Recht und Datenschutz, neue Sicherheitsdienstleistungen und -konzepte, neue Berufsbilder, Nutzerverhalten. Der große Appell: Security muss in Zukunft selbstverständlicher Bestandteil von Anwendungen sein – und eben ganz einfach zu bedienen sein.

Jens Libmann:
Informationssicherheit – kompakt, effizient und unter Kontrolle. Praxisorientierte Prinzipien für ein profitables und effizientes Security-Management und -Controlling für Unternehmen. epubli 2016

Der Experte für Security Management Jens Libmann hat selbst feststellen müssen, dass Sicherheitskonzepte, wie sie in der Literatur oder in Weiterbildungen behandelt werden, aus den verschiedensten Gründen oftmals in der Praxis nur schwer umzusetzen sind. Als Quintessenz aus der Standardliteratur und der eigenen Erfahrung entwickelt er in seinem Buch praxisorientierte Prinzipien für ein profitables und effizientes Security Management und Security Controlling für Unternehmen.



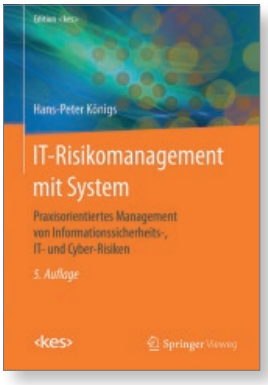
LINKS

» **www.bsi.bund.de**
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht Meldungen, Studien, Veranstaltungshinweise sowie Tipps und Empfehlungen zur Sicherheit im Internet für Bürger und Unternehmen.

» **www.cert-bund.de**
Auf der der Website des CERT-Teams des BSI finden sich Meldungen zu aktuellen Bedrohungen. Registrierte Benutzer können personalisierte Warn- und Informationsdienste nutzen.

» **www.heise.de/security**
Portal des Heise-Verlags mit Nachrichten, Hintergrundinformationen, Foren und Veranstaltungen zum Thema IT-Sicherheit.

» **www.searchsecurity.de**
Portal für IT-Security-Profis mit aktuellen Industrienachrichten, Meldungen über Hackerangriffe, Studien, Ratgebern, Softwaretipps sowie Informationen über Trainingsmöglichkeiten.

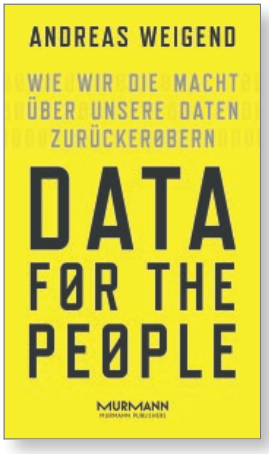


Hans-Peter Königs:
IT-Risikomanagement mit System: Praxisorientiertes Management von Informationssicherheits-, IT- und Cyber-Risiken. Springer Vieweg (5. Aufl., 2017)

Das Buch versteht sich als Leitfaden für das Informationssicherheits-, IT- und Cyber-Risikomanagement in Unternehmen. Ausgehend von allgemeinen Betrachtungen zum Risikomanagement und der Governance, geht der Autor auf IT-Risiken ein und vermittelt dem Leser Methoden, wie er diese beurteilen, damit umgehen und kontrollieren kann. Die 5. Auflage ist an den Stand der Compliance-Anforderungen und der Standardisierung angepasst und enthält ein Kapitel speziell über Cyber-Risiken und deren Besonderheiten.

Andreas Weigend:
Data for the People. Wie wir die Macht über unsere Daten zurückerobern. Murmann Publishers 2017

Der ehemalige Chefwissenschaftler von Amazon Andreas Weigend gibt sich zwar überzeugt, dass der Mehrwert aus der Preisgabe von Daten die Risiken überwiegt. Dennoch formuliert er sechs Grundrechte für Daten, die Bürger und Kunden einfordern sollten, um die Macht über ihre Daten zurückzuerlangen. Er zeigt, wie Google, Facebook und Co. arbeiten und wie viel unsere Daten wert sind, und klärt über den Umgang mit personenbezogenen Daten im Internet auf.



Nitesh Dhanjani:
IoT-Hacking: Sicherheitslücken im Internet der Dinge erkennen und schließen. dpunkt.verlag 2016

Der IT-Sicherheitsexperte Nitesh Dhanjani beschreibt, wie Geräte im Internet of Things von Angreifern missbraucht werden können. Mit seinem Buch präsentiert er einen Leitfaden für die Erkennung und Behebung von Sicherheitslücken. Er erklärt, wie sich Schwachstellen in IoT-Systemen identifizieren lassen, und gibt einen Einblick in die Taktiken der Angreifer.

GLOSSAR

Advanced Persistent Threat (APT)
Gezielter Netzwerkangriff über einen längeren Zeitraum. Der Angreifer will möglichst lange unentdeckt bleiben, um über einen längeren Zeitraum sensible Daten zu stehlen.

Botnet/Botnetz
Menge aktiver Schadsoftwareprogramme (Bots), die über das Internet überwacht und ferngesteuert werden können. Bots infizieren zunächst ungeschützte Rechner, gliedern diese ins Botnet ein und nutzen deren Ressourcen, etwa für Spam-Versand, ohne Wissen des Eigentümers.

CERT
Ein Computer Emergency Response Team wirkt an der Lösung von konkreten IT-Sicherheitsvorfällen mit, befasst sich mit IT-Sicherheit, gibt Warnungen vor Sicherheitslücken heraus und bietet Lösungen an.

Disaster Recovery (DR)
Wiederherstellung der Datenbestände nach einem Katastrophenfall oder einem Absturz zur kurzfristigen Wiederaufnahme der Geschäftstätigkeit. Eine wichtige Kennzahl ist das Recovery Time Objective (RTO), die Zeit bis zum Wiederanlaufen.

Distributed Denial of Service (DDoS)
„Denial of Service" (DoS) steht für die Nichtverfügbarkeit eines Internetdienstes, ausgelöst durch eine Überlastung des Datennetzes, entweder unbeabsichtigt oder durch einen konzentrierten Angriff. Im Fall eines „Distributed Denial of Service" fällt ein Dienst infolge einer Unmenge von Anfragen aus einer Vielzahl von Quellen aus.

Exploit
Mittel, um sich über Sicherheitslücken und Fehlfunktionen Zugang zu bestimmten Systemen (Betriebssystemen, Anwendungssoftware, Smartphones) zu verschaffen.

Incident Response Plan (IRP)
Ein Vorfallreaktionsplan enthält Anweisungen, um Sicherheitsvorfälle zu entdecken, und definiert Reaktionen, um die Auswirkungen eines Vorfalls zu begrenzen.

Information Security Management System (ISMS)
Verfahren und Regeln, um die Informationssicherheit in einem Unternehmen zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Keylogger
Hard- oder Software, mit der sich die Eingaben auf der Tastatur eines Computers protokollieren und damit überwachen oder rekonstruieren lassen, um etwa Passwörter oder PINs aufzuzeichnen.

Malware
Oberbegriff für Computerprogramme, die entwickelt wurden, um unerwünschte/schädliche Funktionen auszuführen.

Managed Security Service (MSS)
Auslagerung der IT-Sicherheit an einen externen Dienstleister, der den Betrieb und die Überwachung von Security-Lösungen übernimmt.

Privacy by Default
Datenschutz als Standardeinstellung. Prinzip, wonach Produkte oder Dienstleistungen standardmäßig datenschutzfreundlich eingestellt sind. In der EU-DSGVO verankert.

Privacy by Design
Datenschutz durch Technik. Prinzip, wonach Technik so angelegt ist, dass die Privatsphäre von Nutzern geschützt wird und Anwender die Kontrolle über die eigenen Informationen haben. In der EU-DSGVO verankert.

Ransomware
Schadsoftware, die den Zugriff auf das Betriebssystem blockiert beziehungsweise potenziell wichtige Dateien verschlüsselt, verbunden mit einer Lösegeldforderung, meist über das digitale Bezahlsystem Bitcoin.

Security Awareness
Bewusstsein und Wissen (der Mitarbeiter) über Risiken für die IT-Sicherheit und für einen verantwortungsvollen Umgang mit Daten und Technik.

Security by Design
Integrierte Softwaresicherheit. Prinzip, wonach Sicherheit als explizite Anforderung in den Entwicklungsprozess aufzunehmen sowie ganzheitliche Sicherheitsmaßnahmen von der Initialisierung an zu berücksichtigen, umzusetzen und zu testen sind.

Security Information and Event Management (SIEM)
Automatisierte Detektion von Angriffen, basierend auf Protokolldaten von Anwendungen, Infrastruktur und Netzwerkkomponenten. Dadurch ermöglicht ein SIEM-System eine schnellere Identifikation, Analyse und Wiederherstellung bei sicherheitsrelevanten Zwischenfällen.

Supervisory Control and Data Acquisition (SCADA)
Überwachen und Steuern technischer Prozesse mittels eines Computersystems.

Threat Intelligence
Intelligente Bedrohungserkennung. Frühwarn- und Erkennungssysteme mit Informationen über Bedrohungen wie Schadprogramme oder Tätergruppen.

AKTUELLE STUDIEN

Managementkompass
Künstliche Intelligenz

Lernende, sich selbst optimierende Systeme sind die Grundlage für die nächsten Entwicklungsstufen der Automatisierung. Welche Potenziale Künstliche Intelligenz kurz- und mittelfristig erschließen kann und welche Vorteile Unternehmen jetzt schon realisieren, zeigt dieser Managementkompass ebenso wie nötige Maßnahmen und Implikationen für die Arbeitswelt.

Branchenkompass
Banking

Der Branchenkompass Banking steht auf neuen Füßen. Praktiker aus der Finanzbranche haben sich getroffen, um die wichtigsten Herausforderungen und mögliche Lösungen zu diskutieren. Die herausgearbeiteten Themen wurden durch eine Online-Befragung von Führungskräften der Branche quantifiziert. Klares Fazit: Der Anpassungsdruck durch Regulierungsmaßnahmen auf nationaler, europäischer und internationaler Ebene bleibt hoch und auch Datensicherheit und Datenschutz stehen auf der Agenda weit oben.

Studie
Datengetriebene Agilität

Sopra Steria Consulting sowie Wissenschaftler der Universität Hamburg und der Leuphana Universität Lüneburg haben das Phänomen der datengetriebenen Agilität in Unternehmen untersucht und zeigen, dass sich diese Arbeitsweise digital exzellenter Unternehmen auch für Organisationen mit gewachsenen Strukturen und IT-Systemen eignet.

IMPRESSUM

Sopra Steria GmbH
Hans-Henny-Jahnn-Weg 29, 22085 Hamburg

F.A.Z.-Institut für Management-, Markt- und Medieninformationen GmbH
Frankenallee 68–72, 60327 Frankfurt am Main

Verlag: FRANKFURT BUSINESS MEDIA GmbH – Der F.A.Z.-Fachverlag
Bismarckstraße 24, 61169 Friedberg
Geschäftsführung: Dr. André Hülsbömer, Hannes Ludwig

Titelfoto: © solarseven/iStock/Thinkstock/Getty Images

ISBN: 978-3-945999-48-6

Redaktion: Jacqueline Preußer (verantwortlich), Andrea van Baal, Juliane Streicher
Gestaltung und Satz: Christine Lambert
Lektorat: Vera Pfeiffer

Druck und Verarbeitung: Boschen Offsetdruck GmbH
Alpenroder Straße 14, 65936 Frankfurt am Main
www.boschendruck.de

Mit Ökofarben auf umweltfreundlichem Papier gedruckt.
Diese Studie wurde klimaneutral hergestellt. Der CO_2-Ausstoß wurde durch Klimaschutzprojekte kompensiert.

klimaneutral
natureOffice.com | DE-644-419329
gedruckt

Ansprechpartner

Sopra Steria GmbH
Corporate Communications
Birgit Eckmüller
Hans-Henny-Jahnn-Weg 29
22085 Hamburg
Telefon: (040) 22703-5219
E-Mail: birgit.eckmueller@soprasteria.com

F.A.Z.-Institut für Management-, Markt- und Medieninformationen GmbH
Jacqueline Preußer
Postfach 20 01 63
60605 Frankfurt am Main
Telefon: (069) 7591-1961
E-Mail: j.preusser@faz-institut.de

ISBN: 978-3-945999-48-6