MANAGEMENTKOMPASS 03 2018

Unternehmen schützen – Risiken minimieren

F.A.Z.-INSTITUT

sopra steria CONSULTING

Urs M. Krämer
CEO
Sopra Steria Consulting

„Unternehmenslenker können der Informationssicherheit nicht genug Bedeutung beimessen. Sie ist obligatorisch für den Geschäftserfolg in der digitalen Ära, denn die fortschreitende Digitalisierung zieht immer perfidere Cyber-Attacken nach sich. Unternehmen wie Behörden benötigen heute neue Verteidigungsstrategien, um ihre Systeme und ihre Reputation nicht aufs Spiel zu setzen."

Andreas Berger
Vorstandsmitglied und CEO für Zentral- und Osteuropa bei der Allianz Global Corporate & Specialty SE

„Das neue Gold der digitalen Ökonomie sind immaterielle Werte wie Daten, Plattformen, Netzwerke oder der Ruf des Unternehmens. Damit wird deren Schutz in Deutschland immer wichtiger. Betriebs- und Lieferkettenunterbrechungen sowie Cyber-Bedrohungen gehören heute zu den größten Risiken."

EXECUTIVE SUMMARY

TREND

THINK TANK

PRAXIS

THINK TANK

PRAXIS

© Bitkom

Achim Berg
Präsident des Bitkom e.V.

„Infrastrukturen, Behörden und Unternehmen stehen zunehmend unter Beschuss international tätiger Cyber-Krimineller. Eine verbesserte Zusammenarbeit im Bereich Cyber-Sicherheit ist dringend nötig. Allein der deutschen Wirtschaft entsteht durch Cyber-Angriffe ein Schaden von 55 Milliarden Euro pro Jahr."

VORWORT

Je mehr der Geschäftserfolg von Vernetzung und digital gesteuerten Prozessketten abhängt, desto umfassender müssen sich Unternehmen schützen – vor dem Diebstahl und dem Missbrauch von Daten ebenso wie vor Sabotage und kostspieligen Betriebsunterbrechungen. Die zunehmende Digitalisierung erfordert von Führungskräften wie von Mitarbeitern ein deutlich höheres Maß an Sicherheitsbewusstsein als bisher.

Heute gehören Cyber-Attacken zu den größten Risiken für geregelte, gesetzeskonforme Geschäftsabläufe, für Infrastrukturen und für den Datenschutz und somit auch für die Reputation und die Erlöse von Unternehmen. Allen Prognosen zufolge dürften die Angriffe in den kommenden Jahren weiter zunehmen, in ihrer Zahl ebenso wie in ihrer Komplexität. Entscheider sind daher doppelt gefordert: Sie müssen dafür Sorge tragen, dass Mitarbeiter von arglosen Gefährdern zu Sicherheitsverteidigern werden. Gleichzeitig gilt es, organisatorische Strukturen (Stichwort: Schatten-IT), Arbeitsweisen und Zugriffsrechte zu hinterfragen. Vor allem aber müssen Unternehmen ihre traditionell reaktiven Abwehrmaßnahmen durch intelligente, agile Lösungen ergänzen.

Wie Unternehmen ihre Sicherheitskultur verändern, auf welche Bedrohungen sie sich einstellen und wie Automatisierung und Künstliche Intelligenz zu ganzheitlicher Prävention und Widerstandsfähigkeit beitragen, zeigt dieser Managementkompass.

Sopra Steria Consulting
F.A.Z.-Institut

Sicherer wirtschaften

Durch die digitale Vernetzung steigt für Unternehmen das Risiko, Opfer von Sabotage, Erpressung und Spionage zu werden. Gegen manche Infiltrationstechniken können vorhandene Sicherheitssysteme kaum etwas ausrichten. Um Schäden für Unternehmen, aber auch für vernetzte Partner, Lieferanten und Kunden zu vermeiden, sollte die Security-Strategie laufend optimiert werden. In einer ganzheitlichen Betrachtung von Betriebs-, Prozess- und Datensicherheit sind mehrschichtige Schutzmechanismen mit intelligenten Erkennungs-, Abwehr- und Reaktionssystemen empfehlenswert.

1. Selbst Unternehmen, die den Schutz ihrer IT und ihrer Daten seit Jahren mit hohem Aufwand betreiben, sind nicht gänzlich unangreifbar. Deshalb ist es besser, sich von der Vorstellung zu verabschieden, umfassende Sicherheit sei ein Dauerzustand. Es ist realistischer zu akzeptieren, dass jedes Unternehmen zum Opfer von IT-Angriffen werden könnte – auch Ihres.

Doch viele Manager sind anderer Meinung, wie eine aktuelle Untersuchung des Digitalverbands Bitkom bei 752 Firmen mit mehr als 50 Mitarbeitern zeigt. So ist die Hälfte der Befragten davon überzeugt, dass sich IT-Angriffe komplett verhindern ließen. Genau das aber ist aus Sicht neutraler Sicherheitsexperten wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) schlicht ausgeschlossen. Möglich ist es jedoch, die Widerstandsfähigkeit der IT zu erhöhen und Erkennungs- und Reaktionsmuster kontinuierlich zu verfeinern. Hierzu ist eine umfassende, anpassungsfähige Sicherheitsarchitektur erforderlich, die alle bekannten neuralgischen Punkte abdeckt und von vernetzten Kleinstgeräten bis zum Cloud Computing reicht.

Wirksamer Schutz und Risikominimierung entstehen in einem Kreislauf aus Erkennen, Lernen und optimierter Vorsorge – und im Zusammenspiel fortschrittlicher Security-Lösungen. Diese müssen Angriffe auf Unternehmensdaten schnellstmöglich entdecken und eindämmen können.

2. Sicherheit ist ein Managementthema: Um Mitarbeiter und Dienstleister in diesem Bereich führen zu können, benötigen Sie keine tiefgreifenden technischen Kenntnisse. Die gesetzlichen Bestimmungen zur Haftung für Sicherheitsvorfälle, etwa im Rahmen der Datenschutzgrundverordnung (DSGVO), sprechen für eine prominente Platzierung des Themas.

Verschaffen Sie sich eine Übersicht über die Sicherheitslage im Unternehmen: Welche Daten sind besonders sensibel, welche erfolgskritisch? Wo entstehen neue Daten, wozu dienen diese, wo werden sie gespeichert und wie verwendet? Wer darf, wer kann auf welche Daten zugreifen? Wer bewegt sich in den Unternehmensnetzwerken, und wer kann systemische Änderungen vornehmen? Fragen wie diese sind alles andere als trivial. Häufig fällt es auch den dafür verantwortlichen Mitarbeitern nicht leicht, sie umfassend zu beantworten.

Angesichts zunehmender Bedrohungen und Angriffe sollte auch die Führungsebene möglichst genau wissen, was mit den Daten im Unternehmen geschieht. Letztlich kann fast jeder vernetzte Punkt zum Angriffsziel gegen die Betriebssicherheit und Handlungsfähigkeit werden. Eine kontinuierliche, bereichsübergreifende Analyse möglicher Schwachstellen und Sicherheitslücken ist unabdingbar.

3. Je mehr Ihr geschäftlicher Erfolg von digitalen Technologien abhängt, desto höher der Schaden bei Datendiebstahl und IT-Sabotage sowie durch Betriebsunterbrechungen. Leider ist mit bewährten Security-Produkten allein kaum etwas gegen die Taktiken und Techniken der aktuell fünften und sich ankündigenden sechsten Generation von Cyber-Bedrohungen auszurichten. Ermitteln Sie, auf welchem Stand Ihre Schutz- und Abwehrmaßnahmen sind.

Wie hoch die Schäden von Cyber-Erpressung, Datendiebstahl und Wirtschaftsspionage sind, hat Bitkom Research im Auftrag des Digitalverbands Bitkom

jüngst in einer Befragung von 500 Industrieunternehmen ermittelt: In den vergangenen beiden Jahren sollen Sicherheitsvorfälle das deutsche verarbeitende Gewerbe 43 Milliarden Euro gekostet haben.

Zwar sind Firewalls, Virenschutz, Sicherheits-Gateways, Intrusion Detection usw. nach wie vor wesentliche Komponenten einer Schutz- und Abwehrstrategie. Doch sie reichen nicht aus. Je mehr Prozesse, Datenquellen und Endgeräte in einem Unternehmen vernetzt sind, desto wichtiger sind ein umfassendes, intelligentes Monitoring, kontinuierliche Abweichungsanalysen und mehrschichtige Abwehrlösungen.

4. Das wachsende Internet der Dinge (IoT) umfasst Liefer- und Produktionsketten der Industrie 4.0, aber auch Gegenstände wie Klimaanlagen, Kameras und Kaffeemaschinen. Dazu können Steuerimpluse und Transaktionen kommen, die per Smartphone erfolgen. Machen Sie sich und Ihren Mitarbeitern die mannigfaltigen Verknüpfungen und Abhängigkeiten bewusst, und achten Sie auf die Gefahr durch ältere Geräte.

Laut Untersuchungen von Vanson Bourne und Trend Micro ist die durch das IoT begründete Angriffs- und Penetrationsgefahr vielen IT-Entscheidern (47 Prozent) gar nicht klar. Eine Sensibilisierung für Security auf Seiten der Mitarbeiter in Fachabteilungen und auf der Geschäftsleitungsebene ist notwendig.

Auch aus Gründen der Haftung und des Versicherungsschutzes sollte Führungskräften wie Mitarbeitern klar sein, dass Compliance mit gesetzlichen Vorgaben nur dann gegeben ist, wenn umfassende Maßnahmen für die IT-Sicherheit ergriffen werden – technisch und organisatorisch. Geschäftsgeheimnisse und -prozesse müssen geschützt werden, und der Schutz muss lückenlos dokumentiert sein.

5. Cyber-Bedrohungen nehmen nicht nur quantitativ, sondern auch an Raffinesse zu. Während brachiale Angriffsformen wie ein Distributed Denial of Service (DDOS) sofort spürbar sind, liegt die Gefährlichkeit von zum Beispiel Advanced Persistent Threats (APTs) in ihrer Unauffälligkeit. Sie sind ganz auf die im Vorfeld sorgfältig recherchierte Sicherheitsarchitektur des betroffenen Unternehmens zugeschnitten.

APT-Angreifer sind in der Regel nicht darauf aus, ein Unternehmen sofort zu schwächen. Vielmehr geht es darum, möglichst lange unentdeckt zu spionieren, Daten abzugreifen oder diese diskret zu manipulieren. Dazu schreiben Hacker ihren Code immer wieder um und setzen verschiedene Umgehungs- und Ausweichtechniken ein. So segeln sie unter dem Radar herkömmlicher Detektionssysteme.

Abhilfe gegen solche Lücken kann laut BSI nur selbstlernende Security-KI (Künstliche Intelligenz) schaffen. Deren verhaltensbasierter Ansatz soll ermöglichen, kleinste Abweichungen im Datenverkehr eines Netzwerks zu erkennen. In vorhandene Sicherheitsprozesse integriert, könnte KI dabei helfen, schnellere Sicherheitsentscheidungen zu treffen und agil auf Bedrohungen zu reagieren. Im Augenblick rät das BSI allerdings dazu, die rein technisch-automatisierte Risikoeinschätzung noch durch die Überprüfung von Spezialisten zu ergänzen.

Auch um regulatorischen Anforderungen gerecht zu werden, rückt in kritischen Prozessen der Ansatz „Man in the Loop" für selbstlernende Systeme in den Fokus. Bei diesem Ansatz trifft das selbstlernende Modell Entscheidungen nicht selbst, sondern macht dem Anwender Vorschläge für gute Entscheidungen. Derzeit werden neue Tools entwickelt, die das Verhalten Künstlicher Intelligenz besser nachvollziehbar machen.

Wer wissen will, wie es um die grundsätzliche Angreifbarkeit seines Unternehmens bestellt ist, kann sich durch reguläre Audits und Zertifizierungen, durch die Risikoermittlung im Vorfeld von Cyber-Versicherungen oder durch den Einsatz eines professionellen „White Hacker" ein klareres Bild davon verschaffen. Voraussetzung für ein Höchstmaß an Schutz ist jedoch, Cyber Security nicht als Kostentreiber, sondern als existenzielle Notwendigkeit zu betrachten. «

kurz & knapp

Jedes **3.** Unternehmen war in den vergangenen zwölf Monaten Ziel eines **CYBER-ANGRIFFS.**

Quelle: Potenzialanalyse Unternehmen schützen – Risiken minimieren (Sopra Steria Consulting), 2018

Widerstandsfähigkeit stärken

Mit zunehmender Vernetzung von Geräten, Sensoren und Prozessen im Internet der Dinge avancieren Cyber-Attacken zum bedeutenden Geschäftsrisiko. Um Unternehmen zu schützen, bedarf es mehr als IT-Security im klassischen Sinne. Auch die Sensibilisierung und Schulung der Mitarbeiter, die Identifikation besonders schützenswerter Assets und der Einsatz automatisierter Intelligenz sind notwendig. Wer Sicherheit will, sollte Verhaltens-, Arbeits- und Kommunikationsweisen in der Organisation verändern.

Realistisch betrachtet, wird die Zahl und Vielfalt der Bedrohungen weiter wachsen. Laut Angaben des „Allianz Risk Barometer 2018" liegt das Risiko für Unternehmen, von Cyber-Kriminalität, Datenschutzverletzungen sowie Systemausfällen und Betriebsunterbrechungen betroffen zu sein, heute durchschnittlich 30 Prozent höher als noch im Vorjahr. Auch das Bundesamt für Verfassungsschutz (BfV) geht von einem signifikanten Wachstum der Bedrohungen aus.

„Illegaler Wissens- und Technologietransfer, Social Engineering und Wirtschaftssabotage sind keine Einzelfälle, sondern ein Massenphänomen. Neben der klassischen Wirtschaftsspionage beschäftigen uns vermehrt Attacken, bei denen Schadsoftware mit dem Ziel in IT-Systeme eingebracht wird, Sabotageakte vorzubereiten." Dies berichtete Thomas Haldenwang, Vizepräsident des BfV, bei der Vorstellung einer gemeinsam mit dem Bitkom durchgeführten Untersuchung („Wirtschaftsschutz in der Industrie") im September 2018 in Berlin. Bitkom-Präsident Achim Berg fand dabei ebenfalls klare Worte: „Wer nicht in IT-Sicherheit investiert, handelt fahrlässig und gefährdet sein Unternehmen."

Mitarbeiter als Verteidigungslinie

Haldenwang und Berg hatten auch Mut machende Nachrichten im Gepäck. Bei Firmen und Organisationen, die gezielt in Security, die Stärkung der Widerstandskraft ihrer Systeme und Anlagen sowie die Sensibilisierung ihrer Mitarbeiter investiert haben, fällt der „Erfolg" von Cyber-Attacken inzwischen geringer aus. Trotz der weiter wachsenden Zahl von

ÜBER 40 MILLIARDEN EURO SCHADEN DURCH IT-ANGRIFFE

Geschätzter Schaden 2016 bis 2017 bei betroffenen Industrieunternehmen; hochgerechnet auf die gesamte deutsche Industrie[1)]

Delikttyp	Schadensumme 2016 bis 2017 (in Mrd. Euro)
Imageschaden	8,8
Patentrechtsverletzungen	8,5
Diebstahl, Schädigung von IT- oder Produktionssystemen	6,7
Kosten für Ermittlungen und Ersatz	5,7
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	4,0
Umsatzeinbußen durch Plagiate	3,7
Sonstiges	6,0
Gesamtschaden	**43,4**

1) n = 343 Unternehmen unterschiedlicher Branchen des produzierenden Gewerbes (insgesamt wurden 503 Unternehmen befragt, davon verzeichneten 47 Prozent Schäden durch Angriffe).

Quelle: Bitkom Research (Studie „Wirtschaftsschutz in der Industrie", September 2018)

Bedrohungen kommen merklich weniger Angreifer an ihr Ziel. Hier scheinen sich Maßnahmen auszuzahlen, die Unternehmen auch aufgrund strengerer gesetzlicher Vorgaben (DSGVO, IT-Sicherheitsgesetz) technisch und organisatorisch umgesetzt haben.

Unverändert bleibt, dass ein Gros der Cyber-Delikte auf aktuelle und ehemalige Mitarbeiter zurückgeht. „Allerdings erfolgen die Taten überwiegend nicht in krimineller Absicht, sondern aufgrund von Fahrlässigkeit und mangelndem Problembewusstsein", berichtet das Bundeskriminalamt. In seinen „Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime" rät das Amt Unternehmen daher dringend, die Sensibilität ihrer Mitarbeiter zu schärfen.

Diese Mahnung ergeht seit einiger Zeit von allen Seiten, sei es von der Allianz für Cyber-Sicherheit, dem Bundeswirtschaftsministerium, von Fachverbänden und IHKs. Bei den Unternehmen fällt die mantrahafte Ermahnung mittlerweile tatsächlich auf fruchtbaren Boden. Die Nachfrage nach Security-Awareness-Schulungen und -Trainings steigt. Dies zeigt auch die „Potenzialanalyse Unternehmen schützen – Risiken minimieren" von Sopra Steria Consulting. Demnach hat mehr als jedes dritte Unternehmen in den vergangenen Jahren Security-Awareness-Programme durchgeführt. Sicherer vor dem „Risiko Mensch" werden digitale Prozesse nur, wenn Mitarbeiter, Lieferanten, Partner und Kunden ihren IT-Umgang ändern.

Internet der Dinge beflügelt Investitionen

Bereits in den frühen 2020er Jahren könnten weltweit 50 Milliarden Geräte digital miteinander verbunden sein. Wie präzise die eine oder andere Prognose zum „Internet of Things" (IoT) zutrifft, ist letztlich unerheblich. Sicher ist: Ein Großteil neuer Vernetzungen entsteht in der Industrie 4.0. Zugriff auf das Internet haben einzelne Maschinen, Geräte und Anlagen ebenso wie komplexe Produktions- und Lieferketten. Damit haben Unternehmen die Aufgabe, nicht nur ihre IT abzusichern, sondern jeden Punkt, der im Internet Daten sendet und empfängt.

Laut Prognose der Marktforscher von Gartner („Forecast: IoT Security, Worldwide, 2018") werden Cyber-Security-Lösungen im laufenden Jahr weltweit 1,5 Milliarden US-Dollar umsetzen. Der Hauptteil entfällt auf professionelle Services. Gefragt sind Endgeräte- und Gateway-Sicherheit, Asset Management, Penetrationstests und die Aufdeckung von Sicherheitslücken als Services. Neben den bekannten Prüf- und Zertifizierungsinstituten sowie Security-Lösungsanbietern haben mittlerweile auch einige Cyber-Versicherungen Sicherheitstests im Angebot.

Der Mangel an Fachkräften und die Komplexität moderner Monitoring-, Analyse- und Präventionssysteme beschleunigen die Nachfrage nach externen Dienstleistungen. Sie stammt vor allem aus der Finanzbranche, dem Gesundheitssektor und anderen Branchen, die sowohl stark reguliert als auch häufiges Angriffsziel sind.

In der öffentlichen Verwaltung, die sich mit Digitalisierung und E-Government-Diensten noch schwertut, gilt IT-Sicherheit nach wie vor als größte Herausforderung, wie der „Branchenkompass Public Services 2018", herausgegeben von Sopra Steria Consulting und F.A.Z.-Institut, zeigt. Auch hier könnten Standards die digitale Transformation in Zukunft beschleunigen.

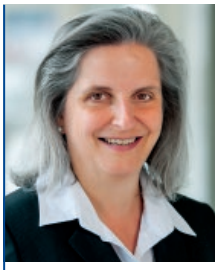
Ganzheitlicher Schutz als Ziel

Unabhängig von der Ausgangslage im Unternehmen wird an einer Modernisierung, Konsolidierung und Homogenisierung der IT-Security kein Weg vorbeigehen. Wie die Klassifizierung schützenswerter Daten und granulare Zugriffsrechte gehört ein ganzheitliches Sicherheitsmanagement zu den Grundlagen jeder „Cyber-Strategie".

Bei der Analyse von Angriffsmustern kommen immer häufiger intelligente, selbstlernende Systeme zum Einsatz. Die Algorithmen Künstlicher Intelligenz durchforsten Unternehmensnetze nach Anomalien und tragen so dazu bei, Bedrohungen zu identifizieren und abzuwehren. Aktuell verfügen 90 Prozent der deutschen Unternehmen über eine Angriffsabwehr. Allerdings arbeiten davon laut „Live Security Studie 2017/2018" von Bitkom Research nur 35 Prozent mit stringenter Erkennungs-, Analyse- und Reaktionsoptimierung.

Statistisch nicht belegt ist die Zahl der Unternehmen, in denen eine Schatten-IT einzelner Fachbereiche oder mangelnde Kommunikation die Datensicherheit gefährdet. Wo Fachabteilungen und IT nicht eng zusammenarbeiten, ist schnell ein nicht gepatchtes Gerät mit dem Internet verbunden, oder eine E-Mail-Kampagne wird zur „Einladung" für Hacker.

Wo Security Management organisationsübergreifend wirkt, wächst dagegen das Fundament für eine erfolgversprechende und gesetzeskonforme digitale Transformation. «



Jacqueline Preußer
ist Leiterin Research & Studien im F.A.Z.-Institut.
j.preusser@faz-institut.de

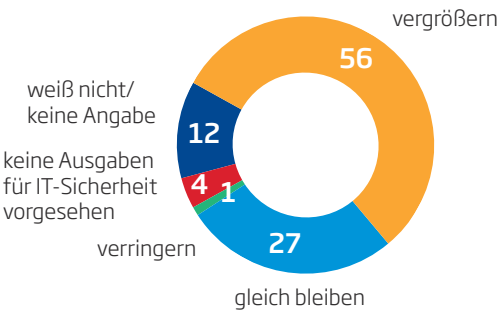
Eric Czotscher
ist Leitender Redakteur Research & Studien im F.A.Z.-Institut.
e.czotscher@faz-institut.de

Abwehrstellung einnehmen

Sopra Steria Consulting hat im Rahmen der Studie „Potenzialanalyse Unternehmen schützen – Risiken minimieren" 308 Entscheider und Führungskräfte aus den Branchen Finanzdienstleistungen, verarbeitendes Gewerbe, öffentliche Verwaltung und Versorgungsunternehmen sowie Telekommunikation und Medien zum Thema IT-Sicherheit befragt.

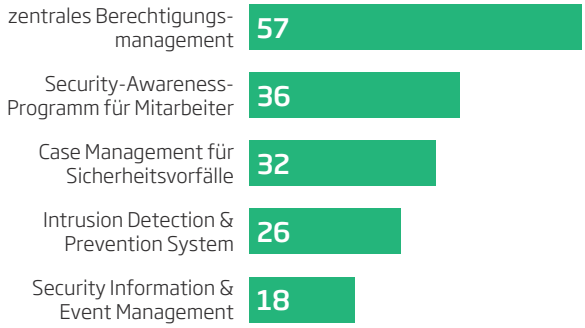
WACHSENDE BUDGETS FÜR IT-SICHERHEIT

Veränderung des unternehmenseigenen Budgets für IT-Sicherheit in den kommenden drei Jahren; in Prozent der Befragten; n = 165



SICHERHEITSLÜCKEN ERKENNEN UND VORBEUGEN

Im eigenen Unternehmen in den vergangenen drei Jahren eingeführte IT-Sicherheitsmaßnahmen; in Prozent der Befragten; n = 184; Mehrfachantworten möglich

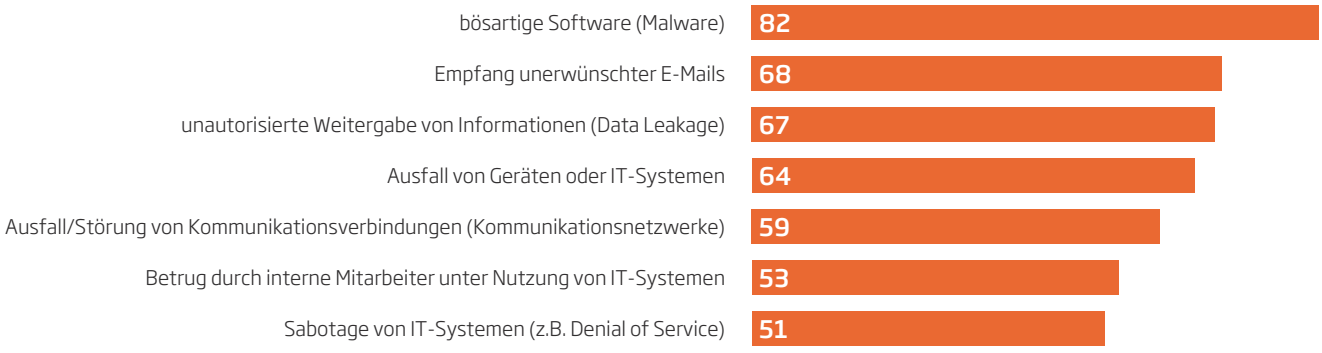


Wer sich schützen will, muss in entsprechende Sicherheitskonzepte investieren: Mehr als die Hälfte der Befragten erwartet in den kommenden drei Jahren ein steigendes Budget für IT-Sicherheit.

Der Mensch steht im Fokus von IT-Sicherheitsmaßnahmen: Die Mehrheit der befragten Unternehmen setzt auf ein zentrales Berechtigungsmanagement. Gut ein Drittel führt Sensibilisierungskampagnen für Mitarbeiter durch.

MALWARE UND SPAM SIND HAUPTROBLEM FÜR IT-SICHERHEIT

Für das eigene Unternehmen relevante Bedrohungsszenarien; in Prozent der Befragten; n = 179; Mehrfachantworten möglich



Im Alltagsgeschäft der befragten Unternehmen ist neben klassischen softwarebasierten Bedrohungsformen und technikseitigen Störungen auch die Interaktion zwischen internen Mitarbeitern und IT-Systemen eine relevante Gefahrenquelle.

Quelle: Potenzialanalyse Unternehmen schützen – Risiken minimieren (Sopra Steria Consulting), 2018

Cyber-Gefahren auf dem Radar

© welcomia/iStock/Thinkstock/Getty Images

Die Digitalisierung von Unternehmen schreitet schneller und schneller voran. Daten werden digital erfasst, Prozesse automatisch oder zumindest digital unterstützt durchgeführt, und Algorithmen helfen Mitarbeitern bei Entscheidungen oder nehmen ihnen diese komplett ab. Neben Chancen birgt diese Entwicklung auch Gefahren für Unternehmen und ihre Kunden. Dabei lassen sich sechs hauptsächliche Gefahrenherde identifizieren: Vernetzung, Outsourcing, Infrastrukturen, Geheimdienste, Künstliche Intelligenz (KI) und Daten.

Für Unternehmen und ihre Kunden ist die erste Gefahrenquelle die zunehmende Vernetzung. So führt die Digitalisierung des Produktionsprozesses – auch Industrie 4.0 genannt – zu einer weitgehenden Vernetzung der Produktionsinfrastruktur. Wo vorher Produktionsmaschinen unabhängig voneinander arbeiteten, entsteht ein hochkomplexes, vernetztes Gebilde. Als Konsequenz daraus muss die Software der darin integrierten Computer permanent auf dem aktuellen Stand gehalten werden.

Die Auswirkungen veralteter Software waren in jüngster Zeit mehrfach öffentlich sichtbar, als „Kryptotrojaner" Teile oder die komplette IT-Infrastruktur von Unternehmen übernahmen. Dabei handelt es sich um eine Software, die getarnt, zum Beispiel als gezipter E-Mail-Anhang, auf den Rechner gelangt und dort die Festplatte verschlüsselt. Damit wird diese unbenutzbar und kann erst nach Zahlung eines Lösegeldes wieder verwendet werden. In den meisten Fällen waren es keine gezielten Angriffe, sondern die Systeme wurden durch allgemein kursierende Schadsoftware infiziert. Allerdings wird in Zukunft die Entwicklung spezialisierter Angriffswerkzeuge wohl zunehmen.

Updates können fehlerhaft sein

Je nach Kritikalität der Umgebung entsteht zusätzliche Arbeit für die Qualitätssicherung und das Einspielen von Patches, um Netzwerkgefahren abzuwehren. Alternativ kann ein Unternehmen die »

Kontrolle über seine Infrastruktur weitgehend aus der Hand geben und den Herstellern durch Autoupdates freie Hand beim Einspielen neuer Software lassen. Dies wiederum birgt aber die Gefahr fehlerhafter Updates, die zum Ausfall ganzer Produktionsstrecken führen können. Im schlimmeren Fall ist die Autoupdate-Routine fehlerhaft, oder ein Angreifer attackiert erfolgreich den Hersteller und kann so unternehmensübergreifend alle Geräte mit der entsprechenden Software übernehmen.

Dies spielt auch abseits von Produktionsumgebungen eine Rolle. Neben allgegenwärtigen Smartphones ziehen mehr und mehr Geräte aus dem Internet der Dinge (IoT) in die Unternehmen ein. Ob Kaffeemaschine, vernetzter Drucker oder Bürostuhl, Heizung, Türschloss oder Sicherheitskamera, all diese Geräte können Computer enthalten. Dabei ist ein wesentliches Problem dieser Geräteklasse, dass die Hersteller oft keine oder nur für einen sehr kurzen Zeitraum Sicherheits-Updates zur Verfügung stellen. Übernimmt ein Angreifer die Kontrolle über eines dieser Geräte, hat er bereits einen Fuß in der Tür und kann von dort tiefer in das Unternehmensnetzwerk eindringen. Erst kürzlich wurde ein Casino über ein vernetztes Aquariumsthermometer erfolgreich angegriffen.

Beim Outsourcing Kontrolle behalten

Moderne IT-Architekturen wie Cloud Computing oder serviceorientierte Architekturen binden vermehrt IT-Dienstleistungen anderer Anbieter in die eigene Infrastruktur ein. Selten wird dabei deren Einfluss auf die IT-Sicherheit des Unternehmens betrachtet. Zwar führt die Auslagerung der IT insbesondere bei kleinen und mittleren Unternehmen zu einer Verbesserung der IT-Sicherheit, jedoch schwindet in jedem Fall die Kontrolle.

Im Gegensatz zur vereinbarten Leistung der in Anspruch genommenen Services ist IT-Sicherheit für den Auftraggeber schwerer mess- oder überprüfbar. Letztlich ist der Auftraggeber auf die Einhaltung von Zusagen des Serviceanbieters oder auf die Zertifikate unabhängiger Dienstleister angewiesen. Dabei wird oft übersehen, dass der Einsatz von Fremdsoftware auf eigenen Computern auch als eine Form des Outsourcing im weiteren Sinne angesehen werden kann. Auch Smartphones können betroffen sein, wenn etwa Angreifer eine bereits bei Benutzern installierte App aufkaufen, um dann über die Aktualisierungen der Software schadhafte Komponenten in großem Stil zu verteilen.

Mehr in **Sicherheit** investieren!

Auditoren für Informationssicherheit suchen laufend nach Verbesserungsmöglichkeiten. Stefan Beck von Sopra Steria Consulting nennt die wichtigsten Herausforderungen.

Herr Beck, warum sind Sicherheits-Audits überhaupt notwendig?

Weil nur durch eine objektive Überprüfung Fehler und Optimierungspotenziale in der IT-Sicherheit identifiziert und behoben werden können. Mit Optimierungspotenzialen meine ich übrigens nicht nur zu wenig Sicherheit, sondern auch zu viel. Denn dies kann einen ineffizienten Ressourceneinsatz bedeuten. Darüber hinaus halte ich Audits aus Gründen der Fairness und zur permanenten Sensibilisierung des Personals für notwendig.

© Wavebreakmedia Ltd/iStock/Thinkstock/Getty Images

Sie untersuchen sicherheitskritische Infrastrukturen. Was sind die häufigsten Lücken?

Was sich immer wieder feststellen lässt, ist erheblicher Personalmangel. Zudem besteht in einigen Organisationen ein mangelhaftes Commitment des Managements für ein angemessenes Sicherheitsniveau. Man erwartet ein hohes Maß an Informationssicherheit, scheut aber die notwendigen Investitionen in Personal, Schulungen, Infrastruktur und externe Unterstützung. Des Weiteren werden Prozesse wie Notfallmanagement, Behandlung von Sicherheitsvorfällen, Wartung und Updates nicht konsequent angewandt, oder sie sind gar nicht definiert. Und, nicht minder gravierend, es werden aufgrund fehlenden Know-hows hinsichtlich möglicher Gefahren zu hohe Risiken eingegangen.

Durch eine weitere Spezialisierung der Unternehmen wird die Einbindung von Dienstleistungen Dritter noch zunehmen und möglicherweise auch die Zahl so ausgeführter Angriffe.

Gefahren aus den Zulieferketten

Unternehmen sind von den ihnen zur Verfügung stehenden (Kritischen) Infrastrukturen für Strom, Wasser, Internet, Transport usw. abhängig. Dazu kommt die Abhängigkeit von Lieferanten. Je enger Prozesse in den Produktions- und Lieferketten miteinander verflochten werden (bis hin zur Just-in-time-Produktion), desto empfindlicher wirken sich einzelne Störungen aus.

Mit der Verflechtung werden nicht nur Dienstleistungen, sondern auch die IT-Sicherheitsrisiken der Anbieter ins eigene Unternehmen importiert. Ein erfolgreicher Angriff auf einen Lieferanten oder auf eine Kritische Infrastruktur kann beim Abnehmer die Produktion stilllegen.

Geheimdienste greifen an

Als risikoverstärkend für die bereits genannten Gefahrenquellen erweist sich, dass unter den Angreifern zunehmend staatliche Akteure wie Geheimdienste oder Militärs zu finden sind. Auch fünf Jahre nach den Snowden-Enthüllungen sind auf diesem Feld weder Zurückhaltung noch Einschränkungen erkennbar. In der Politik werden mittlerweile Maßnahmen zur aktiven Cyber-Abwehr und sogar Gegenangriffe („Hack Back") diskutiert.

Letztendlich ist es dabei ohne Relevanz, ob die Unternehmen selbst oder ihre Zulieferer und Infrastrukturanbieter ein Angriffsziel sind oder ob die Dienste durch das Aufkaufen und Geheimhalten von Sicherheitslücken Dritten die Tür öffnen – mit oder ohne Absicht.

KI stellt neue Sicherheitsaufgaben

Mehr und mehr Unternehmen entdecken das Potenzial Künstlicher Intelligenz und verwenden bereits Algorithmen für einfache Aufgaben bis hin zu komplexen Entscheidungen. Die Ergebnisse von maschinellem Lernen durch künstliche neuronale Netze, Musterkennung oder wissensbasierte Systeme sind oft eindrucksvoll. »

Welche Fehler machen Unternehmen beim Schutz ihrer IT besonders häufig?

Meist wird das Thema Informationssicherheit zu spät berücksichtigt. Erfahrungsgemäß wird für Dienste, Produkte und Verfahren erst kurz vor Produktivsetzung ein Sicherheitskonzept angefordert. Dieses kann deshalb dann nur rudimentär erstellt werden und weist inhaltliche Schwächen auf. Häufig werden die darin geforderten Sicherheitsmaßnahmen nicht einmal realisiert, da dies den Produktivtermin gefährden würde. Also wird gemeldet: alles ok. Nachdem das Vorhaben produktiv ist, schwindet der Druck, das Sicherheitskonzept angemessen zu finalisieren. Und dann wartet auch schon das nächste Vorhaben …

Stefan Beck
ist Senior Manager im Bereich Information Security Solutions bei Sopra Steria Consulting.

Was sollten Unternehmen deshalb unbedingt tun?

Das Thema Informationssicherheit ernst nehmen! Dazu muss es in der gesamten Organisation konsequent und ganzheitlich verinnerlicht sein. Man darf es keinesfalls als notwendiges Übel begreifen. Angemessen betrieben, wird der Mehrwert von allen Beteiligten erkannt und als hoch eingeschätzt. So wirkt Informationssicherheit auch motivierend! Als Auditor sind sehr gute IT-Security- und Risikomanagement-kenntnisse und viel Erfahrung unabdingbar. Nicht zuletzt ist ein gutes Gespür für Risiken entscheidend. Um das zu erreichen, muss man bereit sein zu investieren. Die Erfahrung zeigt, es lohnt sich! «

„Das Löschen oder Nichtspeichern von Daten kann einen Angriff auf ein Unternehmen unattraktiver machen."

Der Prozess dahinter ist aber meist komplex, und es fehlt in vielen Fällen die notwendige Transparenz, damit der einzelne Mitarbeiter das Ergebnis eines Algorithmus auch nachvollziehen kann. Dies führt dazu, dass Entwickler oder Trainer von Algorithmen Entscheidungen über die Ausführung bestimmter Prozesse im Unternehmen treffen, ohne überhaupt ein klares Mandat dafür zu haben.

Auch externe Angreifer können sich den Einsatz Künstlicher Intelligenz zunutze machen. Ein möglicher Angriff besteht in der gezielten Erzeugung von Eingabewerten für den Algorithmus der KI, die dann falsch klassifiziert werden. Beispiele hierzu liegen oft im visuellen Bereich. So führte in einem Fall eine für Menschen nicht sichtbare Manipulation eines Panda-Bildes zur Klassifizierung des Pandas als Gibbon-Affe. Andere Beispiele sind manipulierte Zahlen, die von der KI falsch gelesen werden, oder Verkehrszeichen, die mit minimalen Änderungen so manipuliert werden, dass sie von der KI falsch erkannt werden.

Daneben gibt es Angreifer, die den Trainingsprozess der KI ausnutzen, um mit manipulierten Trainingsdaten dafür zu sorgen, dass ein bösartiges Modell erstellt wird. Da das Training mitunter den Hauptteil der Arbeit beim maschinellen Lernen ausmacht, wird für diesen Prozess oft die Hilfe Dritter in Anspruch genommen, zum Beispiel von Google, Amazon oder Microsoft. Wegen der Komplexität maschinellen Lernens verbunden mit den Gefahren des Outsourcing ist es für Unternehmen oft schwer zu entdecken, wenn ihre KI mit einem fehlerhaften Modell arbeitet. Auf der anderen Seite unterstützt KI Unternehmen und Organisationen auch zunehmend dabei, Angriffe zu entdecken und zu verhindern.

Datenrisiken lassen sich minimieren

Die zunehmende Digitalisierung erzeugt auch immer mehr Daten. Dabei ist es für Unternehmen wichtig zu lernen, welche Daten einen Wert für sie darstellen und welche nur Ballast sind. Bei der Speicherung von Daten müssen Regulierungen wie die Datenschutzgrundverordnung (DSGVO) beachtet werden, und es ist dafür Sorge zu tragen, dass die Speicherung sicher ist. Weniger Augenmerk liegt oft auf dem Löschen nicht benötigter Daten. Die Reduktion von Daten erleichtert nicht nur die Einhaltung der Regulierung, sondern verringert auch die mögliche Datenmenge, die ein Angreifer erbeuten kann. Schlussendlich kann das Löschen oder Nichtspeichern von Daten einen Angriff auf ein Unternehmen auch unattraktiver machen.

Eine weitere Gefahrenquelle sind Informationen, die Dritte über ein Unternehmen besitzen. Schon jetzt lässt sich beobachten, dass Social Engineering eine Komponente erfolgreicher Angriffe ist. Mitarbeiter, die auf Links in E-Mails klicken, die Anhänge herunterladen und diese in Office-Programmen öffnen oder direkt ausführen, erlauben es Angreifern, ein erstes Standbein im Unternehmen aufzubauen. Mit zunehmendem Wissen über Mitarbeiter, Prozessabläufe und Sicherheitsregeln im Unternehmen können Angreifer – gegebenenfalls unter Zuhilfenahme maschinellen Lernens – ihre Angriffe noch zielgerichteter gestalten. Man denke dazu an die Fortschritte der synthetischen Sprachausgabe, die klanglich kaum noch als Roboterstimme zu erkennen ist.

Die genannten Bedrohungen in diesem Beitrag sind beunruhigend. Und dennoch ist festzustellen, dass bislang die meisten Unternehmen ihre Investitionen in IKT-Sicherheit erst nach mehr oder weniger schwerwiegenden Vorfällen im eigenen Haus erhöht haben. Das gilt unabhängig davon, ob die Investitionen direkte Kosten oder Umorganisationen verursachen oder ob bereits bei Innovationen IKT-Sicherheit mitberücksichtigt wird. «

Dr. Sebastian Pape
ist Senior Researcher bei der Deutsche Telekom Stiftungsprofessur für Mobile Business & Multilateral Security an der Goethe-Universität Frankfurt am Main.

sebastian.pape@m-chair.de

Prof. Dr. Kai Rannenberg
hat die Deutsche Telekom Stiftungsprofessur für Mobile Business & Multilateral Security an der Goethe-Universität Frankfurt am Main inne.

kai.rannenberg@m-chair.de

„Erklärtechnik“ für Künstliche Intelligenz

Mit dem Einsatz Künstlicher Intelligenz (KI) und der wachsenden Lernfähigkeit von KI steigt das Risiko, dass die Systeme irgendwann mehr wissen als ihre eigenen Entwickler und fachlichen Trainer. So können Organisationen die Entscheidungen ihrer Technologie möglicherweise nicht mehr nachvollziehen. Es besteht deshalb Bedarf an einer Art Erklärtechnik für KI-Systeme.

Die Nachvollziehbarkeit Künstlicher Intelligenz ist für alle Unternehmen und Organisationen, die KI einsetzen, ein sensibles Thema. Dies gilt insbesondere für komplexe lernende Systeme: Durch selbstlernende Algorithmen erhalten Maschinen die menschenähnliche Fähigkeit, aus Erfahrungen zu lernen und bessere Entscheidungen zu treffen. So vielfältig die Einsatzbereiche selbstlernender Algorithmen bereits sind, so unterschiedlich sind die Anforderungen an solche Systeme. Sicherheitskritische Anwendungen wie die Wartung von Flugzeugen, die Analyse von Patientendaten oder auch selbstfahrende Autos werfen nicht nur beim Anwender Fragen auf („warum fährt das Auto jetzt links?“). Auch regulatorische Anforderungen müssen erfüllt werden.

Güte versus Verstehbarkeit

In der europäischen Datenschutzgrundverordnung (DSGVO) ist das Recht auf Erklärbarkeit automatisierter Entscheidungen enthalten. Betroffene Personen haben demnach das Recht, nicht einer ausschließlich automatisierten Entscheidung unterworfen zu werden. Zumindest sollen betroffene Personen bei Bedarf aussagekräftige Informationen über die angewendete Logik erhalten können. »

Technisch können selbstlernende Systeme bereits spezielle Entscheidungen vollautomatisiert treffen. Die Algorithmen stoßen aber an technische Grenzen, wenn es um die Erklärbarkeit ihrer eigenen Entscheidungsfindung geht. Zwischen Erklärbarkeit und Güte eines selbstlernenden Modells besteht eine negative Korrelation. So gelten neuronale Netze, die aus Millionen von Neuronen und Verknüpfungen bestehen, als Modelle höchster Güte. Doch ihre Entscheidungen sind am schwierigsten nachzuvollziehen.

„XAI-Tools öffnen die Blackbox der Künstlichen Intelligenz und machen Entscheidungen nachvollziehbar."

Um den regulatorischen Anforderungen gerecht zu werden, rückt in kritischen Prozessen der Ansatz „Man in the Loop" für selbstlernende Systeme in den Fokus. Bei diesem Ansatz trifft das selbstlernende Modell kritische Entscheidungen nicht selbst, sondern gibt dem Anwender nur Entscheidungsvorschläge.

XAI als Erklärtechnik

Dies ist auch eine Kernkomponente der Forschungsarbeit der Defense Advanced Research Projects Agency (DARPA), einer Behörde des US-Verteidigungsministeriums. Ziel des Programms „Explainable Artificial Intelligence" (XAI) ist es, Verfahren für die Erklärbarkeit und Nachvollziehbarkeit von KI-basierten Handlungsempfehlungen zu finden.

Künstliche Intelligenz gilt als Blackbox, die beliebigen Input über verborgene Schichten und nicht nachvollziehbare Algorithmen zu einem Output verdichtet, der so lange trainiert wird, bis gewünschte Ergebnisse herauskommen. Ein gutes XAI-Tool öffnet diese Blackbox, macht die entscheidungsrelevanten Attribute nachvollziehbar und deckt die darunterliegenden Informationen auf. Dabei liegt der Fokus auf der Interaktion zwischen Mensch und Maschine: Wie kann ein Mensch mit den Ergebnissen eines selbstlernenden Systems bestmöglich umgehen?

Anwendung bei Drohnen

Das Projekt COGLE für den Einsatz unbemannter Fluggeräte ist eine Anwendung aus dem DARPA-XAI-Programm. COGLE soll maschinell gelernte Fähigkeiten von Drohnen mit Konzepten und Abstraktionsmethoden, wie sie Menschen verwenden, verbinden. Die Informationen werden in einer spezifischen Anwendungsoberfläche zusammengetragen, damit der Anwender die Entscheidung nachvollziehen kann. Aufgrund der unterschiedlichen kognitiven Fähigkeiten von Mensch und Maschine wird erwartet, dass sich die Entscheidungsqualität durch die Menschen verbessert. Die bei COGLE gewonnenen Konzepte können auch auf andere autonome Systeme wie selbstfahrende Autos übertragen werden.

Flugzeugbau, Medizin und Finanzen

Auch außerhalb des Militärs erkennt man den Nutzen von XAI-basierten Lösungen. So präsentierten Forscher der niederländischen Universität Twente eine Lösung für die automatische Erkennung fehlerhafter Bauteile von Flugzeugen. Das XAI-Tool extrahiert die entscheidungsrelevanten Attribute, die für den Materialausfall identifiziert wurden. Die Ergebnisse werden dann in Bezug zu den Referenzwerten grafisch dargestellt.

In der medizinischen Diagnostik werden neuronale Netze unter anderem zur Analyse von Röntgenbildern eingesetzt. Forschungen haben gezeigt, dass selbstlernende Algorithmen Anomalien in Bildern mit hoher Genauigkeit bestimmen können. Diese oft minimalen Abweichungen zu Bildern von gesunden Patienten sind für Menschen schwer erkennbar.

XAI-Lösungen können die Bildanalysen neuronaler Netze verstehen und dem Anwender die Bildbereiche hervorheben, die Auffälligkeiten zeigen. Somit kann der Anwender die Entscheidung des neuronalen Netzes nachverfolgen und erklären.

Im Finanzwesen ergeben sich bezüglich regulatorischer Anforderungen viele Einsatzmöglichkeiten. Schlägt eine KI-basierte Anwendung die Ablehnung eines Kredits vor, muss der Kreditspezialist die Entscheidung zurückverfolgen und – wichtiger noch – die Entscheidung auch selbst erklären können. Eine große dänische Bank setzt in der Geldwäscheprävention das XAI-Framework LIME (Local Interpretable Model-Agnostic Explanations) ein, um die relevanten Faktoren zu extrahieren und visuell darzustellen.

Die Einsatzfähigkeit smarter Systeme hängt eng mit der Erklärbarkeit und Nachvollziehbarkeit ihrer Entscheidungen zusammen. Gelingt es, die Blackboxes selbstlernender Algorithmen zu öffnen, ist eine große Verbreitung autonomer Systeme zu erwarten. «

Claudio Ceccotti
ist Senior Consultant Artificial Intelligence bei Sopra Steria Consulting.

claudio.ceccotti@soprasteria.com

Gemeinsam mehr Sicherheit

Gesellschaften und Sozialsysteme weltweit führen einen harten Wirtschafts- und Innovationswettbewerb. Dieser beschränkt sich aber nicht nur auf die Entwicklung besserer Technologien und Produkte. Bedingt durch die starke digitale Vernetzung ist die Menge von Spionage- und Sabotagevorfällen dramatisch gestiegen. Durch einen verbesserten Wissensaustausch und eine engere Zusammenarbeit bei der Entwicklung neuer Lösungen können sich die Unternehmen besser und kostengünstiger gegen Angriffe schützen.

© avdeev007/iStock/Getty Images

In Deutschland herrscht immer noch die Meinung vor, die Wirtschaft sei ein „ehrlicher Sport", unfaire Methoden seien zu unterlassen. Dies ist aber realitätsfern. Wir sollten uns dem neuen Wettbewerb konsequent stellen und alle unsere Stärken einsetzen:

» Erstens kann unsere Innovationskraft gestärkt werden, wenn wir unsere intellektuellen Kapazitäten effizienter nutzen. Dazu sollten Forschungsstätten viel direkter und enger mit Unternehmen zusammenarbeiten. Als Folge müssten die Unternehmen allerdings lernen, Forscher als Geschäftspartner ernst zu nehmen und die durch Know-how-Transfer erzielten Gewinne fair zu teilen.

» Zweitens sollte der Schutz von Unternehmen nicht als Wettbewerb, sondern als Gemeinschaftsaufgabe gesehen werden. Aktuell verfolgt jedes Unternehmen ein eigenes Sicherungskonzept und tauscht sich nur gelegentlich über Verbände mit anderen Martktteilnehmern aus. Dies führt aber zu hohen Kosten und zu einem schwachen Abwehrriegel.

Sinnvoller wäre eine zentrale Institution, die ein umfassendes, breit einsetzbares Schutzkonzept zur Verfügung stellt und alle angeschlossenen Organisationen bei der Implementierung unterstützt. Flankierend sollte sie laufend über aktuelle Bedrohungen und beobachtete Angriffen informieren. Die Kosten für die zentrale Koordination könnten aus den Einsparungen der Einzelunternehmen gedeckt werden.

Praktische Umsetzung

Einzelne Punkte einer solchen gesamtheitlichen Abstimmung hat die gemeinnützige Gesellschaft zur Förderung des Forschungstransfers e.V. (GFFT) bereits umgesetzt. So hat sie gemeinsam mit Sopra Steria Consulting ein „Security Lab" gegründet, das zentrale Sicherheitsservices entwickelt und umsetzt.

Zum Beispiel dienen sogenannte GFFT Technology Races dem direkten Wissensaustausch zwischen Sicherheitsverantwortlichen. In diesem Rahmen werden aktuelle Innovationsthemen für Workshops in regionalen Ballungsräumen aufbereitet. Im Bereich Security stehen derzeit die Absicherung Kritischer Infrastrukturen, Schwachstellen bei der Codierung und mögliche Kostensenkungen durch Automatisierung im Fokus.

Neben der Organisation des Wissenstransfers skizziert das Security Lab auch technische Lösungen, die es für die Verbesserung der Sicherheit für unerlässlich hält. Diese werden mit interessierten Unternehmen besprochen und als Gemeinschaftsprojekt aufgesetzt. Im Fall einer Realisierung werden führende Technologiepartner und Institute eingebunden.

Der Weg zu einem übergreifenden Verständnis von Sicherheit ist weit, aber wenn man keine ersten Schritte unternimmt, wird man dort nicht ankommen. «

Dr. Gerd Große
ist Vorstandsvorsitzender des GFFT e.V.

managementkompass@faz-institut.de

Sicherheitsfaktor Mensch

Sicherheitsvorfälle sind immer auch Organisationsversagen, da Technik von Menschen und Prozessen gesteuert wird. Angreifer verwenden Social Engineering, um Menschen zu manipulieren. Aber der Mensch sollte nicht nur als Schwachstelle innerhalb eines Sicherheitskonzepts gesehen werden, denn er kann selbst Sicherheitsvorfälle erkennen und verhindern. Eine entsprechende Sensibilisierung und fachliche Ausbildung unterstützen ihn dabei.

Informationssicherheit bezieht sich allzu oft auf die Technik und deren Schutz, seien es Firewalls, Passwörter und Verschlüsselungen sowie Sicherheitstüren und Kameras am Serverraum. Eine weitaus wichtigere Rolle spielt jedoch der Mensch. So gibt es Angriffsmethoden wie das verbreitete Phishing, bei dem mehr oder weniger gut gestaltete E-Mails verschickt werden, um Opfer dazu zu bewegen, geheime Zugangsdaten auf manipulierten Webseiten einzugeben. Ausgefeiltere Angriffe setzen auf typische menschliche Verhaltensweisen. Damit werden in Telefongesprächen Zugangsdaten erschwindelt, oder es werden Informationen für einen späteren Angriff gesammelt.

Sechs manipulierbare Verhaltensweisen

Derartige Angriffe setzen bei dem sogenannten Instinktverhalten von Menschen an, das angeboren ist und durch Schlüsselreize ausgelöst werden kann. Solche Verhaltensweisen können nicht einfach „abgeschaltet" werden. Nicht nur geschulte Social-Engineering-Angreifer nutzen diese Verhaltensweisen aus, sondern auch Marketing- und Verkaufsspezialisten. Die Sozialpsychologie hat bisher sechs solcher Verhaltensweisen identifiziert: Reziprozität, Konsistenz, soziale Bewährtheit, Autorität, Sympathie und Knappheit.

Reziprozität bedeutet, dass man den Gefallen eines anderen durch eigenes wohlwollendes Verhalten erwidern will. Konsistenz sagt aus, dass man ein gegebenes Versprechen oder eine Zusage einhält. Wer in eine unbekannte Situation gerät, verhält sich meist so wie die Menschen um ihn herum – das ist soziale Bewährtheit. Autorität oder Symbole von Autorität manipulieren ebenfalls das menschliche Verhalten – seien es Uniformen oder akademische Titel. Menschen, denen wir augenscheinlich sympathisch erscheinen, sind uns in der Regel ebenfalls sympathisch, und Optionen, die knapp und damit wenig verfügbar sind, erscheinen uns als wertvoller als die möglichen Alternativen.

Schutz vor und mit Menschen

Wie kann sich ein Unternehmen vor derartigen Angriffen schützen? Zu einfach gedacht ist es, Menschen nur als Sicher-

heitsrisiko einzuordnen und sie durch technische und organisatorische Maßnahmen einzuschränken. Diese Herangehensweise reicht nicht aus, da sich menschliche Herausforderungen nicht allein mit technischen Maßnahmen lösen lassen. Denn dem Menschen und Mitarbeiter fällt in der Unternehmenssicherheit auch eine aktive Rolle zu, die deshalb nicht zu sehr eingeschränkt werden sollte. Mitarbeiter sind ein wertvolles Asset, das es klug zu nutzen gilt.

In jedes Sicherheitskonzept gehört eine verhaltenswissenschaftlich fundierte Security-Awareness-Kampagne. Ziel einer solchen Kampagne ist es, Mitarbeiter für das Thema Sicherheit zu interessieren und zu sensibilisieren. Dazu ist es notwendig, die Mitarbeiter bereits im Vorfeld dafür zu motivieren und die Kampagne an den jeweiligen Bildungsstand bezüglich IT-Sicherheit anzupassen.

Man sollte allen Mitarbeitern die eigene Rolle und ihre Wichtigkeit im Sicherheitskonzept des Unternehmens klarmachen. Gelingt dies nicht, ist das Sicherheitskonzept von vornherein zum Scheitern verurteilt.

© RawpixelIStock/Thinkstock/Getty Images

Es reicht aber nicht aus, die Mitarbeiter nur zu sensibilisieren. Schließlich sollen sie ihr Verhalten ändern und eigene Sicherheitskompetenzen entwickeln. Dazu ist es notwendig, in einem weiteren Schritt Schulungen zu relevanten Sicherheitsthemen anzubieten. Neben technischen Fragen wie sicherer Passwortwahl, sicherem Verhalten in öffentlichen Netzen oder dem Einsatz von Kryptografie gehört in jedem Fall auch Social Engineering auf die Agenda. Hier ist es notwendig, wirklich alle Mitarbeiter zu schulen – auch solche, die keinen Zugang zu Computern haben, dafür aber Schlüssel zu den Büros.

Social-Engineering-Schulung am Arbeitsplatz

Alle sollten über die Gefahren von Social-Engineering-Angriffen aufgeklärt werden. Dabei ist es wichtig, auch die psychologischen Grundlagen für solche Attacken darzustellen. Typische Warnsignale für Manipulationen menschlichen Verhaltens gehören ebenfalls in den Lehrplan. Aus didaktischen Gründen ist es sinnvoll, auch Schulungsvideos zum Thema anzubieten. Darüber hinaus sind Beispiele aus der Praxis und Fallstudien, die in Gruppen analysiert werden, bewährte Methoden, um über Social Engineering aufzuklären. Webbasierte Trainings können ebenfalls eingesetzt werden, sollten aber von Präsenzveranstaltungen flankiert sein.

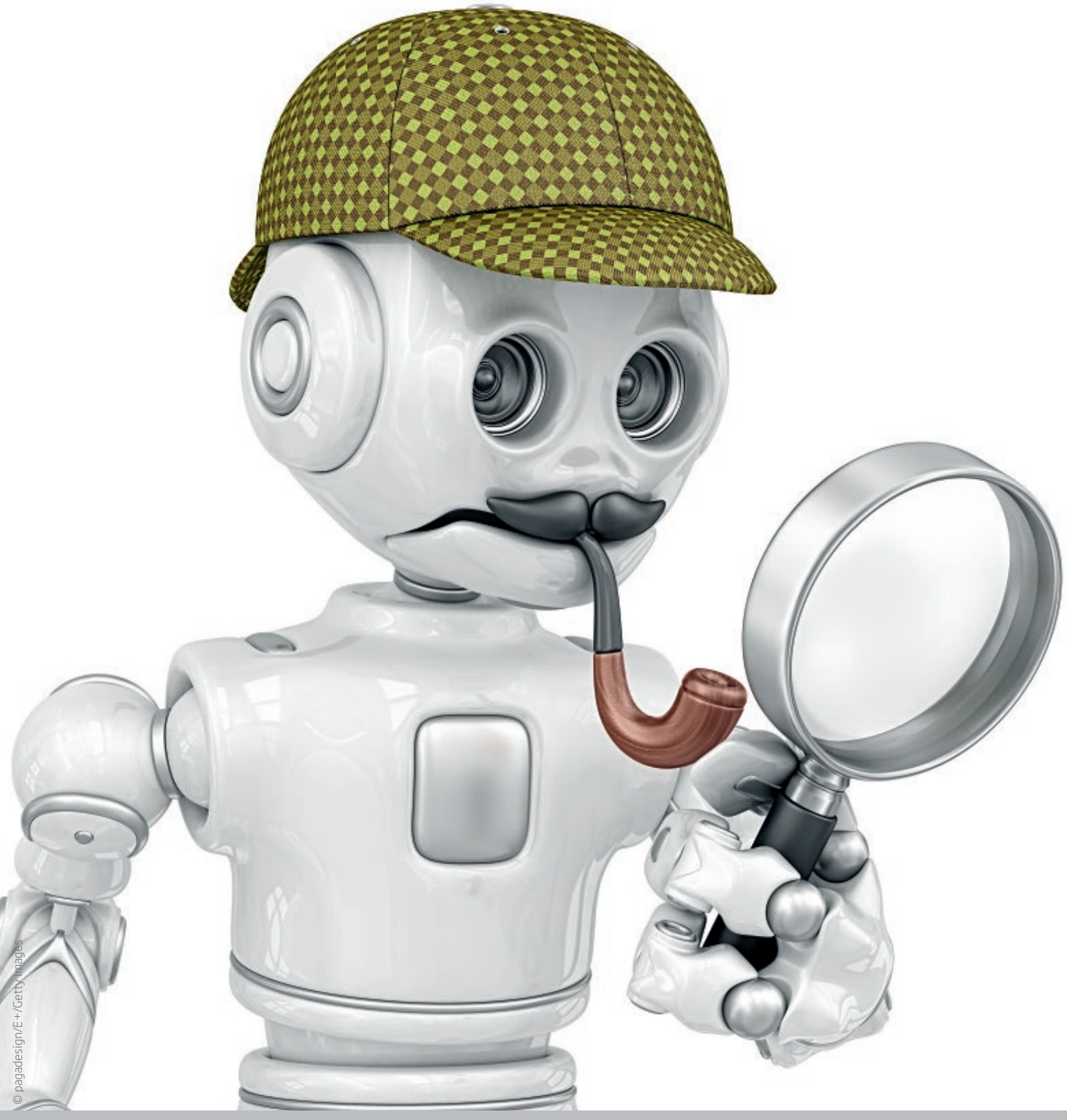
Wichtig ist der Transfer des erworbenen Wissens an den Arbeitsplatz. Mögliche Hemmnisse sind bereits im Vorfeld zu identifizieren und auszuräumen. In der Praxis heißt dies, dass die Mitarbeiter frühzeitig in die Planung einbezogen werden und dass die Inhalte an ihre Bedürfnisse angepasst werden. Nach den Schulungen sollten die Mitarbeiter genügend Zeit haben, um ihr Verhalten anzupassen.

Unterstützend kann solch eine Kampagne durch Werbemaßnahmen begleitet werden, beispielsweise durch Poster, Flyer, Webseiten oder sogar ein Maskottchen. Nicht zu vergessen ist hierbei auch die Vorbildfunktion der Managementebene. Nimmt diese sich selbst von den Sicherheitsmaßnahmen aus, funktioniert eine Security-Awareness-Kampagne nicht. Und auch nach der Einführungsphase sollten die Mitarbeiter laufend zum Thema betreut und geschult werden. «

Stefan Schumacher
ist Geschäftsführender Direktor des Magdeburger Instituts für Sicherheitsforschung.

managementkompass@faz-institut.de

Digitale Forensik – mit Spürsinn gegen Cybercrime



Sind Unternehmen oder Behörden von einem IT-Sicherheitsvorfall betroffen, stellen sich schnell die Fragen nach der Ursache, nach dem genauen Tathergang und nach den Verursachern beziehungsweise Tätern. Wenn sich Hinweise auf eine Straftat ergeben, müssen gerichtsverwertbare Beweise gesichert werden. In volatilen IT-Umgebungen ist dies nicht gerade einfach, doch die digitale Forensik liefert eine Reihe geeigneter Methoden und Werkzeuge. Allerdings bleiben eine gute Vorbereitung für den Ernstfall und die Unterstützung durch erfahrene Spezialisten unabdingbar.

Wenn vertrauliche Informationen von einer internen Datenbank entwendet werden oder eine verdächtige Software Verbindungen vom internen Netzwerk zu unbekannten Servern im Ausland herstellt, können daraus Schäden für die betroffenen Unternehmen, für deren Kunden und für Geschäftspartner entstehen. Es liegt deshalb im Interesse der Unternehmen, solche Vorfälle schnell und gründlich aufzuklären.

Eine gute Aufklärung unterstützt auch die Strafverfolgung und schafft die Grundlage für Schadenersatzforderungen gegenüber Tätern, falls diese ermitteln werden sollten. Außerdem werden Schwachstellen identifiziert, und es lassen sich Präventivmaßnahmen einleiten, um künftige Vorfälle zu verhindern. Nicht zuletzt liegt die Strafverfolgung von IT-Angriffen im öffentlichen Interesse, da potenziell jedes Unternehmen, jede Organisation und auch Privatpersonen Opfer werden können.

Auf Spurensuche

Jegliche Nutzung von IT – sei es die erwünschte durch Mitarbeiter oder die unerwünschte durch Angreifer – hinterlässt digitale Spuren. Diese lassen sich auch bei größter Sorgfalt nicht vollständig beseitigen. Soweit die gute Nachricht bezüglich der Aufklärung von IT-Angriffen. Die schlechte Nachricht lautet, dass sich die Spuren auf einer Vielzahl unterschiedlicher IT-Systeme befinden können. Dazu gehören Server, Netzwerkgeräte, Peripheriegeräte, mobile Geräte und alle Arten externer Medien wie USB-Sticks und USB-Laufwerke, Speicherkarten, CDs, DVDs oder Magnetbänder.

Die Interpretation solcher Spuren und das Erkennen von Zusammenhängen erfordern meist jahrelange Erfahrung. Unterstützend lassen sich Daten aus der Videoüberwachung und aus Zutrittssystemen sowie aus Sicherheitssystemen wie Malware-Schutz, Intrusion-Detection-Systeme, Content-Filter oder Firewalls und Proxies für die Analyse verwenden. Ein digitaler Tatort lässt sich zwar aufgrund der Vernetzung der IT-Systeme kaum verlässlich eingrenzen, doch es gibt immer ein IT-System, das der Auslöser und damit Ausgangspunkt für digitale Ermittlungen ist.

Bei einer „Post-mortem-Analyse" wird ein mutmaßlich in der Vergangenheit liegender und nicht mehr anhaltender Vorfall untersucht; der Täter hat gewissermaßen den Tatort bereits verlassen. Das Hauptaugenmerk liegt hier auf der Analyse von Datenspeichern und Protokollinformationen. Diese werden dann nach der Spurensicherung abseits vom Tatort genauer untersucht.

Demgegenüber wird bei der „Live-Forensik" versucht, unbemerkt vom Täter während seiner noch laufenden dolosen Handlung flüchtige Daten zu gewinnen und zu untersuchen. Diese beinhalten unter anderem sich verändernde Hauptspeicherinhalte, Netzwerkverbindungen sowie laufende Prozesse, die sich ebenfalls verändern. Ein IT-Forensiker muss dafür Zugang zu den betroffenen IT-Systemen erhalten.

Schlüssel zum Erfolg liegt in der Vorbereitung

Der erste Schritt ist die Erstellung einer „Digital Forensic Policy" (DFP), die verbindliche Leitlinien zur Herstellung der Einsatzbereitschaft („Forensic »

kurz & knapp

Weltweit sind

33 Prozent

der befragten IT-fernen Führungskräfte bereit, das **RISIKO EINER LÖSEGELDFORDERUNG** von Hackern einzugehen, wenn sie dadurch weniger in Datensicherheit investieren müssten.

Quelle: NTT Security (Risk: Value Report 2018)

Readiness") sowie Randbedingungen zur Durchführung forensischer Analysen vorgibt.

Die DFP legt zum Beispiel fest, dass eine forensische Analyse nur streng zweckgebunden zur Aufklärung eines Informationssicherheitsvorfalls durchgeführt werden darf, um nicht in Konflikt mit Regelungen zum Datenschutz zu geraten. Schließlich erhält der IT-Forensiker Zugriff zu einer Vielzahl von Daten, aus denen sich theoretisch auch Verhaltensweisen von an der Tat unbeteiligten Mitarbeitern ableiten lassen.

Ferner stellt die DFP Mindestanforderungen an das korrekte Handeln während einer forensischen Analyse. Dazu gehören meist folgende Punkte:

- Die Methoden müssen in der Fachwelt beschrieben und allgemein akzeptiert worden sein.
- Die Methoden müssen robust, funktional und legal sein, so dass das Ergebnis der Untersuchung möglichst ausgewogen, vollständig und nicht tendenziös ist.
- Die eingesetzten Hilfsmittel müssen transparent sein, und sie müssen bei einer Anwendung durch Dritte dieselben Ergebnisse aus dem Ausgangsmaterial liefern.
- Sichergestellte Spuren dürfen durch die Untersuchung selbst nicht verändert worden sein.
- Die Integrität digitaler Beweise muss jederzeit belegbar sein.
- Die Spurensicherung darf durch keine Personen durchgeführt werden, die potenziell an dem Informationssicherheitsvorfall beteiligt sind.
- Die Methoden müssen so ausgewählt werden, dass sie logisch nachvollziehbare Verbindungen zwischen Ereignissen und Beweisspuren und eventuell auch Personen herstellen können.
- Jeder Schritt des Untersuchungsprozesses muss angemessen dokumentiert werden.

Regelmäßige Übungen forensischer Analysen, die in das Security Incident Management integriert werden können, belegen die Funktionsfähigkeit der Abläufe im Ernstfall und stellen den fehlerfreien Umgang mit den Werkzeugen sicher.

Wenn eine forensische Untersuchung durch externe Experten unterstützt wird, müssen die Anforderungen der DFP vertraglich an den Dienstleister weitergegeben werden. Außerdem sollte der Dienstleister zu einer Rufbereitschaft mit kurzer Reaktionszeit und zu einem Vor-Ort-Einsatz verpflichtet werden.

Forensic Readiness durch passende Technik sichern

Nach der Verabschiedung einer DFP muss die IT-Forensik in bestehende Prozesse integriert werden. Forensic Readiness bedeutet in technischer Hinsicht,

dass IT-Systeme bestimmte Konfigurationen aufweisen müssen, etwa besondere Log-Einstellungen. Oder auf den Systemen wird bereits Software zur forensischen Analyse vorinstalliert, zum Beispiel zur Erstellung eines Speicherabbilds („Speicher-Dump").

Solche Werkzeuge haben meist keinen großen Speicherbedarf. Sie sollten zugriffsgeschützt sein, um Missbrauch zu vermeiden. Damit Integritätsverletzungen wichtiger Dateien oder Programme zügig feststellbar sind, sollten in regelmäßigen Abständen automatisiert Prüfsummen (Hash-Werte) dieser Daten gebildet und separat gesichert werden.

Für solche technischen Maßnahmen empfiehlt es sich, die IT-Forensik in den Prozessen der IT-Systembeschaffung, -entwicklung und -wartung zu verankern. Damit wird Forensic Readiness Teil des Lebenszyklus eines IT-Systems. Speziell für IT-Forensik notwendige Konfigurationen oder Werkzeuge sind idealerweise im zugehörigen IT-Sicherheitskonzept zu dokumentieren. Eine unverfälschte und verifizierte Zeitquelle, die für die Protokollierung im System benutzt wurde, ermöglicht dem IT-Forensiker, die Ereignisse in eine korrekte Reihenfolge zu bringen, selbst wenn ein Täter die Systemzeit manipuliert hat.

Organisatorisch den Überblick behalten

Die Aussagekraft von Untersuchungsergebnissen hängt von der Kenntnis des Einsatzzweckes der untersuchten Anwendungen und des erwünschten Ablaufs von Geschäftsprozessen ab. Denn nur wenn der Soll-Zustand bekannt ist, können Anomalien in Daten und Handlungen entdeckt werden.

Die gegenseitigen Abhängigkeiten von Prozessen sowie Berechtigungsschemata müssen bei einer forensischen Analyse jederzeit abrufbar sein. Für jeden Systemtyp, der möglicherweise forensisch analysiert werden muss, sollten beispielsweise aktuelle Daten zur Hardware und deren Standort, zu Konfigurationen, Kommunikationsprotokollen und Systemprozessen vorliegen. Dies gehört typischerweise zu den Aufgaben des Asset Management.

Daneben ist eine aktuelle Dokumentation des organisationsinternen Netzes erforderlich. Auf diese Weise lassen sich leicht passende Einsatzpunkte für forensische Werkzeuge und für Netzwerksonden eines Intrusion-Detection-Systems finden.

Die genannten Informationen und Daten müssen so zugänglich sein, dass der Zugangsweg selbst die Daten nicht verfälschen kann. Hierfür ist eine verschlüsselte Übertragung unabdingbar.

Durch geeignete Prozesse und Maßnahmen wie Rufbereitschaften und Vorabgenehmigungen ist außerdem dafür Sorge zu tragen, dass jederzeit Personal bereitsteht, um einen Zugriff durchzuführen.

> *„Die größte Verwundbarkeit ist die Unwissenheit."*
>
> *Sunzi (chinesischer Philosoph und Militärstratege, 534 bis 453 v. Chr.)*

Schließlich müssen für einen reibungslosen Ablauf die Rollen und Verantwortlichkeiten aller Beteiligten und die Schnittstellen festgelegt werden. Mit Schulungs- und Awareness-Maßnahmen ist sicherzustellen, dass sich die beteiligten Personen bei forensischen Untersuchungen richtig verhalten, um nicht etwa versehentlich Informationen zu zerstören.

Unternehmen mit einer geeigneten DFP, die darüber hinaus alle notwendigen technischen und organisatorischen Maßnahmen getroffen haben, um „forensic ready" zu sein, haben gute Chancen, Angriffe rechtzeitig zu erkennen und zu dokumentieren.

Wenn es einem Täter trotz Sicherheitsmaßnahmen gelingen sollte, die Verfügbarkeit, Vertraulichkeit oder Integrität von Informationen in einem Unternehmen oder einer Organisation zu verletzen, muss er angesichts der bereitstehenden digitalen Forensik mit einer schnellen Aufklärung und einer wirksamen Strafverfolgung rechnen. «

Dr. Gerald Spiegel
ist Senior Manager im Bereich Information Security Solutions bei Sopra Steria Consulting.
gerald.spiegel@soprasteria.com

Kenne deinen Gegner

Hacker entwickeln stetig neue Methoden, um in Netzwerke einzudringen. Damit IT-Systeme effektiv geschützt werden können, müssen Unternehmen verstehen, wie Angreifer denken, sagt Prof. Dr. Thorsten Holz, Inhaber des Lehrstuhls für Systemsicherheit an der Ruhr-Universität Bochum.

Herr Professor Holz, warum wird jemand zum Hacker?

Es gibt ganz unterschiedliche Motive. Das Spektrum reicht von Personen, die ihre technischen Fähigkeiten demonstrieren wollen und keine finanziellen Absichten verfolgen, bis zu staatlich gesponserten Angreifern, die Regierungen ausspionieren und – im Extremfall – sogar Wahlen beeinflussen. Dazwischen liegt die kriminelle Szene, in der sich Angreifer über Spam, Phishing oder Kreditkartendiebstahl bereichern. Auch Wirtschaftsspionage gehört hierher: Hacker wollen Informationen über Patente, aktuelle Produktentwicklungen oder über Kunden stehlen. Eine weitere Gruppe sind „Hacktivisten", die aus politischer Überzeugung handeln. Hacker bewegen sich auf einem schmalen Grat: Es kommt darauf an, wie die Technik eingesetzt wird – offensiv oder defensiv.

Prof. Dr. Thorsten Holz
ist Inhaber des Lehrstuhls für Systemsicherheit an der Ruhr-Universität Bochum.

„Der Angreifer muss einen Weg finden, um die IT-Schutzmechanismen zu überwinden. Der Verteidiger muss alle Wege kennen."

Wie machen Hacker Schlupflöcher in der IT ausfindig?

Wie ein Hacker vorgeht, ist vom Ziel seines Angriffs und vom Netzwerk abhängig. Am Anfang steht die Recherche, um einen Weg ins Netzwerk zu finden. Dabei werden potenzielle Sicherheitslücken gesucht. Wenn der Angreifer hier nicht weiterkommt, kann er über Phishing, Social Engineering oder ein Telefonat versuchen, Mitarbeiter des Unternehmens auf eine bestimmte Webseite zu locken. Manchmal wird sogar ein infizierter USB-Stick auf dem Parkplatz des Zielunternehmens hinterlassen – in der Hoffnung, dass ein Mitarbeiter den Datenträger am Arbeitsplatz öffnet.

Hat ein Hacker die Kontrolle über einen Computer des Netzwerks erlangt, wird es einfacher für ihn. Dann kann er die Netzwerkumgebung und dazugehörige Passwörter ausspähen. Entscheidend ist es, auf einen strategisch bedeutenden Server zu gelangen und beispielsweise E-Mails mitzulesen.

Existiert ein Verhaltenskodex unter Hackern?

Angenommen ein unabhängiger IT-Sicherheitsforscher entdeckt eine Schwachstelle: Für diesen Fall gibt es den Verhaltenskodex „Coordinated Disclosure". Dieser besagt, dass die Sicherheitslücke dem Hersteller gemeldet werden muss. Typischerweise vereinbaren Entdecker und Hersteller, dass die Schwachstelle innerhalb von 90 Tagen beseitigt werden muss. Geschieht dies nicht, veröffentlicht der Entdecker die Information.

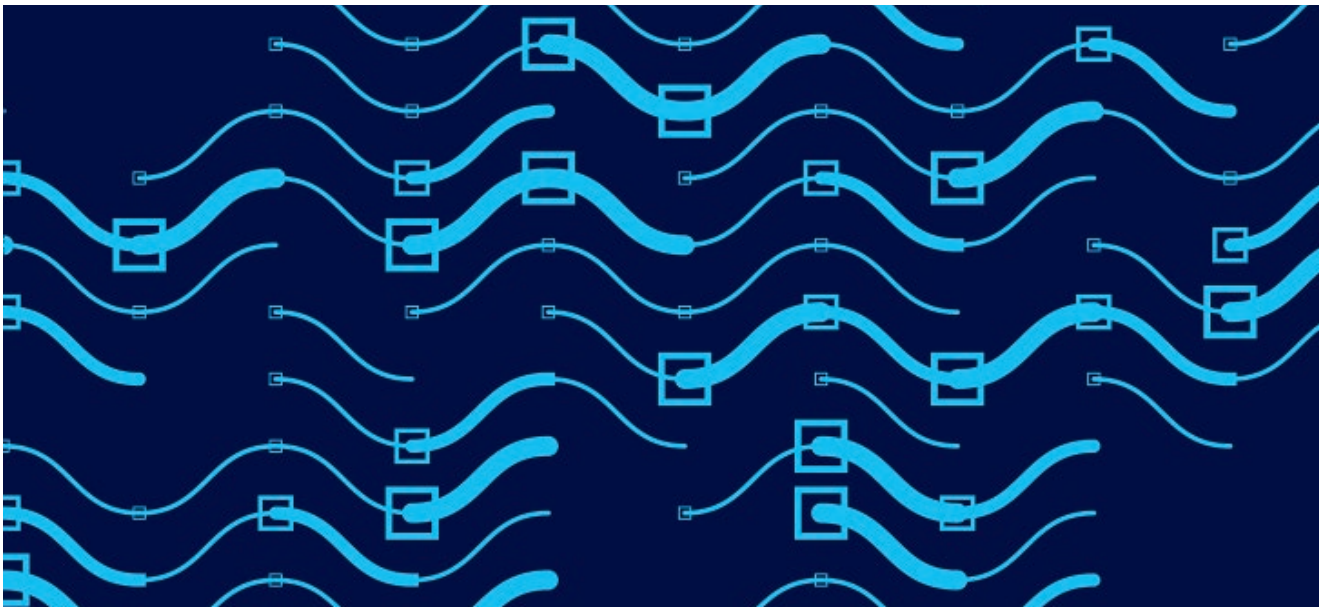
Kommen Unternehmen als Arbeitgeber für Hacker in Frage?

Durchaus: Die meisten Konzerne haben ein Computer Emergency Response Team (CERT), eine Art digitale Feuerwehr. Solche Teams entwickeln Richtlinien und Strategien zur Reaktion auf IT-Sicherheitsvorfälle. In großen Unternehmen gibt es neben einem „Blue Team" für Cyber-Abwehr auch ein „Red Team". Dieses handelt wie ein Angreifer und simuliert das Eindringen in die Unternehmens-IT.

Als Unternehmen allein reaktiv vorzugehen ist also der falsche Weg?

Das zeigt die Praxis deutlich! Deshalb ist IT-Sicherheit zunehmend auf Managementebene angesiedelt. Ein IT-Sicherheitsvorfall kann das Aus für ein Unternehmen bedeuten, insbesondere wenn sensible Informationen gestohlen werden. Je digitaler unser Leben, desto wichtiger die Daten.

Das Interview führte Georg Poltorak. «



Flow Records auswerten

Firmennetze werden immer häufiger zum Ziel von Cyber-Attacken. Eine der wichtigsten Gegenmaßnahmen besteht darin, möglichst viele Angriffswege von vornherein auszuschließen. Bei der IT-Sicherheit müssen dabei in jedem Fall auch die Datenschutzvorgaben für Mitarbeiter beachtet werden. Flow Record Fingerprinting stellt einen geeigneten und wirtschaftlich effizienten Ansatz dar, beide Anforderungen zu erfüllen.

Für den Schutz eines komplexen Firmennetzes muss die IT-Abteilung wissen, welche Betriebssysteme und Software firmenweit genutzt und welche Informationen übertragen werden. Oft ist das Netz aber nur unvollständig dokumentiert. Manche Nutzer betreiben außerhalb der eigenen Infrastruktur sogenannte Schatten-IT, installieren eigenmächtig Software oder nutzen Netzressourcen auf unvorhergesehene Weise. In der Regel verfolgen sie damit lautere Absichten, jedoch können Angreifer davon profitieren und im schlimmsten Fall Schaden anrichten. Jedes Unternehmen sollte daher die für den Zustand seines Netzes sicherheitsrelevanten Metadaten – also Daten zu den genutzten Daten – erheben, um einen besseren Überblick zu bekommen.

Aktive und passive Netzanalyse

Um den Zustand eines Netzes zu ermitteln, wurden in den vergangenen Jahren verschiedenste Verfahren entwickelt. Diese basieren zum einen auf einer aktiven Untersuchung des Netzes und den mit dem Netz verbundenen Geräten, zum Beispiel mit „Network Mapper" (nmap).

Zum anderen existieren passive Verfahren, die den Netzverkehr selektiv oder komplett analysieren, um aus den aufgezeichneten Daten Rückschlüsse auf das Netz zu ziehen. Ein einfaches passives Verfahren überprüft anhand der IP-Adressen der Kommunikationsteilnehmer beziehungsweise mit Hilfe des Domain Name System (DNS), ob zum Beispiel ein bestimmtes Gerät regelmäßig die Domain update.microsoft.com besucht. Durch diese Information kann man auf die Verwendung von Microsoft-Produkten schließen. Weitere sichtbare Informationen aus diesen Verbindungsdaten erlauben es, Rückschlüsse auf die eingesetzten Versionen zu ziehen.

Flow Records erlauben Rückschlüsse

Beim Flow Record Fingerprinting handelt es sich um ein passives Verfahren, das in den vergangenen »

Jahren entwickelt wurde. Es analysiert die Metadaten des Kommunikationsflusses, die sogenannten Flow Records. Diese Flow Records erlauben es, anhand der IP-Adresse, des verwendeten Protokolls, des übertragenen Byte-Volumens usw. Rückschlüsse auf die eingesetzte Software sowie die verwendete Version zu ziehen.

> *„Metadaten erlauben eine Bestandsaufnahme des untersuchten Netzes. Außerdem lässt sich erkennen, wenn ein Netzverhalten vom typischen Nutzerprofil abweicht. Die Erkennungsrate ist sehr hoch."*

Zu diesem Zweck werden bei allen Netzkomponenten automatisiert entsprechende Analysedaten erfasst. Basierend auf diesen Metadaten ist es dann mit Hilfe von Wahrscheinlichkeitsberechnungen und Analysen möglich, Informationen zum Netz abzuleiten und entsprechende Sicherheitsmaßnahmen zu planen.

In der Regel ist jede im Unternehmensumfeld eingesetzte Hardware in der Lage, Flow Records zu erfassen und an eine zentrale Stelle zu schicken. Hierbei ist es nicht von Relevanz, ob die Kommunikation direkt hinter dem Client, also dem ersten Gerät, das Serverdienste abruft, oder erst mehrere Geräte entfernt untersucht wird.

Metadaten übersetzen

Die im Netz gesammelten Metadaten lassen sich beispielsweise für die Berechnung des genutzten Datenvolumens je Endgerät verwenden. Außerdem kann man damit erkennen, wenn das Netzverhalten vom typischen Nutzerprofil abweicht. Neben der Untersuchung der Übertragungsdaten erlauben die Metadaten auch eine Bestandsaufnahme (Inventarisierung) des überwachten Netzes.

Bei korrekter Durchführung fällt die Erkennungsrate sehr hoch aus: In einer 2017 experimentell durchgeführten Untersuchung mit einem eigens eingerichteten Testnetz wurden 15.096 Datensätze erzeugt und analysiert. Über 92 Prozent der Betriebssysteme sowie mehr als 88 Prozent der untersuchten Anwendungen (Dropbox, SSH, TeamViewer, OpenOffice, Skype, MySQL) konnten korrekt klassifiziert werden. Der Rest wurde falsch zugeordnet.

Missbrauch möglich

Da sich die Erhebung von Flow Records auch auf große Unternehmensnetze skalieren lässt, ist die Methode bei IT-Architekten beliebt. Sie bringt jedoch auch Sicherheitsrisiken mit sich, zum Beispiel wenn externe Angreifer die Methode einsetzen. Da viele Softwareupdates meist nur für eine bestimmte Version geladen werden, eröffnet dies Angreifern die Möglichkeit, Rückschlüsse auf bestehende Sicherheitslücken zu ziehen und entsprechend klassifizierte Geräte gezielt anzugreifen. Erschwerend kommt hinzu, dass beim Flow Record Fingerprinting die überwachten Geräte nicht erkennen können, dass sie überwacht werden – die Datensammlung findet an den Kommunikationsknoten des Netzes und nicht direkt am Endgerät statt.

Unter der Annahme, dass die IT-Abteilung das Netz vor Angriffen Dritter abgeschottet hat und dass das Flow Record Fingerprinting ausschließlich zu lauteren Zwecken eingesetzt wird, kann man gerade als Endanwender beruhigt sein: Die Genauigkeit der Methode nimmt mit der Entfernung zum Endgerät immer weiter ab. Gerade in Unternehmensnetzen kommunizieren so gut wie immer mehrere Endgeräte über einen Netzknoten mit dem Internet. Nach außen hin verwenden sie dabei dieselbe IP-Adresse und sind nur schwer voneinander zu unterscheiden. Deshalb ist der Einsatz der Methode im World Wide Web sinnlos.

Sinnvolle Alternative

IT-Verantwortliche müssen den Überblick über die eigene Infrastruktur behalten. Da aus Datenschutzgründen in den meisten Fällen kein direkter Zugriff auf alle Systeme möglich ist, stellt die Methode der Flow-Record-Analyse eine erfolgversprechende Alternative zur klassischen Netzüberwachung dar. Die gewonnenen Metadaten helfen, Sicherheitsrisiken frühzeitig zu erkennen, und können damit wirtschaftlichen Schäden durch Cyber-Attacken vorbeugen. «

Christian Walonka
ist Consultant
bei it-economics.
cwalonka@it-economics.de

Wie bei der Blockchain der Datenschutz greift

Neben klassischen IT-Systemen in Unternehmen und Organisationen müssen auch neue Systeme mit innovativen Technologien wie der Blockchain DSGVO-konform arbeiten. Dies sollte bereits bei ersten Planungen zur Einführung einer Blockchain-Technologie berücksichtigt werden.

Spätestens seit Ende Mai 2018 muss die neue Datenschutzgrundverordnung (DSGVO) umgesetzt werden. Hierdurch werden die Rechte der Kunden bezüglich der Informations- und Auskunftspflicht von Organisationen gestärkt. Für Unternehmen heißt das, dass bestehende Systeme angepasst werden müssen, um die neuen Pflichten gegenüber den Kunden zu erfüllen. Abhängig von der IT-Architektur und der Komplexität des Systems kann dies aufwendig und teuer sein.

© ismagilov/iStock/Thinkstock/Getty Images

Neben den bereits vorhandenen müssen selbstverständlich auch neue datenverarbeitende Systeme und Technologien DSGVO-konform arbeiten. Die Blockchain-Technologie erfährt derzeit branchenübergreifend breites Interesse. Sie kann unterschiedliche Parteien über ein Netzwerk sicher miteinander verbinden, ohne dass zur Vertrauensbildung ein neutraler Intermediär notwendig ist. Innerhalb des Netzwerks können vertrauliche Transaktionen zwischen zwei oder mehreren Vertragsparteien durchgeführt werden, ohne dass ihre Identitäten offengelegt werden müssen. Möglicherweise lassen sich in manchen Branchen durch diese Technologie zentralisierte Marktplätze ersetzen (Disruption).

Zu den generellen Vorgaben der DSGVO gehören:

» Informationspflicht: Ein Unternehmen muss seinen Kunden innerhalb von vier Wochen Auskunft darüber geben können, welche personenbezogenen Daten zu welchem Zweck gespeichert werden.

» Recht auf Berichtigung: Haben sich personenbezogene Daten geändert, zum Beispiel der Nachname durch eine Heirat, oder wurden falsche Daten gespeichert, muss das Unternehmen diese umgehend korrigieren.

» Recht auf Löschung: Sind personenbezogene Daten für ein Unternehmen rechtlich nicht (mehr) erforderlich, etwa wenn ein Vertrag ausläuft, so muss das Unternehmen auf Wunsch des Kunden alle personenbezogenen Daten löschen oder sperren.

» Sichere Datenübertragung und Meldung: Unternehmen müssen dafür sorgen, dass personenbezogene Daten sicher übertragen werden. Des Weiteren müssen bei allen Datenschutzverstößen die Aufsichtsbehörden informiert werden. »

Die Blockchain hat gute Voraussetzungen für den Datenschutz

Unter den neuen Technologien spielt die Blockchain innerhalb der DSGVO aufgrund der besonderen Mechanismen zur Vertrauensbildung eine besondere Rolle. Auf den ersten Blick kann die Blockchain diesbezüglich sogar als „Musterplattform", gelten da alle Transaktionen zusammenhängend in Blöcken chronologisch sortiert, nachvollziehbar, manipulationssicher und redundant gespeichert sind. Deshalb kann jede betroffene Person eine sichere Auskunft darüber erhalten, welche personenbezogenen Daten zu welchem Zweck gespeichert werden. Somit erfüllt die Blockchain die Informationspflicht mit Leichtigkeit.

Eine Berichtigung personenbezogener Daten kann auf einer Blockchain lediglich durch eine neue Transaktion in einem neuen Block durchgeführt werden. Hierdurch wird der alte Datensatz allerdings nicht gelöscht. Es können alle Berichtigungen jederzeit nachvollzogen werden.

Löschen personenbezogener Daten erfordert Umweg

Auf einer Blockchain sind keine Löschvorgänge möglich. Dies ist sogar ihr wichtigstes und charakteristisches Merkmal. Denn nur so kann die Blockchain in einem dezentralen Netzwerk das Vertrauen in die Integrität der Daten gewährleisten. Doch damit ist die DSGVO-Vorgabe „Recht auf Löschung personenbezogener Daten" nicht ohne Weiteres zu erfüllen. Ersatzweise ist die Sperrung einzelner Daten in der Blockchain durchführbar, ohne dass damit die Blockchain komplett unbenutzbar würde.

Bei der Planung einer Blockchain sollte zunächst genau geprüft werden, ob überhaupt personenbezogene Daten zwingend im Datenmodell und in den Transaktionen enthalten sein müssen, damit der gewünschte Geschäftsprozess funktioniert. Sind personenbezogene Daten jedoch notwendig, dann ist darauf zu achten, dass diese auf einer separaten Datenbank in einer sicheren Umgebung gespeichert werden, die eine Löschung der personenbezogenen Daten erlaubt.

Eine empfehlenswerte Möglichkeit besteht darin, in der Blockchain nur einen sogenannten Zeiger zu speichern. Dieser verweist auf einen Speicherplatz, an dem die personenbezogenen Daten abgelegt sind. Mit Hilfe des Zeigers kann ein Leseberechtigter von der Blockchain aus auf extern zu lesende Daten zugreifen.

Außerdem wird auf der Blockchain der Hash-Wert der personenbezogenen Daten gespeichert. Der Hash-Wert wird durch eine mathematische Funktion („Einwegfunktion") aus den personenbezogenen Daten berechnet. Er stellt die Richtigkeit der verwendeten personenbezogenen Daten sicher.

Dies geschieht vereinfacht dargestellt, indem auf die personenbezogenen Daten die Hash-Funktion angewandt und der berechnete Hash-Wert mit dem Hash-Wert auf der Blockchain verglichen wird. Stimmen beide Hash-Werte überein, so handelt es sich bei den gelesenen Daten um die richtigen personenbezogenen Informationen.

Sollte ein Kunde die Löschung seiner Daten wünschen, können die personenbezogenen Angaben leicht in der separaten Datenbank gelöscht werden. Dann wären in der Blockchain weiterhin nur der Zeiger, der nun auf eine ungültige Adresse verweist, und der Hash-Wert gespeichert, mit denen sich die personenbezogenen Daten nicht mehr rekonstruieren lassen. Somit ist die DSGVO-Vorgabe des „Rechts auf Löschung" erfüllt.

Sichere Datenübertragung durch Authorisierung ergänzen

Die sichere Übertragung von Daten ist ein besonderes Merkmal der Blockchain-Technologie und damit DSGVO-konform. Allerdings muss auch der Zugriff auf die personenenbezogenen Daten im separaten Speicher bestimmte Authorisierungs- und Authentifizierungsanforderungen erfüllen, damit nur Berechtigte auf die Daten zugreifen können. Der notwendige Token hierzu könnte sicher in der Blockchain abgelegt werden.

Die Blockchain kann die Vorgaben der DSGVO also erfüllen. Das Recht auf Auskunft und auf Datenkorrekturen lässt sich gut umsetzen. Bezüglich Löschrechten müssen die Projektbeteiligten allerdings frühzeitig entscheiden, welchen (Um-)Weg sie einschlagen wollen. Denn einmal in eine Blockchain übertragene Daten können nachträglich nicht verändert oder gar gelöscht werden. «

Mustafa Cavus
ist Senior IT Architect und Head of Blockchain bei Sopra Steria Consulting.
mustafa.cavus@soprasteria.com

Dennis Heinemeyer
ist Volljurist und bei Sopra Steria Consulting im Bereich Informationssicherheit zuständig für Datenschutzrecht.
dennis.heinemeyer@soprasteria.com

Physikalisch sicher

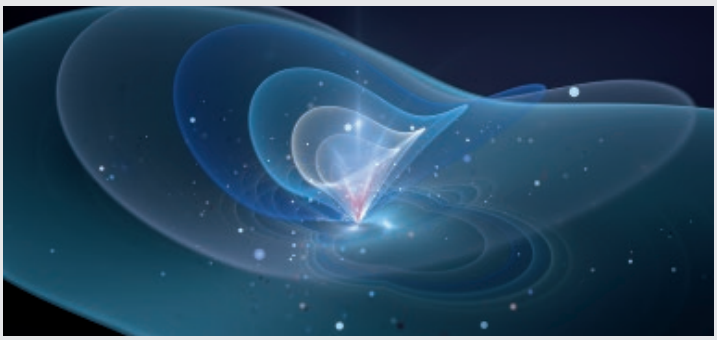
Wenn wir heute verschlüsselt Daten um die Welt schicken, lässt sich nicht mit 100 Prozent Sicherheit sagen, ob der Code entschlüsselbar ist. Denn selbst die trickreichsten Verschlüsselungsverfahren sorgen im Prinzip nur dafür, dass sich der Aufwand einer Entschlüsselung lediglich deshalb nicht lohnt, weil die benötigte Rechenleistung sehr groß ist. Quantenkryptografie verspricht dagegen – zumindest aus heutiger Sicht – „absolute" Sicherheit, weil hier Mathematik durch Physik ersetzt wird.

Die Sicherheit aktueller Verschlüsselungsmethoden basiert darauf, dass es enormer Rechenleistung bedarf, eine sehr große Zahl in ein Produkt aus Primzahlen zu zerlegen. Sicherheit entsteht somit durch viel Mathematik. Hingegen nutzen Quantencodes physikalische Gesetze, die sich nicht unentdeckt brechen lassen. Die Idee stark vereinfacht: Sogenannte Quantenobjekte erhalten ihre Eigenschaften erst dann, wenn sie gemessen werden. Versucht ein Angreifer mitzuhören, so ist dies nicht möglich, ohne dass er die Lichtquanten und damit die ursprüngliche Nachricht verändert und somit verfälscht. Er würde sofort auffliegen.

Verschlüsselungsverfahren ändern sich

Mit Hilfe von Quantencomputern können alle heutigen kryptografischen Algorithmen ohne große Probleme berechnet werden. Die schlechte Nachricht für alle Codedesigner von heute sowie für ihre Kunden und Arbeitgeber lautet deshalb: Die mathematischen Public-Key-Verfahren verlieren ihre Sicherheit, sobald Quantenrechner voll einsatzbereit sind. Physiker gehen zum Beispiel davon aus, dass ein Quantencomputer in zehn Jahren die heutigen Verschlüsselungsverfahren für die digitalen Signaturen der Blockchain innerhalb von 30 Minuten „knacken" kann.

Die gute Nachricht: Quantencomputer können nicht nur entschlüsseln, sondern auch verschlüsseln. Die Lösung liegt somit darin, Codes mit Hilfe der Quantentechnologie zu entwickeln und somit abhörsicher zu gestalten. In Unternehmen, Behörden und Haushalten stünde dann ein Sicherheits-Update von „biblischem" Ausmaß an. Denn sämtliche Netze und Systeme müssten auf neue Verschlüsselungsverfahren umgestellt werden, um noch als sicher gelten zu können.



© sakkmesterke/iStock/Thinkstock/Getty Images

Vorerst noch zu teuer

Dass sich die Quantenkryptografie eines Tages durchsetzen wird, kann angenommen werden. Aktuelle Experimente ermöglichen bereits die Übertragung kryptografischer Schlüssel über tausend Kilometer. Auch eine satellitengestützte Übertragung kryptografischer Schlüssel dürfte möglich sein.

Dennoch: Für das Ziel einer „absolut" sicheren Kommunikation muss nicht nur der Kommunikationskanal an sich sicher sein, sondern auch die eingesetzten Geräte auf Sender- und Empfängerseite dürfen nicht zu knacken sein. Für einen umfassenden und kommerziellen Einsatz ist die Quantenkryptografie noch nicht bereit. Die Quantenverschlüsselung und der Aufbau quantensicherer Kommunikationswege sind dafür noch zu kostspielig.

Angesichts der rasanten Entwicklung der Übertragungstechnik und mit Blick auf bereits fortgeschrittene Tests scheint der Durchbruch in nicht allzu weiter Ferne zu liegen. Dann werden Unternehmen und Regierungen dringend Experten mit Abschluss in Quantenkryptografie suchen, um – vereinfacht ausgedrückt – ein gigantisches Sicherheits-Patch zu erstellen. «

Darian Weber
ist Senior Consultant für Information Security Solutions bei Sopra Steria Consulting
darian.weber@soprasteria.com

Notfälle ganzheitlich managen

Für ein wirksames IT-Notfallmanagement empfiehlt sich ein integriertes Sicherheitssystem. Dazu gehören eine Notfallorganisation, ein Störungsmanagement sowie regelmäßige Notfalltrainings, damit im Ernstfall das Geschäft weiterlaufen kann.

Medien berichten fast täglich über IT-Sicherheitsvorfälle, so dass der Eindruck entsteht, im Grunde gebe es keinen wirksamen Schutz. Dennoch müssen Unternehmen ihr Know-how und ihre Kundendaten als wichtiges Gut schützen und IT-Ausfälle vermeiden.

Wie geht ein Unternehmen diese Aufgaben an? Den vielfältigen Schwachstellen hinterherzulaufen und permanent Lücken zu schließen bedeutet hohen Aufwand und Personalbindung. Letztlich bringt dieses Vorgehen nur kurzzeitig Erfolg, da immer neue Risiken und Schwachstellen auftauchen. Sinnvoller ist es, sich auf wenige Gefährdungen, die überall gegeben sind, zu konzentrieren. Die Verantwortung zu verlagern, etwa mittels Outsourcing und Cloud Services, ist ebenfalls eine Alternative. Doch selbst in diesem Fall bleibt die Verantwortung für die Sicherheit im Unternehmen. Ausschlaggebend für ein Outsourcing sollten daher nur die operativen Vorteile und Kosten sein.

Standards als roten Faden nutzen

Ein empfehlenswerter Ansatz besteht dagegen in einem „integrierten" Managementsystem, das die unterschiedlichen Sicherheitsaspekte abdeckt. Dazu eignen sich einschlägige Standards wie die ISO 27001 für Informationssicherheit und die ISO 22301 für Business Continuity. Diese liefern einen roten Faden für den Aufbau eines Managementsystems nach dem Stand der Technik.

Was wird hier in Sachen IT-Notfallmanagement gefordert? Folgende Punkte sind hervorzuheben:

- Aufbau einer Notfallorganisation, die beim Eintreten von gravierenden und katastrophalen Vorfällen auf den Plan tritt und die Behebung beziehungsweise Begrenzung des Notfalls steuert

- Betreiben eines Störungsmanagements (Incident Management) und Bearbeitung aktueller Meldungen des Computer Emergency Response Teams (Deutscher CERT-Verbund) über Schwachstellen

» Einrichtung kompetenter Notfallteams für die technische Notfallbehebung

» Regelmäßige Durchführung von Notfalltrainings, um Routine aufzubauen, aber auch um Schwachstellen aufzudecken

Ein zentraler Punkt ist die Analyse geschäftlicher Folgen: Man betrachtet einzelne Geschäftsprozesse und ermittelt deren sogenannte Kritikalitätsfunktion, das ist die mögliche Schadenhöhe in Abhängigkeit von der Dauer eines Ausfalls. Über einen „Vererbungsprozess" berechnet man Kritikalitäten von Teilprozessen und IT-Anwendungen und von genutzten IT-Ressourcen. Mit diesen Daten lassen sich zeitkritische Elemente erkennen, Single Points of Failure (die einen Komplettausfall bewirken würden) bestimmen und geeignete Kontinuitätslösungen finden. Schnell wird dabei klar, ob man mehr (kostspielige) Redundanz benötigt oder mit klassischen Wiederanlaufverfahren auskommt.

Nach gravierenden Vorfällen sind Meldepflichten zu beachten, etwa von Unternehmen aus Kritischen Infrastrukturen. Im Hinblick auf Ursachenforschung, Haftung und Strafverfolgung kann es erforderlich sein, eine IT-Notfall-Forensik zu betreiben, um gerichtsfeste Nachweise zu sichern. Auch für diese Themen gibt es Standards in der ISO-27000-Reihe.

Synergien mit anderen Systemen

Liest man die Standards, erscheinen sie zunächst sehr abstrakt. Wie kann man solche Vorgaben überhaupt in der Praxis umsetzen? Zunächst muss es das Ziel sein, unnötigen Verwaltungsaufwand zu vermeiden. Deshalb gleich der wichtige Hinweis: Am Anfang sollte eine qualifizierte Beratung stehen, um Klarheit zu schaffen und Aufwand zu begrenzen. Auch ein Schulungsbudget ist hier gut angelegt.

Durch den integrierten Ansatz – Datenschutz, Informationssicherheit, Business Continuity – lassen sich erhebliche Synergien nutzen. Dies gilt noch mehr, wenn im Unternehmen bereits standardisierte Managementsysteme (zum Beispiel nach ISO 9001) laufen. Der generelle Aufbau und die Prozesse sind nahezu identisch.

Die Vereinheitlichung von Risikoanalysen, Zuständigkeiten und Maßnahmen reduziert den Aufwand und vermeidet finanzielle Verluste sowie Image- und Motivationsschäden.

Gleichzeitig wird der Nachweis von Compliance (gegenüber Aufsichtsstellen und Kunden) erleichtert und die Abdeckung der wichtigsten geschäftlichen Risiken durch entsprechende Gegenmaßnahmen geleistet.

Ein solches Managementsystem kann außerdem zertifiziert werden und auf diese Weise das Image des Unternehmens in den genannten Handlungsfeldern stärken. Auch regulative Rahmenbedingungen und der internationale Wettbewerb fordern immer häufiger eine Zertifizierung.

Nicht stehenbleiben

Eine laufende Aktualisierung dieses Systems ist nötig, da regelmäßig neue Gesetze zu erfüllen sind, neue Risiken auftauchen, Geschäftsprozesse sich ändern, neue Kundenanforderungen entstehen, die Technologie wechselt usw. Deshalb sollte eine Überarbeitung des Managementsystems quasi „eingebaut" sein.

Das Feedback vieler Unternehmen zum integrierten Managementsystem lautet: Der Aufwand lohnt sich. Die Prozesse seien transparenter geworden, und die tägliche Sicherheitspraxis werde erleichtert. So wird Sicherheit auf allen Ebenen in qualifizierter, professioneller Weise gemanagt. «

CHECKLISTE FÜR EIN BUSINESS CONTINUITY MANAGEMENT

Folgende Punkte sollten abgedeckt werden:

- ☐ Führungsaufgaben des oberen Managements festlegen (Leitlinien, Notfallorganisation)
- ☐ Einrichten eines effektiven Change, Asset und Incident Management
- ☐ Ermittlung und Analyse der geschäftlichen Rahmenbedingungen
- ☐ Aufsetzen eines qualifizierten Risikomanagements
- ☐ Analyse der Business Impacts von Notfallsituationen (Kritikalitätsanalyse)
- ☐ Maßnahmen zum Umgang mit Risiken und Kritikalitäten
- ☐ Awareness- und Trainingsprogramme
- ☐ Steuern von Dokumentation und Aufzeichnungen
- ☐ Leistungsbewertung und kontinuierliche Verbesserung („Lessons learned")

Dr. Heinrich Kersten
ist Buchautor sowie Berater und Auditor für IT-Sicherheit.

managementkompass@faz-institut.de

Autonome Systeme verlangen Vertrauen

Die Autonomie technischer Systeme nimmt zu. Das hat Konsequenzen für die Gewichtung von Kontrolle und Vertrauen. Während nicht autonome Technik prinzipiell eher kontrollierbar ist, bestehen die Chancen von autonomen Anwendungen gerade darin, Kontrolle abgeben zu können. Doch dafür ist Vertrauen in die Technologie erforderlich.

Vertrauensvoll zu handeln bedeutet, Informationen aus der Vergangenheit in die Zukunft zu verlängern. Diese Haltung ist in Zeiten der Digitalisierung riskant, denn je höher die Wandlungsdynamik ist, desto weniger ähneln sich Vergangenheit und Zukunft. Doch wer jeden Vorgang kontrollieren will, bleibt im Mikromanagement der Geringfügigkeiten stecken. Für Ambitionierte gilt deshalb in der Regel: „Kontrolle ist gut, Vertrauen ist besser."

Kontrolle stößt an Grenzen

Vertrauen in die Technik gerät in der heutigen Veränderungsdynamik aber zum Dilemma: Im Umgang mit neuen Technologien ist ein gewisses Vertrauen in die Systeme unumgänglich. Denn deren Komplexität übersteigt zunehmend die Kompetenz und Kontrollfähigkeit der Menschen. Gleichzeitig steigt das Risiko, dass dieses Vertrauen enttäuscht wird.

VERTRAUEN STATT KONTROLLE

Delegieren bedeutet letztlich Kontrollverlust. Im Vertrauen auf die Eignung des Vertrauensempfängers setzt der Vertrauensgeber sich einem Risiko aus. Dabei kann das Risiko den erwarteten Nutzen übersteigen. Vertrauen ist aber keine rationale Kalkulation im Sinne einer Kosten-Nutzen-Optimierung. Dafür trägt Vertrauen auch dort, wo ungenügende Informationen zur Verfügung stehen und große Ungewissheit über künftige Entwicklungen herrscht.

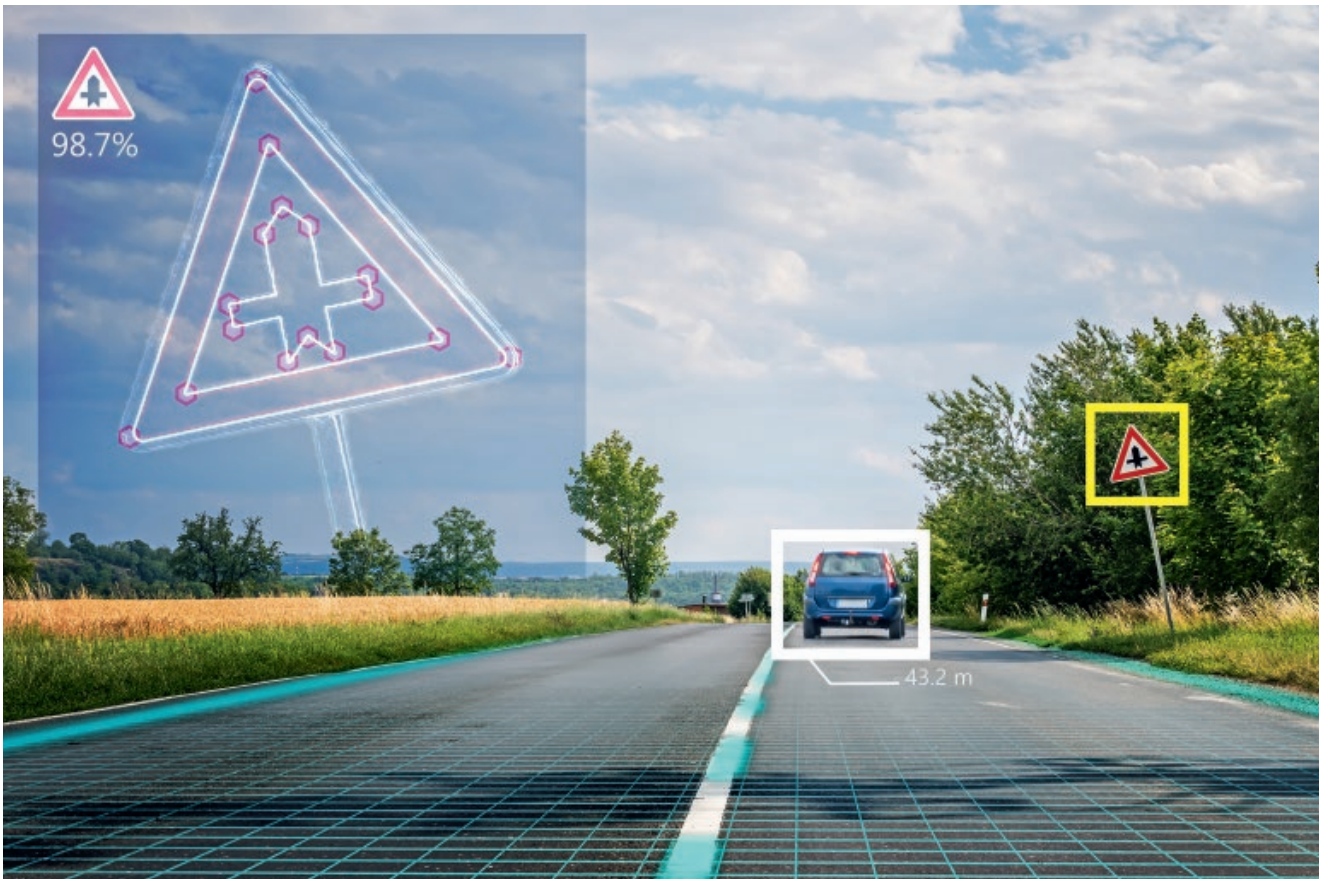
Zugleich ist für den Nutzer nicht immer klar, mit wem oder womit er in der digitalen Welt interagiert, wem oder was er demnach vertrauen sollte und was noch kontrollierbar ist. Wer mit einem Smartphone oder „Amazon Echo" kommuniziert, tritt in Verbindung mit einer Technosphäre voller Hintergrundbeziehungen aus Geräten, Netzwerken, Servern, Sensoren, Prozessen, Algorithmen, Filtern, Services und Geschäftsmodellen. Hinter jeder Entität stehen andere Akteure mit anderen Rechtssystemen, Logiken und Motivationen.

Wenn wir Dienstleistungen vernetzter Systeme nutzen, können wir unmöglich alle Prozesse aller Entitäten kontrollieren. Wegen der Eigendynamik dieser Systeme können wir die Kontrolle auch immer weniger an feste Kontrollinstanzen abgeben.

Das zwingt uns, entweder allen komplex zusammenwirkenden Teilen pauschal zu vertrauen oder jeglichen nicht kontrollierbaren Umgang einzustellen. Letztere Option verwehrt uns aber beispielsweise den Zugang zu den Vorteilen autonomer Systeme. Damit lassen wir die Chancen vieler innovativer Anwendungen ungenutzt.

Zum Vertrauen genötigt

Wenn weder Kontrolle noch Ausstieg Optionen darstellen, sind wir zum Vertrauen in Technik „genötigt". Gerade Entscheider werden jedoch versuchen, einen Zustand von Nötigung zu vermeiden. Denn sie sind verantwortlich für ihre Entscheidungen, auch wenn sie nicht alle Abläufe selbst gestalten können.



Wenn Investitionsentscheidungen nur zwischen nicht perfekten Optionen gefällt werden können – sollte man dann der bestmöglichen Option trotz Risikopotenzial vertrauen? Ein Beispiel: Die anfallenden Daten von Geschäftsprozessen müssen gespeichert und gesichert werden. Welche IT-Lösung man auch wählt, sie wird weder absolut sicher noch gänzlich transparent und kontrollierbar sein. Wegen der Vernetzung der Technosphäre – als Konsequenz aus Industrie 4.0 und Internet der Dinge – weiß allerdings keiner genau, was man „ungewählt mitwählt". Wie riskant das sein kann, zeigte 2017 ein Datenschutz-GAU, als die US-Wirtschaftsauskunftei Equifax gehackt und Kreditkarten-, Sozialversicherungs- und Ausweisnummern, also die digitalisierte Identität von mehr als 145 Millionen US-Amerikanern, gestohlen wurden.

Nur „falsche" Lösungen zur Auswahl

In einem Dilemma gibt es per definitionem keine richtige, sondern nur unterschiedliche falsche Lösungen. Das Vertrauensdilemma lässt sich nicht auflösen. Man muss es im Blick haben, denn schlimmer als eine falsche Lösung ist es, diese für richtig zu halten. Man sollte die soziotechnischen Entwicklungen so gestalten, dass Schadenspotenziale begrenzt bleiben. Vertrauensgeber sollten zumindest die Wahl haben, wem oder was sie Vertrauen schenken und an wen oder was sie Entscheidungen delegieren. Dies gilt für Nutzungsentscheidungen genauso wie für Entwicklungs- und Governance-Entscheidungen. Hier Spielräume zu eröffnen und zu verteidigen ist eine politische, kulturelle, rechtliche und gesamtgesellschaftliche Aufgabe und keineswegs nur die von Informatikern.

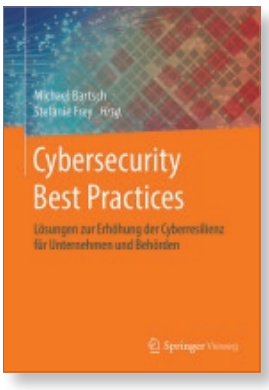
Die Entscheidung, autonome Technologien in allen Lebensbereichen einzusetzen, ist eine Entscheidung über künftige Spielräume. Vertrauen als bewusster Kontrollverzicht spielt eine elementare Rolle bei der Gestaltung dieser Möglichkeiten. Es wird darauf ankommen, die Dynamik der Vertrauensgabe so einzubetten, dass Vertrauen nicht fremdbestimmt abgenötigt wird, sondern dass es soweit möglich selbstbestimmt geschenkt werden kann. «

Dr. Bruno Gransche
ist Philosoph und Zukunftsforscher, derzeit am Forschungskolleg FoKoS der Universität Siegen.

managementkompass@faz-institut.de

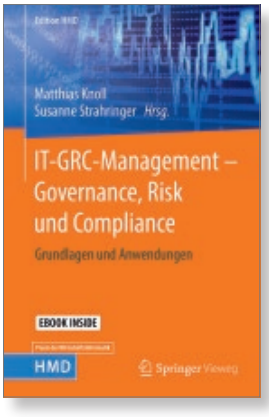
Buch & Web

FACHLITERATUR



Michael Bartsch und Stefanie Frey (Hrsg.):
Cybersecurity Best Pratices. Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden. Springer Vieweg 2018

Wie kann IT-Sicherheit gewährleistet werden? Und wie sollte man im Fall eines Cyber-Angriffs reagieren? Ein einheitliches Regelwerk dafür gibt es nicht. Deshalb haben Bartsch und Frey in ihrem Herausgeberwerk Best Practices und Strategieansätze renommierter, internationaler IT-Sicherheitsexperten zusammengetragen. Die Autoren aus unterschiedlichen Institutionen, Behörden und Unternehmen erläutern grundlegende Überlegungen und Ziele ihrer jeweiligen IT-Sicherheitsstrategie. Das kann Lesern dabei helfen , eigene Lösungsansätze zu entwickeln und umzusetzen.



Matthias Knoll und Susanne Strahringer (Hrsg.):
IT-GRC-Management – Governance, Risk und Compliance. Grundlagen und Anwendungen. Springer Vieweg 2017

Stetig komplexere IT-Systeme durchdringen alle Lebens- und Geschäftsbereiche. Deshalb müssen Governance, Risiken und Compliance im IT-Umfeld eines Unternehmens heute mehr denn je ganzheitlich gemanagt werden. Neben einer theoretischen Einführung in das Thema zeigt das Buch auch die Wechselwirkungen zwischen diesen drei Faktoren auf. Anhand praxisorientierter Fragestellungen wird die Notwendigkeit eines systematischen IT-GRC-Managements erläutert. Die Botschaft der beiden Herausgeber: Als Dreiklang innerhalb des IT-Managements ermöglichen Governance, Risk und Compliance Management eine nachhaltige Wertschöpfung.

LINKS

» **https://www.security-insider.de**
Online-Magazin mit aktuellen Nachrichten zu IT-Sicherheitsthemen, Fachartikeln, Ratgebern und Webcasts.

» **https://www.allianz-fuer-cybersicherheit.de**
Website der vom Bundesamt für Sicherheit in der Informationstechnik ins Leben gerufenen Allianz für Cyber-Sicherheit in Deutschland mit einem umfangreichen Informationsangebot und der Möglichkeit zur Meldung von Cyber-Angriffen sowie zum Austausch zwischen Unternehmen und Institutionen.

» **https://www.golem.de/specials/security**
Online-Nachrichtenportal, das mit Hintergrundberichten, Tests, Interviews und Analysen des Marktgeschehens Informationen zum Thema IT-Sicherheit liefert.

Constanze Kurz und Frank Rieger:
Cyberwar – Die Gefahr aus dem Netz. Wer uns bedroht und wie wir uns wehren können.
C. Bertelsmann 2018

Die IT-Sicherheitsexperten Kurz und Rieger warnen vor den Gefahren eines Cyber-Kriegs. Anlass dazu geben ihnen die immer zahlreicheren großangelegten Hacker-Angriffe der vergangenen Jahre. Diese werden durch die zunehmende Vernetzung in allen Lebensbereichen begünstigt. Die Autoren weisen auf das grundlegende Dilemma einer digitalisierten Gesellschaft hin: Bei den rapiden technologischen Veränderungen und dem wachsenden Druck auf Herstellerseite, stets der Erste sein zu wollen, werde die Systemsicherheit zunehmend vernachlässigt. Kurz und Rieger wollen dafür sensibilisieren, dass adäquater Schutz nur möglich ist, solange wir die Konsequenzen und Risiken unseres digitalen Handelns noch verstehen.

Kevin D. Mitnick mit Robert Vamosi:
Die Kunst der Anonymität im Internet. So schützen Sie Ihre Identität und Ihre Daten.
mitp 2017

Der eigenen Angaben zufolge „berühmteste (ehemalige) Hacker der Welt", Kevin Mitnick, zeigt zusammen mit Co-Autor Robert Vamosi, wie User mehr Privatsphäre im Internet erlangen. Die grundlegende Botschaft ihres Buchs: Jeder Mensch wird in jeder Situation beobachtet. Um diese These zu untermauern, verweisen die Autoren auf ihre eigenen Erfahrungen, und sie beschreiben reale Sicherheitsvorfälle und deren Konsequenzen für die Privatsphäre des Einzelnen. Mit praktischen Tipps zur Verschlüsselung von E-Mails, zum anonymen Surfen im Internet und mit einer Anleitung zum Passwortmanagement klären die Autoren ihre Leser über Sicherheitslücken auf und zeigen, wie ein individuell regulierbarer Grad an Anonymität erreicht werden kann.

Glossar

» Client
Computerprogramm, das auf dem Endgerät eines Netzwerks ausgeführt wird und mit einem Zentralrechner (Server) kommuniziert. Auch Endgeräte, die Dienste von einem Server abrufen, werden Clients genannt.

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

» Content-Filter
Ein System, das Webseiten oder E-Mails nach einzelnen Wörtern, typischen Phrasen, Bildern oder Links filtert.

» Digitale Forensik
Teilgebiet der Forensik, auch IT-Forensik, Computer- oder Netzwerkforensik genannt, das sich auf dolose Handlungen, die mit IT-Systemen und Datenträgern durchgeführt werden, fokussiert.

» Firewall
Sicherungssystem, das ein Netzwerk oder Computer vor unerwünschten Netzwerkzugriffen schützt.

» Flow Record Fingerprinting
Passives Verfahren, das die Metadaten des digitalen Kommunikationsflusses, die sogenannten Flow Records, analysiert. Diese erlauben es, anhand der IP-Adresse, des verwendeten Protokolls und des übertragenen Byte-Volumens Rückschlüsse auf die eingesetzte Software zu ziehen.

» Hack Back
„Digitaler Gegenangriff": Seit dem Angriff auf die IT-Systeme des Deutschen Bundestags im Jahr 2015 beschäftigen sich deutsche Behörden mit der Frage, wie man offensiv auf Cyber-Angriffe reagieren kann.

» Hash
Hash-Funktionen reduzieren große Datenmengen auf kleine Werte (Hashs), um durch einen Wertevergleich – auch absichtlich herbeigeführte – Integritätsverletzungen von großen Datenmengen feststellen zu können.

» IKT
Informations- und Kommunikationstechnik. Auch: ITK.

» Industrie 4.0
Die intelligente Vernetzung von Maschinen und Abläufen in der Industrie.

» Internet der Dinge
Vernetzung und Interaktion von Maschinen, Geräten und Anwendungen über digitale Plattformen. Auch: Internet of Things (IoT). Das IoT ist Treiber für die Digitalisierung der Logistik und Basis für die Industrie 4.0.

» Intrusion-Detection-System
System zur Erkennung von Angriffen gegen Computer oder Rechnernetze.

» Inventarisierung
Bestandsaufnahme von Hardware, Software und Lizenzen in einer Organisation.

» Kryptotrojaner
Software, die getarnt auf den Rechner gelangt und dort die Festplatte verschlüsselt. Damit wird die Festplatte unbenutzbar und kann erst nach Zahlung eines Lösegeldes wieder verwendet werden. Auch: Ransomware.

» Live-Forensik
Der Fokus liegt auf der Sicherung und Analyse flüchtiger Daten, wie dem Arbeitsspeicher, gestarteten Prozessen und bestehenden Netzverbindungen.

» Log-Einstellungen
Einstellungen für das Protokoll von Ereignissen eines Computerprogramms, das in einer Log-Datei oder einer Log-Datenbank gespeichert wird.

» Malware-Schutz
Schutz vor schädlicher Software, die Computer infizieren und Schaden anrichten kann. Malware sind zum Beispiel Viren, Würmer, Trojaner oder Spyware.

» „Man in the Loop"
Verfahren, dass die Interaktion eines Menschen erfordert. Auch: „Human in the Loop".

» Network Mapper (nmap)
Werkzeug zum Scannen und Auswerten von Zentralrechnern in einem Computernetzwerk.

» Post-mortem-Analyse
Forensische Analyse nach dem Ende eines Cyber-Angriffs.

» Proxy
Kommunikationsschnittstelle in einem Netzwerk.

» Quantenkryptografie
Einsatz quantenmechanischer Effekte in kryptografischen Verfahren.

» Security Incident Management
dient der angemessenen Bewältigung von IT-Sicherheitsvorfällen.

» Social Engineering
Psychotechniken, die das Verhalten von Menschen beeinflussen sollen, zum Beispiel um in IT-Systeme einzudringen.

» Speicher-Dump
Kopie oder Auszug eines Speicherinhalts. Auch: Speicherabbild.

» Explainable Artificial Intelligence (XAI)
Technische Disziplin, die nachvollziehbar macht, auf welche Weise Künstliche Intelligenz zu ihren Ergebnissen kommt.

Aktuelle Studien

Managementkompass
flexibel wachsen

Der wirtschaftliche, technische und gesellschaftliche Wandel vollzieht sich mit rasanter Geschwindigkeit. Damit Wachstum unter diesem Eindruck stattfinden kann, müssen sich Unternehmen flexibel aufstellen, Strategien miteinander kombinieren und Synergien aus altem und neuem Geschäft erzeugen. Dieser Managementkompass zeigt, dass das Strategieportfolio eines Unternehmens erst seinen Zweck erfüllen kann, wenn die dafür nötigen innerbetrieblichen Voraussetzungen geschaffen beziehungsweise interne Wachstumshürden abgebaut werden.

Branchenkompass
Banking

Um im Zuge der Digitalisierung konkurrenzfähig zu bleiben, müssen die Kreditinstitute ihre internen Prozesse und Geschäftsmodelle überdenken und modifizieren. Und ganz entscheidend: Die digitale Transformation muss von den Banken als Ganzes akzeptiert und umgesetzt werden. Wo stehen deutsche Banken in diesem Prozess? Wie gehen sie mit dieser Herausforderung um? Die Ergebnisse der Befragung von 109 Führungskräften aus der Finanzwirtschaft und die vertiefenden Interviews mit Spitzenvertretern aus der Branche geben hier Aufschluss.

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. Die Studie zeigt, dass sich die Arbeitsweise digital exzellenter Unternehmen auch für Organisationen mit gewachsenen Strukturen und IT-Systemen eignet.

IMPRESSUM

Sopra Steria SE
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: Dominik Heyer, Hannes Ludwig

Titelfoto: beanimages/Shutterstock.com

ISBN: 978-3-945999-71-4

Redaktion: Andrea van Baal, Eric Czotscher, Jacqueline Preußer, Georg Poltorak
Gestaltung und Satz: Christine Lambert
Lektorat: Juliane Streicher

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 SE
Corporate Communications
Birgit Eckmüller
Hans-Henny-Jahnn-Weg 29
22085 Hamburg
Telefon: (040) 2 27 03-52 19
E-Mail: birgit.eckmueller@soprasteria.com

F.A.Z.-Institut für Management-, Markt- und Medieninformationen GmbH
Jacqueline Preußer
Frankenallee 68–72
60327 Frankfurt am Main
Telefon: (069) 75 91-19 61
E-Mail: j.preusser@faz-institut.de

ISBN: 978-3-945999-71-4