IDG

COMPUTERWOCHE

Ausgabe 2017 – 32-33 7. August 2017 Nur im Abonnement erhältlich VON IDG

IT Security Automation

Unternehmen lernen den professionellen Umgang mit IT-Sicherheit nur langsam.

Seite 14

IoT-Plattformen

Device Development gewinnt an Bedeutung.

Seite 6

Datenschutz

DSGVO: Anwender unterschätzen ihre Pflichten.

Seite 34

Urlaub ist Urlaub ...

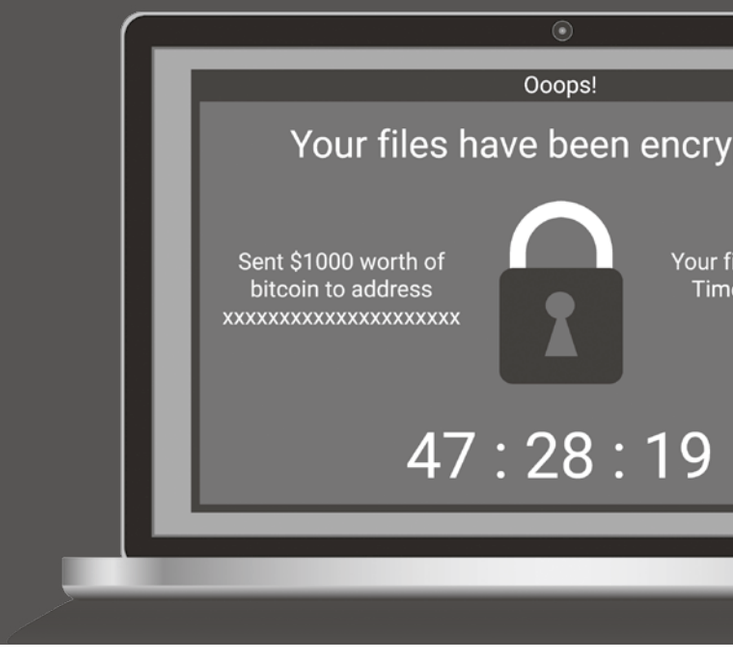
... und ständige Erreichbarkeit oft ein Problem.

Seite 38

IDG Business Media GmbH, DataM-Services GmbH, Postfach 9161, 97091 Würzburg

IT-Security-Automation bringt keine Sicherheit auf Knopfdruck

Virenscanner und Firewalls reichen schon lange nicht mehr aus, um Angriffe auf IT-Systeme abzuwehren. Eine zentrale Rolle werden Konzepte wie IT-Security-Automation spielen. Allerdings sind noch etliche Hürden zu nehmen, bis dieser Ansatz in der Praxis seinen vollen Nutzen entfalten kann. Das ist eines der Ergebnisse eines Roundtables der COMPUTERWOCHE zum Thema Automatisierung im Bereich IT-Sicherheit.



Von Bernd Reder, freier Journalist in München

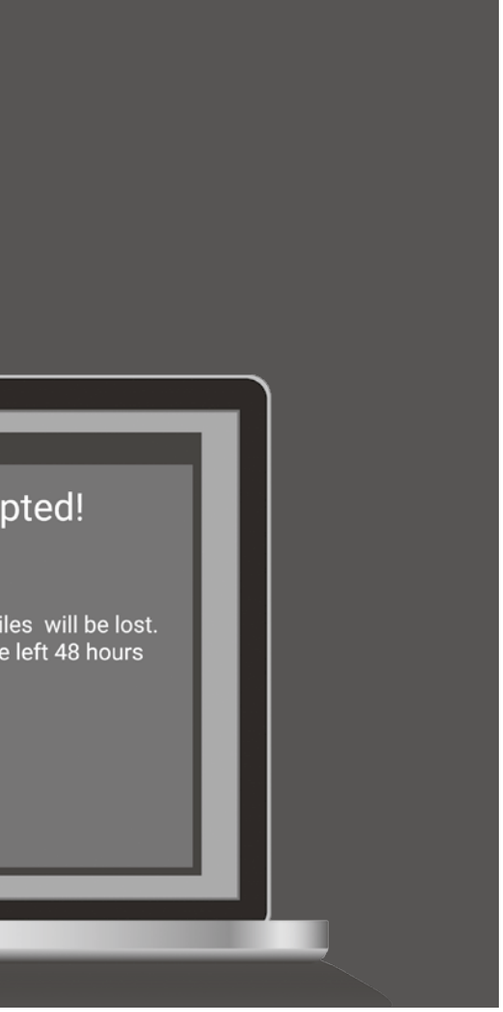
Die breit angelegte Attacke mit der Erpressersoftware „WannaCry“ hat in jüngster Zeit wieder einmal deutlich gemacht, wie anfällig IT-Systeme für Angriffe von Cyber-Kriminellen sind – auch Server, Arbeitsplatzrechner und Mobilsysteme von Unternehmen. „Gerade die Attacken mit Ransomware zeigen, dass zunehmend auch mittelständische Firmen in das Visier der Angreifer geraten“, so Tommy Grosche, Director Channel Sales Germany bei Fortinet, einem Anbieter von Produkten für die Netz- und Content-Sicherheit sowie Secure Access. Zusammen mit neun anderen Experten von führenden IT-Sicherheitsunternehmen nahm Grosche am COMPUTERWOCHE-Roundtable zum Thema Security Automation teil.

Eine zentrale Frage, die im Rahmen der Diskussionsrunde erörtert wurde: ob sich Angriffe auf die IT-Infrastruktur von Unternehmen und öffentlichen Einrichtungen wirkungsvoller abwehren lassen, wenn IT-Security-Systeme automatisch auf solche Attacken reagieren können. Handlungsbedarf besteht in jedem Fall, so Oliver Dehning, Chief Executive Officer von Hornetsecurity, einem Unternehmen, das sich auf Cloud-Security-Services spezialisiert hat: „Ein Faktor, der die Diskussion über IT-Sicherheit und Security Automation voranbringt, sind die verschärften gesetzlichen Vorgaben, vor allem die Datenschutz-Grundverordnung der EU. Solche Regelungen verlangen beispielsweise einen Security-by-Design-Ansatz.“

Sicherheit muss integriert sein

Das heißt, die IT-Sicherheitskonzepte von Unternehmen müssen Datenschutz und Informationssicherheit bereits bei Prozessen, Anwendungen, dem Daten-Management und Produkten berücksichtigen. Das erfordert einen ganzheitlichen Ansatz, so Benjamin Breu, Cyber Security Manager beim Beratungshaus Capgemini: „Wichtig ist, dass IT-Sicherheit ein integraler Bestandteil der Enterprise-Architektur ist.“ Andreas Süß, Vorstand und Chief Operating Officer bei iT-Cube Systems, einem Full-Service-Provider für IT-Sicherheit, geht noch einen Schritt weiter: „Bereits bei der Software- und App-Entwicklung sollte IT-Security eine zentrale Rolle spielen.“

Foto: iPIXEL PLUS/Shutterstock



Doch exakt an dieser ganzheitlichen Sicht fehlt es laut Hornetsecurity-CEO Dehning noch: „IT-Sicherheit ist mittlerweile auch in Branchen wie dem Automobilbau oder der Fertigungsindustrie hochrelevant. Das Problem besteht darin, dass IT-sicherheitsrelevante Aspekte häufig nicht per se in ein Produktdesign integriert werden." Das ist insofern problematisch, als Technologien wie die Vernetzung von „Dingen" (Internet of Things), Industrie 4.0 und Home Automation die Angriffsfläche für Hacker erheblich vergrößern. Daher sind nach Einschätzung der Diskussionsteilnehmer Konzepte wie IT-Security-Automation künftig unverzichtbar, um Angriffe proaktiv zu erkennen und schnellstmöglich zu unterbinden.

Anwender brauchen schärferes Bewusstsein

Doch ehe sie vorhandene IT-Sicherheitsansätze in Richtung Security Automation weiterentwickeln, müssen IT-Abteilungen und Business-Entscheider erst ihre Hausaufgaben machen. Dazu zählt, sich generell über die wachsende Bedeutung von IT-Sicherheit klar zu werden. Darüber sind sich alle Teilnehmer des Roundtables einig: „Die Awareness im Bereich IT-Sicherheit ist bei vielen Unternehmen noch ausbaufähig. Derzeit sind viele Unternehmen zu stark darauf fokussiert, Attacken durch externe Hacker abzuwehren. Viele vernachlässigen die Tatsache, dass auch die eigenen Mitarbeiter die Sicherheit der IT gefährden können", stellt beispielsweise Alexander Haugk fest, Senior Consultant und Trainer bei Baramundi Software. Das Kernprodukt des Unternehmens aus Augsburg ist eine modulare Suite für das Client-Management.

Daher ist es nicht verwunderlich, dass viele Unternehmen einen relativ neuen Ansatz wie das Automatisieren von Aktionen im Bereich IT-Sicherheit noch nicht „auf dem Radar" haben. „Automatisierung im Bereich IT-Security wird heute in den wenigsten Unternehmen zielgerichtet eingesetzt. Eigentlich könnte man sagen, dass diese Technologie noch in den Kinderschuhen steckt", so Matthias Straub, Director Consulting Services bei NTT Security. Das Unternehmen bietet insbesondere Services in den Bereichen Informationssicherheit und Risiko-Management an.

Vor allem bei kleinen und mittelständischen Unternehmen besteht Aufklärungsbedarf, was IT-Security-Automation betrifft. „Mittelständische Unternehmen stehen nach unserer Einschätzung in dieser Beziehung ganz am Anfang", bestätigt Joachim Braune, der als Chief Commercial Officer bei Netfox für die Geschäftsbereiche Cisco und Security zuständig ist. Dies ist Braune zufolge insofern bemerkenswert, als nach Angaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) bereits bei 19 Prozent der kleinen und mittelständischen Unternehmen IT-Sicherheitsprobleme zu massiven Störungen der Arbeitsprozesse geführt haben.

Security Automation wird wichtiger

Auch Hornetsecurity-Chef Dehning sieht Unterschiede zwischen großen und kleinen

Die Studie

Zum Thema „Security Automation" hat die COMPUTERWOCHE eine Multi-Client-Studie durchgeführt, in deren Rahmen IT-Entscheider befragt wurden. Die Untersuchung zeigt auf, in welchem Umfang Unternehmen und öffentliche Einrichtungen in Deutschland bereits Lösungen zur IT-Security-Automation einsetzen und welche Erfahrungen sie damit gemacht haben. Die Studie wird in Kürze im Online-Shop der COMPUTERWOCHE zur verfügung stehen:
shop.computerwoche.de/portal/navigation/marktstudien-66

Mit einem anderen zentralen Aspekt im Bereich IT-Sicherheit, der Cloud Security, beschäftigt sich eine weitere Studie, die IDG im vergangenen Jahr erstellt hat. Sie basiert ebenfalls auf einer umfassenden Befragung von IT-Führungskräften. „Cloud Security 2016" gibt einen umfassenden Überblick über den Stand von Sicherheitsmaßnahmen im Bereich Cloud Security und zeigt auf, wo Unternehmen Handlungsbedarf sehen.

Die Studie „Cloud Security 2016" steht als PDF ebenfalls im Shop der COMPUTERWOCEH zum Herunterladen bereit:
https://shop.computerwoche.de/portal/studie-cloud-security-2016-pdf-download-direkt-im-shop-5677

Matthias Straub, Director Consulting Services bei NTT Security: „Eine Lösung für Unternehmen, speziell kleinere und mittelständische, sind Managed Services im Bereich IT-Security und Security Automation. Sie bieten einen Effizienzgewinn."

Jochen Rummel, Regional Director DACH-Region bei FireEye: „Ein Problem besteht darin, dass es viel zu lange dauert, bis Angriffe als solche erkannt werden – teilweise mehr als 100 Tage!"

Oliver Dehning, CEO von Hornetsecurity: „Ein Faktor, der die Diskussion über IT-Sicherheit und Security Automation voranbringt, sind die verschärften gesetzlichen Vorgaben, vor allem die Datenschutz-Grundverordnung der EU."

- Unternehmen: „Das Wissen über IT-Sicherheit im Allgemeinen und speziell über IT-Security-Automation ist vor allem bei kleinen und mittleren Firmen noch ausbaufähig. Größere Unternehmen sind in diesem Punkt nach unserer Erfahrung weiter." Ein Grund für die zögerliche Haltung ist laut NTT- Security-Manager Straub, dass „zielgerichtete Angriffe fast 20 Jahre lang für die meisten Unternehmen kein Thema waren. Das hat sich nun geändert".

Unternehmen sehen sich mit Attacken konfrontiert, die eine deutlich höhere Durchschlagskraft haben als noch vor einigen Jahren. „Angreifer verfügen heute über erhebliche Ressourcen, und zwar in technischer wie personeller Hinsicht", warnt Jochen Rummel, Regional Director der DACH-Region bei FireEye. Das Unternehmen hat sich auf IT-Sicherheitslösungen spezialisiert, die den gesamten Sicherheitszyklus abdecken – vor, während und nach einem Angriff. Ein Problem, zu dessen Lösung Security Automation beitragen kann, ist Rummel zufolge, „dass es viel zu lange dauert, bis Angriffe erkannt werden – teilweise mehr als 100 Tage".

Ein Grund ist das Datenvolumen, das untersucht werden muss. „Bei der Analyse von Sicherheits-Events besteht das Problem darin, aus der Masse der Informationen die wirklich wichtigen, relevanten Daten herauszufiltern", konstatiert Benjamin Breu von Capgemini. Abhilfe kann eine automatisierte Analyse von sicherheitsrelevanten Daten schaffen, in Verbindung mit neuen Verfahren: „Technologien wie künstliche Intelligenz helfen dabei, große Datenmengen auf Spuren von Angriffen zu untersuchen", ergänzt NTT-Security-Mann Straub.

Standards müssen her

Zu den größten Herausforderungen aus Sicht der Anwender zählt, dass es keine schlüsselfertigen Security-Automation-Lösungen gibt. FireEye-Regionalchef Rummel: „Unser Ansatz ist daher, die mühevollen händischen Aufgaben von Security-Analysten zu automatisieren." Durch die Orchestrierung von wichtigen Prozessen von IT-Sicherheitslösungen sei es möglich, die Antwortzeiten und damit die Angriffsfläche zu reduzieren. Eine umgehende Reaktion auf Bedrohungen sei jedoch eine zentrale Anforderung an Security-Automation-Lösungen.

Dieser Ansatz erfordert, dass IT-Sicherheitskomponenten unterschiedlicher Couleur miteinander „sprechen" können. Doch daran hakt es noch, so die übereinstimmende Meinung der Teilnehmer des Roundtables. „Ein Punkt, der sich bei Security Automation als hinderlich erweist, sind Silos, die sich im Bereich IT-Sicherheit herausgebildet haben. Es gibt eine große Zahl von Lösungen, die nicht miteinander kommunizieren und nur für spezielle Aufgaben ausgelegt sind", kritisiert Andreas Süß von iT-Cube Systems. Ins gleiche Horn stößt Oliver Keizers, Regional Director DACH bei Fidelis Cybersecurit: „Viele IT-Fachleute, aber auch Experten aus Systemhäusern, denken noch zu sehr in Silostrukturen."

Immerhin haben die Anbieter von IT-Sicherheitslösungen die Problematik erkannt: „Ein Problempunkt von Security Automation ist, dass es bislang noch zu wenig herstellerübergreifende Standards gibt. Diese sind noch in Entwicklung", räumt Fortinet-Manager Grosche ein. Kritik wurde in der Runde jedoch in Bezug auf das Engagement einiger IT-Security-Anbieter laut, was die Mitarbeit an solchen Normen betrifft. „Einige nehmen nur und geben nichts", so eine der Anmerkungen zum Verhalten mancher Mitbewerber.

Der Faktor Mensch

Damit Security-Automation-Konzepte in der Praxis funktionieren, muss allerdings nicht nur Technik mitspielen. Gleiches gilt für den Menschen, also die Nutzer von IT-Systemen, die IT-Administratoren und die Security-

Fotos: NTT Security; FireEye; Hornetsecurity; Baramundi

Spezialisten. „Ein wesentlicher Punkt ist das Bewusstsein für Sicherheitsrisiken bei den Mitarbeitern. Nach unserer Einschätzung bestehen hier noch große Potenziale“, sagt beispielsweise Capgemini-Mann Breu. Sich darauf zu verlassen, dass IT-Security-Systeme automatisch Fehler oder das fahrlässige Verhalten von Mitarbeitern „ausbügeln“, ist demnach der falsche Weg. „Mitarbeiter müssen verstehen, welch hohen Stellenwert der Schutz von Daten und Anwendungen hat“, unterstreicht Joachim Braune von Netfox.

Ebenso wie einige andere Teilnehmer des Roundtables bietet FireEye weiterreichende Hilfsmaßnahmen: „Um Kunden auf den Ernstfall vorzubereiten, führen wir auf Wunsch Trockenübungen durch“, erläutert Rummel. „In diesen spielen wir den IT-Sicherheitsvorfall durch und überprüfen das Sicherheitsprogramm sowie die Incident-Response-Prozesse.“ Um die Reaktion auf Sicherheitsvorfälle zu optimieren, kommen laut Rummel auch Security-Automation-Technologien zum Zuge.

Einstieg über Managed Services

Die Erfahrungen, die Anwender mit dem Automatisieren von IT-Sicherheitsmaßnahmen gemacht haben, sind durchaus positiv, so Benjamin Breu von Capgemini: „Mit Hilfe von Security Automation können Unternehmen ihre Kosten im Bereich IT-Sicherheit um etwa 20 bis 30 Prozent senken; diese Budgets lassen sich dann direkt für Innovationen verwenden.“

Unternehmen, die sich trotz dieser handfesten Vorteile scheuen, ihre IT-Sicherheitslandschaft in einem Zug auf Security Automation umzustellen, können dies in mehreren Etappen tun: „Automatisierung im Bereich Sicherheit fängt mit einfachen Dingen an, etwa einem effektiven Patch-Management“, betont Alexander Haugk von Baramundi Software. „Häufig werden Updates, die Sicherheitslücken bei Software aller Art schließen, zu spät oder gar nicht eingespielt.“ Dies war auch im Fall von WannaCry so. Die Schadsoftware nistete sich vorzugsweise auf nicht gepatchten Windows-Rechnern ein.

Eine weitere Option, um von den Vorzügen automatisierter IT-Security-Prozesse zu profitieren, ist die Nutzung von gemanagten Diensten: „Speziell für kleinere und mittelständische Unternehmen sind Managed Services im Bereich IT-Security und Security Automation eine Lösung. Sie bieten einen Effizienzgewinn“, sagt Matthias Straub von NTT Security.

Auch Hornetsecurity-CEO Dehning plädiert für einen solchen Ansatz, um Einstiegshürden zu überwinden: „Für Unternehmen und öffentliche Einrichtungen ist es eine Überlegung wert, einen Security-Dienstleister oder Anbieter von Managed Services mit ins Boot zu holen. Dieser verfügt im Gegensatz zu hauseigenen IT-Abteilungen über das Know-how und die technischen Hilfsmittel, um Angriffe frühzeitig zu erkennen und gegebenenfalls zu stoppen.“ *(ba)*

Fazit

An IT-Security-Automation kommt mittelfristig kein Anwender vorbei, so die Einschätzung der Teilnehmer des COMPUTERWOCHE-Roundtables. Allein schon deshalb, weil Hacker-Angriffe schnellstmöglich abgefangen werden müssen, um den Schaden zu begrenzen. Dennoch werden Experten aus Fleisch und Blut nicht überflüssig. Sie müssen beispielsweise entscheiden, ob unternehmenswichtige IT-Komponenten oder Prozesse abgeschaltet werden können, wenn sie von Hacker-Attacken betroffen sind. „IT-Sicherheit auf Knopfdruck“ wird es somit auch weiterhin nicht geben. Einig waren sich die Experten in einem weiterem Punkt: Das Zusammenspiel der diversen Sicherheitslösungen muss verbessert werden, damit IT-Security-Automation in der Praxis funktioniert. Dazu ist es erforderlich, Standards zu erarbeiten und in den IT-Sicherheitslösungen zu implementieren. Doch auch die Anwender haben Hausaufgaben zu erledigen, so die Expertenrunde. Sie müssen ihr Bewusstsein für die Risiken schärfen, die mit dem Verlust unternehmenskritischer Daten verbunden sind, und es gilt Vorkehrungen gegen solche Attacken zu treffen.

Security-Herausforderung: Schneller reagieren auf immer komplexere Angriffe

Die Security-Verantwortlichen in den Unternehmen sind nicht zu beneiden: Die Attacken der Hacker werden immer raffinierter. Gleichzeitig gilt es, schnell auf die Angriffe zu reagieren, um die Schäden möglichst gering zu halten. Helfen kann dabei Security Automation, das haben die Sicherheitsspezialisten vielerorts erkannt, wie eine Studie der COMPUTERWOCHE ermittelt hat. Allerdings sind sie zumeist noch mit anderen grundlegenden Hausaufgaben beschäftigt.

Von Martin Bayer, Deputy Editorial Director

Die Bedrohung von IT-Infrastrukturen in den Anwenderunternehmen nimmt immer weiter zu. Das zeigt die COMPUTERWOCHE-Studie „Security Automation", für die im Juni dieses Jahres über 400 IT-Entscheider und Sicherheitsverantwortliche aus Unternehmen in Deutschland, Österreich und der Schweiz befragt wurden. Fast drei Viertel (73 Prozent) der Befragten identifizierten immer versiertere und komplexere Cyber-Angriffe als die größte Herausforderung in ihrem Sicherheitsbereich. Vor allem in kleineren Firmen ist das offenbar das größte Sicherheitsproblem. Vier von fünf Befragten aus diesem Bereich sprachen von einer wachsenden Bedrohung durch immer raffiniertere Hacker-Attacken.

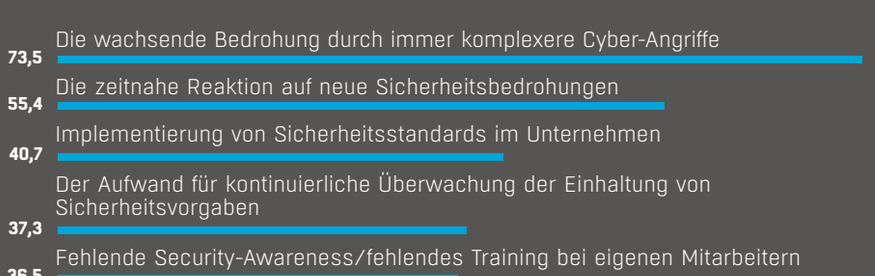
Der an zweiter Stelle genannte Aspekt in der Liste der größten Sicherheitsherausforderungen hängt unmittelbar mit dem erstgenannten Problem zusammen: Wie gelingt es, möglichst schnell auf neue Sicherheitsbedrohungen zu reagieren? 55,4 Prozent der Befragten halten das für die drängendste Aufgabe, die derzeit im Security-Umfeld zu lösen ist. Die Implementierung von Sicherheitsstandards (40,7 Prozent), die Überwachung, ob Sicherheitsvorgaben eingehalten werden (37,3 Prozent), und das nach wie vor fehlende Sicherheitsbewusstsein bei vielen Mitarbeiten (36,5 Prozent) rangieren mit deutlichem Abstand auf den weiteren Plätzen im Ranking der größten Herausforderungen.

Obwohl mehr als die Hälfte der Unternehmen bekundet, Cyber-Attacken müssten umgehend gestoppt werden, sobald sie entdeckt sind, steht das strategische Thema Security Automation auf der Agenda der wichtigsten Sicherheitsthemen für 2018 nicht ganz vorne. Stattdessen werden Maßnahmen wie das Absichern und Managen mobiler Endgeräte und Apps (56,4 Prozent) genannt sowie die Cloud Security (55,3 Prozent). Auch die neue Datenschutz-Grundverordnung (52,1 Prozent), die ab Mai 2018 greift, das IT-Sicherheitsgesetz (49,2 Prozent) sowie Techniken rund um Identity- und Access-Management (IAM, 43,4 Prozent) haben unter dem Security-Blickwinkel eine höhere Priorität. Security Automation folgt mit einem Anteil von 42,8 Prozent der Nennungen.

Obwohl die Automatisierung der Sicherheitsmaßnahmen also derzeit nicht mit allzu hoher Priorität vorangetrieben wird, dürfte ihre Bedeutung mittel- und langfristig steigen. Für die überwiegende Mehrheit der Studienteilnehmer

Die größten IT-Security-Herausforderungen

Was sind in in Ihren Augen für die Unternehmen die großen Herausforderungen in Bezug auf IT-Security?



Angaben in Prozent; Basis: n = 408, Mehrfachnennungen möglich, Top-5-Nennungen; Quelle: IDG

Wahrnehmung der Grundproblematik und der Notwendigkeit von Security Automation

Inwieweit können Sie den folgenden Statements zur IT-Security zustimmen?

„Ein Grundproblem ist, dass es viel zu lange dauert, bis bestimmte Arten von Angriffen überhaupt erkannt werden."

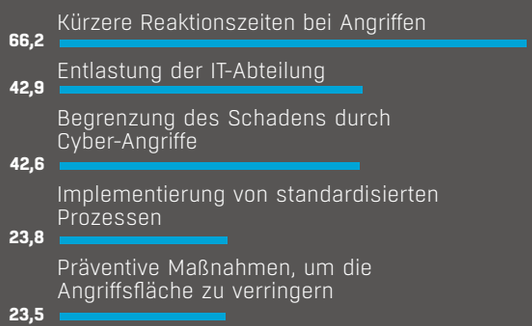
„IT-Security-Automation ist künftig unverzichtbar, um Angriffe proaktiv zu erkennen und schnellstmöglich zu unterbinden."

stimme voll und ganz zu | stimme zu | stimme eher zu

Angaben in Prozent; Basis: n = 408; Quelle: IDG

Die wichtigsten Vorteile automatisierter IT-Sicherheitslösungen

Welches sind für Sie die drei wichtigsten Vorteile von automatisierten IT-Sicherheitslösungen?



Angaben in Prozent; Basis: n = 408, Mehrfachnennungen möglich, Top-5-Nennungen; Quelle: IDG

(64 Prozent) stellt Security Automation einen wichtigen Baustein in ihrem künftigen Sicherheitskonzept dar. Offenbar haben die Verantwortlichen erkannt, dass die wachsenden Herausforderungen neue Lösungsansätze erfordern. Demnach sehen zwei Drittel (65 Prozent) der befragten IT-Entscheider ein Grundproblem darin, dass es viel zu lange dauere, bis bestimmte Arten von Angriffen überhaupt erkannt würden. Infolgedessen sei Security Automation in Zukunft unverzichtbar, um Angriffe proaktiv zu erkennen und schnellstmöglich zu unterbinden.

Jeder fünfte Umfrageteilnehmer (20,6 Prozent) gab an, automatisierte Sicherheitslösungen in jedem Fall einsetzen zu wollen. Weitere 62 Prozent erklärten, dies unter bestimmten Voraussetzungen tun zu wollen. Hier divergieren die Prioritäten allerdings je nach Unternehmensgröße. Während von den mittelgroßen (100 bis 999 Mitarbeiter) und den großen (ab 1000 Mitarbeiter) Unternehmen über 85 Prozent Security-Automation-Lösungen gegenüber aufgeschlossen sind, sind es bei den kleineren Firmen (unter 100 Mitarbeitern) nicht einmal drei von vier (73,9 Prozent). Nach Einschätzung von rund 40 Prozent der teilnehmenden Unternehmen sind hier Techniken wie künstliche Intelligenz zur Analyse von Angriffen ein Hoffnungsträger.

Als wichtigste Vorteile automatisierter Sicherheitslösungen sehen die Unternehmen kürzere Reaktionszeiten bei Angriffen (66,2 Prozent), die Entlastung der eigenen IT-Abteilung (42,9 Prozent) sowie die Begrenzung von Schäden durch Cyber-Angriffe (42,6 Prozent). Dagegen sieht nicht einmal jeder vierte Befragte Security Automation als präventive Maßnahme, um die Angriffsfläche zu verringern, beziehungsweise als Mittel, um standardisierte Prozesse zu implementieren. Die Kosten sind von untergeordneter Bedeutung. Gerade einmal 18 Prozent der Befragten identifizierten den monetären Aufwand als wichtigen Vorteil.

Auch an anderer Stelle spielt Geld nur eine untergeordnete Rolle – was aber durchaus kritisch zu bewerten ist. So plant derzeit gerade einmal jedes zehnte Unternehmen zusätzliche Investitionen in Security Automation und künstliche Intelligenz – trotz zunehmend kritischer Bedrohungslage. Um den Gefahren vorzubeugen, setzen Unternehmen eher auf Schulungen sowie die Aus- und Weiterbildung der eigenen Mitarbeiter (45,8 Prozent).

Wenn Investitionen geplant sind, dann fließen diese häufiger in klassische Security-Bereiche wie Backup- und Disaster-Recovery-Lösungen (44,9 Prozent), die grundlegende Sicherheitsarchitektur (42,6 Prozent), die IT-Security-Prävention (40,2 Prozent) oder in Security-Audits (30,9 Prozent). Grundsätzlich wollen die Verantwortlichen die Security-Fäden in der Hand behalten. Die Zusammenarbeit mit Anbietern für Managed-Security-Services (20,8 Prozent) oder ein verstärktes Outsourcing von IT-Security (16,7 Prozent) ist nur für einen kleinen Teil der befragten Unternehmen eine Option, um auf die steigenden Sicherheitsanforderungen zu reagieren.

Security-Lösungen sind zu komplex

Dass mehr Automatisierung notwendig wäre, zeigt indes die Beurteilung der bestehenden IT-Sicherheitslösungen. Anwender kritisieren vor allem, dass zu viele manuelle Eingriffe durch Administratoren notwendig seien (48,3 Prozent). Knapp vier von zehn Befragten monieren zudem eine zu hohe Komplexität der eingesetzten Security-Lösungen sowie deren schwierige Bedienung. Zudem wünschen sich die Unternehmen weniger voneinander abgeschottete Silolösungen (36 Prozent) sowie weniger Insellösungen (31 Prozent). Vor allem die großen Unternehmen mahnen an, dass die Lösungen unterschiedlicher Anbieter besser miteinander funktionieren müssten. In zu hohen Kosten für die aktuell eingesetzten Sicherheitslösungen sieht indes nur gut ein Viertel (26 Prozent) der Befragten ein Problem.

Nur eine offene Zusammenarbeit kann Cyber-Kriminelle aufhalten

Rund 55 Milliarden Euro Schaden haben Hacker im vergangenen Jahr hierzulande verursacht, rechnet der ITK-Branchenverband Bitkom vor. Nur wenn Unternehmen, Behörden und Gesetzgeber an einem Strang zögen, lasse sich verhindern, dass die Digitalisierung in einem Security-Desaster ende.

Von Martin Bayer, Deputy Editorial Director

Unternehmen müssen viel mehr für ihre digitale Sicherheit tun", warnte Bitkom-Präsident Achim Berg und verwies im gleichen Atemzug auf eine aktuelle Studie, für die über 1000 Geschäftsführer und Sicherheitsverantwortliche quer durch alle Branchen befragt wurden. Demzufolge sind mehr als die Hälfte der Firmen in Deutschland (53 Prozent) in den vergangenen beiden Jahren Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden. Den dadurch entstandenen Schaden beziffern die Experten auf rund 55 Milliarden Euro pro Jahr. „Die Studie zeigt, dass die Gefahr für Unternehmen aller Branchen und jeder Größe real ist", konstatierte Berg. Jeder könne Opfer werden.

Obwohl Security-Experten bereits seit Jahren vor steigenden Sicherheitsrisiken und Gefahren im Cyber-Raum warnen und mehr Anstrengungen für IT-Sicherheit anmahnen, hat sich die Situation nicht entschärft. Verglichen mit einer ersten Studie vor zwei Jahren ist der Anteil der Betroffenen gestiegen, von 51 auf 53 Prozent. Der von den Cyber-Kriminellen angerichtete Schaden ist sogar um rund acht Prozent von 51 auf 55 Milliarden Euro jährlich gewachsen.

„Unglaubliche Schadensbilanz"

Hans-Georg Maaßen, Präsident des Bundesamts für Verfassungsschutz (BfV), sprach mit Blick auf diese Zahlen von einer unglaublichen Schadensbilanz. Die Summe komme fast an den Staatshaushalt des Freistaats Bayern mit 58 Milliarden Euro heran. In Zeiten von Digitalisierung und Industrie 4.0 müsse man besonderes Augenmerk auf die Abwehr von Spionageangriffen auf die deutsche Wirtschaft richten, mahnte Maaßen. „Im Sinne eines ganzheitlichen und nachhaltigen Wirtschaftsschutzes gehören dazu nicht allein IT-bezogene Maßnahmen, sondern risikominimierende Pläne in den Bereichen Organisation, Personal und Sensibilisierung." Wichtig sei darüber hinaus auch die intensive Zusammenarbeit zwischen Wirtschaft und Behörden sowie den Behörden untereinander.

Noch scheint jedoch vieles Theorie. Nach wie vor fallen Unternehmen immer raffinierteren Hacker-Angriffen zum Opfer. Dabei sind die Interessen der Angreifer breit gefächert. In jedem sechsten Unternehmen (17 Prozent) wurden der Bitkom-Studie zufolge in den vergangenen zwei Jahren sensible Daten gestohlen. Vor allem Kommunikationsdaten wie

Fast 55 Milliarden Euro Schaden pro Jahr

	Schadenssummen (in Mrd. Euro)
Kosten für Ermittlungen und Ersatzmaßnahmen	21,1
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	17,1
Patentrechtsverletzungen (auch schon vor der Anmeldung)	15,4
Imageschaden bei Kunden oder Lieferanten/ negative Medienberichterstattung	15,4
Kosten für Rechtsstreitigkeiten	11,0
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	10,5
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	6,9
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	6,4
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	1,3
Sonstige Schäden	4,5
Gesamtschaden innerhalb der letzten zwei Jahre	**109,6**

Basis: Selbsteinschätzung aller befragten Unternehmen, die in den letzten zwei Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren, n = 571; Quelle Bitkom

E-Mails (41 Prozent) oder Finanzdaten (36 Prozent) seien in die Hände der Angreifer gefallen. In 17 Prozent der Fälle von Datendiebstahl wurden Kundendaten entwendet, in elf Prozent Patente oder Informationen aus Forschung und Entwicklung, in zehn Prozent Mitarbeiterdaten.

Viele wissen gar nicht, ob sie betroffen sind

Auch der Diebstahl von Hardware ist ein nicht zu unterschätzendes Problem. Knapp einem Drittel aller Unternehmen (30 Prozent) wurden in den vergangenen beiden Jahren IT- oder Telekommunikationsgeräte wie Notebooks und Smartphones gestohlen. Allerdings ist dabei in der Regel unklar, ob die Täter die Geräte selbst oder die darauf gespeicherten Daten im Visier hatten. Rund jedes fünfte Unternehmen berichtete, Opfer von Social Engineering geworden zu sein. Dabei versuchen die Angreifer, Mitarbeiter zu manipulieren, um an sensible Informationen wie Passwörter oder Zugangskennungen zu kommen, mit deren Hilfe dann im nächsten Schritt zum Beispiel Schadsoftware auf die Firmenrechner eingeschleust werden kann.

Jedes achte Unternehmen (zwölf Prozent) wurde Opfer von digitaler Sabotage, durch die beispielsweise die Produktion gestört wurde. Auffällig ist an dieser Stelle die hohe Dunkelziffer: So gaben weitere 29 Prozent der Befragten an, vermutlich von digitaler Sabotage betroffen gewesen zu sein. Diese Zahl macht deutlich, wie anfällig offenbar Produktionsanlagen hierzulande gegen Cyber-Attacken sind und wie unsicher die Verantwortlichen hinsichtlich des das daraus resultierenden Gefahren- und Risikopotenzials reagieren.

Kommissar Zufall

Dass im Aufbau funktionierender IT-Security-Strukturen in deutschen Unternehmen vieles im Argen liegt, zeigt auch die Art und Weise, wie die Unternehmen auf Datendiebstahl und Sabotage aufmerksam werden. Drei von zehn betroffenen Unternehmen gaben an, nur zufällig auf entsprechende Vorfälle gestoßen zu sein. 37 Prozent der Befragten erklärten, interne Einzelpersonen hätten die entscheidenden Hinweise zur Aufdeckung gegeben, und je 28 Prozent sagten, die eigene interne Revision beziehungsweise unternehmensexterne Personen hätten Alarm geschlagen.

IT-Sicherheitstechnik selbst scheint bei der Erkennung keine Rolle zu spielen. Lediglich ein Prozent der Unternehmen gab an, durch eigene Sicherheitssysteme, den Virenscanner beziehungsweise die Firewall auf sicherheitsrelevante Vorgänge aufmerksam geworden zu sein. Ob die Technik selbst versagt oder falsch eingesetzt wird, lässt sich an dieser Stelle allerdings nicht genau sagen.

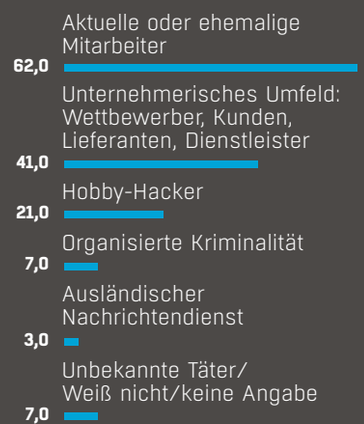
Die eigenen Mitarbeiter helfen zwar, IT-Sicherheitsvorfälle aufzuklären, sind aber am häufigsten auch die Täter. 62 Prozent der Unternehmen, die in den vergangenen zwei Jahren Opfer von Spionage, Sabotage oder Datendiebstahl wurden, haben die Täter im Kreis aktueller und ehemaliger Mitarbeiter identifiziert. Gut vier von zehn betroffenen Unternehmen (41 Prozent) machen Wettbewerber, Kunden, Lieferanten oder Dienstleister für die Angriffe verantwortlich, 21 Prozent geben Hobby-Hackern und sieben Prozent Personen aus der organisierten Kriminalität die Schuld. Ausländische Nachrichtendienste wurden in drei Prozent der Unternehmen als Täter identifiziert. Sieben Prozent der Unternehmen gaben an, dass die Täter unbekannt waren.

Mitarbeiter werden zu Tätern

Ein gutes Drittel der von Angriffen betroffenen Unternehmen (37 Prozent) berichtete, dass die Täter aus Deutschland kamen. Der Großteil der Angriffe wird jedoch aus dem Ausland gesteuert: 23 Prozent der Unternehmen identifizierten die Täter in Osteuropa, 20 Prozent in China und 18 Prozent in Russland. Danach folgen die

Mitarbeiter werden zu Tätern

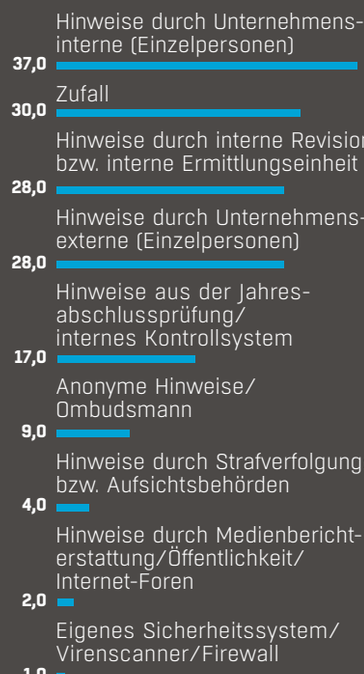
Von welchem Täterkreis gingen die Angriffe in den letzten zwei Jahren aus?



Angaben in Prozent; Basis: Alle befragten Unternehmen, die in den letzten zwei Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren, n = 571, Mehrfachnennungen möglich; Quelle Bitkom

Aufmerksame Mitarbeiter schlagen Alarm, Kommissar Zufall hilft

Wie ist Ihr Unternehmen auf diese Handlungen erstmalig aufmerksam geworden?



Angaben in Prozent; Basis: Alle befragten Unternehmen, die in den letzten zwei Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren, n = 571, Mehrfachnennungen möglich; Quelle Bitkom

- USA (15 Prozent), westeuropäische Länder (zwölf Prozent) und Japan (sieben Prozent).

Behörden bleiben außen vor

Bemerken die Unternehmen, dass Cyber-Kriminelle in die eigene IT-Infrastruktur eingedrungen sind, werden diese Fälle untersucht – das zumindest ist eine gute Nachricht. Lediglich drei Prozent der Unternehmen räumten ein, entsprechende Sicherheitsvorfälle auf sich beruhen zu lassen und keine weiteren Recherchen anzustoßen. Vor zwei Jahren reagierte noch jedes zehnte Unternehmen mit einer solchen Vogel-Strauß-Politik. 46 Prozent der Unternehmen leiten eine interne Untersuchung ein, externe Spezialisten wurden von 34 Prozent hinzugezogen.

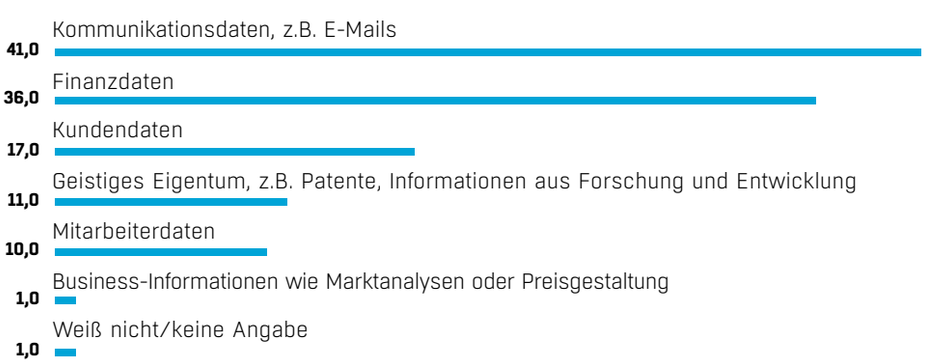
Als kritisch wird von Experten allerdings die weitverbreitete Praxis beurteilt, Behörden außen vor zu lassen. Nicht einmal jedes dritte betroffene Unternehmen (31 Prozent) wendet sich laut Bitkom an Behörden und bittet um Unterstützung bei der Aufklärung. Hauptgrund für diese Zurückhaltung ist die Angst vor Imageschäden (41 Prozent). Jedes dritte Unternehmen erklärte, man habe auf eine entsprechende Information verzichtet, weil man Angst vor negativen Konsequenzen habe (35 Prozent). Die Täter würden ohnehin nicht gefasst (34 Prozent), außerdem sei der Aufwand zu hoch (29 Prozent). „Nur wenn Unternehmen Angriffe melden, können die Sicherheitsbehörden ein realitätsnahes Lagebild erstellen und Abwehrstrategien entwickeln“, kritisierte Verfassungsschutz-Chef Maaßen das Misstrauen. „Es gilt der Grundsatz ‚Need to share‘, wenn wir gemeinsam die deutsche Volkswirtschaft widerstandsfähiger gegen Wirtschaftsspionage machen wollen.“

Angesichts der Studienergebnisse appellierten Vertreter des Bundesamts für Sicherheit in der Informationstechnik (BSI) an deutsche Unternehmer, Informationssicherheit mit höchster Priorität zu behandeln und mit den staatlichen Behörden zusammenzuarbeiten. „Die hohe Zahl der betroffenen Unternehmen zeigt deutlich, dass wir auf dem Gebiet der Cyber-Sicherheit in Deutschland noch Nachholbedarf haben“, warnte BSI-Präsident Arne Schönbohm. Zwar seien die großen Konzerne und insbesondere die Betreiber kritischer Infrastrukturen wie Stromversorger oder Wasserwerke in aller Regel gut aufgestellt, viele kleine und mittlere Unternehmen aber würden die Bedrohungen nicht ernst genug nehmen. „Informationssicherheit ist die Voraussetzung einer erfolgreichen Digitalisierung“, so Schönbohm. „Deshalb muss IT-Sicherheit Chefsache sein!“

Um ihre Appelle zu untermauern, verweisen die BSI-Verantwortlichen auf aktuelle Beispiele, die das Schadenspotenzial durch Cyber-Angriffe für die Wirtschaft aufzeigen würden. So hätten mit „WannaCry“ und „NotPeya“ in jüngster Vergangenheit zwei breit angelegte Cyber-Attacken erheblichen volkswirtschaftlichen Schaden angerichtet. In etlichen Unternehmen sei es zu massiven und lang anhaltenden Einschränkungen der Produktion oder geschäftskritischer Prozesse gekommen. Die Behörde forderte daher alle betroffenen Unternehmen auf, schwerwiegende IT-Sicherheitsvorfälle – gegebenenfalls auch anonym – zu

Unterschiedliche Daten geraten in die Hände der Diebe

Welche der folgenden Arten von digitalen Daten wurden in Ihrem Unternehmen gestohlen?



Angaben in Prozent; Basis: Alle befragten Unternehmen, die in den letzten zwei Jahren von Datendiebstahl von sensiblen Daten betroffen waren, n = 178, Mehrfachnennungen möglich; Quelle Bitkom

melden, und bietet mit dem Nationalen IT-Lagezentrum sowie der Allianz für Cyber-Sicherheit auch Anlaufstellen für betroffene Unternehmen.

Es fehlen die nötigen Security-Spezialisten

Das ist bitter nötig, denn auf Seiten der Unternehmen scheint es derzeit schwierig zu sein, der Security-Herausforderungen Herr zu werden. So schlägt der VDE (Verband der Elektrotechnik Elektronik Informationstechnik e. V.) Alarm, gerade einmal 13 Prozent der hiesigen Unternehmen sähen sich in Sachen IT-Sicherheit gut gerüstet. Mit der Digitalisierung würden die Probleme in Zukunft noch zunehmen. Für 88 Prozent der VDE-Mitgliedsunternehmen sei die IT-Sicherheit zwar wesentliche Voraussetzung für die Digitalisierung, hieß es. „Die Crux ist jedoch, dass viele Unternehmen nicht ausreichend IT-Spezialisten finden, die zum einen die Digitalisierung intern vorantreiben und zum anderen die Organisation vor externen Angriffen schützen", erklärte VDE-Chef Ansgar Hinz.

Die VDE-Unternehmen fürchten Hinz zufolge vor allem eines: den massiven Angriff auf ihre wertvollsten Divisionen Forschung und Entwicklung, IT und Produktion. Die Folgen wären in ihrem Umfang kaum absehbar: System- und Produktionsausfälle, Fehlfunktionen mit Folgen für Leib und Leben sowie Industriespionage. 71 Prozent der Unternehmen mit mehr als 5000 Mitarbeitern hätten dem Technologieverband zufolge bereits zugegeben, Opfer digitaler Angriffe geworden zu sein, doch die Dunkelziffer dürfte weitaus höher sein. Lediglich zehn Prozent seien der Meinung, dass Deutschland im internationalen Vergleich bei IT-Sicherheit eine führende Rolle spiele.

Sicherheit braucht eine Kultur der Offenheit

„Wir brauchen eine Kultur der Offenheit", forderte deshalb Hinz. Nur gemeinsam könne man den Hackern Paroli bieten. Vor allem der deutsche Wirtschaftsmotor Mittelstand müsse in Sicherheitstechnik investieren. „Wir wissen, dass viele kleinere Unternehmen nicht über die Ressourcen für eigene Computer Emergency Response Teams (CERTs) verfügen", konstatierte Hinz. Mit CERT@VDE hat der Technologieverband deshalb eine Plattform zur Koordination von IT-Security-Problemen im Bereich Industrieautomation ins Leben gerufen. „Auf ausdrücklichen Wunsch des Mittelstands", betonte der VDE-Chef. Auf einer anonymen Plattform könnten sich jetzt die Unternehmen vertrauensvoll austauschen. Der VDE unterstütze sie flankierend im Rahmen eines nichtkommerziellen CERT bei der Verbesserung ihrer Cybersecurity.

Tatsächlich scheinen neue Wege nötig, um die IT-Sicherheit in deutschen Unternehmen zu verbessern. Laut Bitkom-Umfrage haben viele Firmen zwar Maßnahmen ergriffen, um sich besser gegen Angreifer zu schützen. Dabei handelt es sich jedoch meist um Klassiker aus dem technischen Basisschutz wie etwa Passwörter, Firewalls und Virenscanner sowie regelmäßige Backups der Daten. Anspruchsvollere Maßnahmen seien dagegen eher selten, beispielsweise Intrusion-Detection-Systeme (20 Prozent) oder Penetrationstests (17 Prozent).

Nullachtfünfzehn funktioniert in Sachen Security nicht

Auch im Bereich der organisatorischen Sicherheit sind zumeist Standardmaßnahmen verbreitet, etwa die Festlegung von Zugriffsrechten für bestimmte Informationen (99 Prozent), die eindeutige Kennzeichnung von Betriebsgeheimnissen (85 Prozent) oder die Festlegung von Zutrittsrechten in bestimmte Unternehmensbereiche (81 Prozent).

Dagegen setze nur eine Minderheit auf Sicherheits-Zertifizierungen (43 Prozent) oder regelmäßige Sicherheits-Audits durch externe Spezialisten (24 Prozent). Nachholbedarf gibt es dem Bitkom zufolge auch im Bereich der personellen Sicherheit. Nur 58 Prozent der Unternehmen führen demnach Background-Checks bei Bewerbern für sensible Positionen durch, und nur jede zweite Organisation hat einen Sicherheitsverantwortlichen benannt (54 Prozent) oder schult Mitarbeiter zu Sicherheitsthemen (53 Prozent).

Jeder dritte Betroffene schaltet staatliche Stellen ein

Wer hat die Angriffe untersucht?

*Polizeibehörden	84%
Staatsanwaltschaft	57%
Datenschutz-Aufsicht	15%
Bundesamt für Sicherheit in der Informationstechnik (BSI)	15%
Verfassungsschutz	3%

Angaben in Prozent; Basis: Alle befragten Unternehmen, die in den letzten zwei Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren, n = 571, Mehrfachnennungen möglich; Quelle Bitkom