UNTERNEHMENSSTRATEGIEN ZU BEHEBUNG DER GRÖSSTEN AKTUELLEN SCHWACHSTELLEN

WHITE PAPER

Was vergangenes Jahr vielleicht noch ein Zustand nahtloser, grundsolider Cybersicherheit war, kann heute bereits eine unzulängliche Sicherheitsstrategie prall gefüllt mit Lücken sein. Dies ist eine Realität, der sich viele Unternehmen gegenübersehen. Um mit dem Ansturm von Cyberbedrohungen Schritt zu halten, müssen Unternehmen über eine proaktive Sicherheitsstrategie verfügen. Die meisten Führungskräfte und Vorstände haben jedoch Zweifel, dass ihre Unternehmen ausreichend vorbereitet sind. In einer vor Kurzem durchgeführten Studie der globalen Beratungsgruppe EY wurde festgestellt, dass 87 Prozent von ihnen kein volles Vertrauen in das Cyber-Sicherheitsprofil ihres Unternehmens haben.[5]

Die Sicherheitsprogramme ändern sich auch aufgrund eines weiteren Faktors: der Entwicklung der Compliance-Anforderungen. Unternehmen müssen ihre Sicherheitsprofile aufgrund der Einführung neuer Vorschriften kontinuierlich ändern, wie etwa der EU-Datenschutz-Grundverordnung (General Data Protection Regulation, GDPR) und des Framework des National Institute of Standards and Technology (NIST), sowie aufgrund von Änderungen bestehender Regelungen, wie der Version 3 des PCI DSS (Payment Card Industry Data Security Standard).

Ein weiterer Grund für Änderungen ist die sich entwickelnde und größer werdende Unternehmensinfrastruktur. Zahlreiche Technologien wie mobile Geräte und Cloud-Fähigkeiten existierten vor 10 Jahren noch nicht. Und das Aufkommen von Cloud-Services und des Internet der Dinge (IoT), einschließlich industrieller Steuerungssysteme (ICS) und SCADA-Systemen (Supervisory Control and Data Acquisition), machen den Schutz der Unternehmensinfrastruktur zu einer ständig wachsenden Herausforderung.

Diese Probleme stellen eine Reihe der größten Cybersicherheitsfragen, die Sicherheitsexperten heute beantworten müssen.

87 % der Führungskräfte und Vorstände haben kein volles Vertrauen in das Cyber-Sicherheitsprofil ihres Unternehmens.[1]

27 % der Unternehmen verzeichneten im vergangenen Jahr einen Ransomware-Incident.[2]

In jedem Unternehmen gibt es durchschnittlich **10,7** eindeutige Anwendungs-Exploits.[3]

Ransomware ist dabei, im Jahr 2017 einen Branchen-Jahresumsatz von **1 Mrd. US-Dollar** zu erwirtschaften.[4]

VERWENDEN DER AUTOMATISIERUNG ZUR VERBESSERUNG DES SICHERHEITSPROFILS

Um auf die sich ändernden Dynamiken zu reagieren, müssen Unternehmen fortfahren, die Triade von Technologie, Personen und Prozessen weiterzuentwickeln. Vorbei sind die Tage, in denen Unternehmen einfach die richtigen technischen Steuerkomponenten implementieren und von da an auf ihr Sicherheits- und Compliance-Profil vertrauen konnten. Unternehmen müssen ihre „Sicherheits-Triade" für die kontinuierliche Incident-Überwachung konfigurieren und damit eine schnelle und effektive Reaktionsfähigkeit sicherstellen. Es steht fest, dass kein Cybersicherheitsprogramm statisch bleiben kann. Ein Sicherheitsprofil muss dynamisch sein und sich an häufige technische Störungen, neue und sich ändernde Vorschriften und eine sich ständig ändernde Bedrohungslandschaft anpassen.

Automatisierte Sicherheitskontrollen und -prozesse sind eine Möglichkeit für Unternehmen, diese neue Cybersicherheitsumgebung bereitzustellen. Sie ermöglichen es ihnen, ihr Sicherheitsprofil zu verbessern und gleichzeitig die Effizienz und Reichweite ihrer Sicherheitsteams zu steigern. Ein Bereich, in dem die Automatisierung eine große Rolle spielt, sind die Bedrohungsdaten. Unternehmen, die ein proaktives Sicherheitsprofil implementieren, können Angriffe schneller antizipieren und sie mithilfe modernerer Techniken besser blockieren.

Die Automatisierung bezieht auch die Vorbereitung auf das Unausweichliche ein. Angesichts einer Zahl von Dreiviertel aller Unternehmen, die nach eigenen Berichten im vergangenen Jahr von irgendeiner Form von Cybereignissen betroffen waren, stehen die Chancen, dass ein Unternehmen dieses Jahr gehackt wird, sehr hoch. Das erklärt auch, warum dem Management des kontinuierlichen Geschäftsbetriebs zusammen mit der Notfallwiederherstellung und dem Schutz vor Datenverlusten von Unternehmen in einer neuen EY-Studie höchste Priorität (57 Prozent) gegeben wird.[6] Die meisten Unternehmen haben jedoch bei der Vorbereitung auf das Unvermeidliche einen weiten Weg vor sich. Bei der Optimierung ihrer Maßnahmen sollten sie nach Wegen suchen, ihre Kommunikation im Angriffsfall, Gegen- und Eindämmungsmaßnahmen gegen Eindringlinge und die Wiederherstellung von Daten, Anwendungen und Geschäftsabläufen zu automatisieren.

Automatisierung führt nicht nur zu einer größeren Sicherheit und effizienteren Abläufen, sondern kann Unternehmen auch helfen, den bestehenden Mangel an Sicherheitsexperten aufzufangen, der ein echtes Problem darstellt. Eine vor Kurzem durchgeführte Studie zeigte auf, dass derzeit eine Million Cybersicherheitsexperten fehlen und diese Zahl bis 2020 voraussichtlich sogar auf 1,5 Millionen anwachsen wird.[7] Dass diese Posten nicht gefüllt werden können, hat direkte Auswirkungen auf die Cybersicherheit von Unternehmen. 40 Prozent der Unternehmen geben an, dass sie den Expertenmangel zu spüren bekommen haben.

Nahezu die Hälfte aller Unternehmen bezweifelt, dass sie alle ihre Ressourcen kennen und **43 %** von ihnen geben an, dass sie Zweifel haben, ob alle von Ressourcen fehlerfrei sind und sie Schwachstellen schnell genug beseitigen können.[8]

Nur **22 %** der Unternehmen haben die Auswirkungen von Sicherheitsrisiken in vollem Umfang erkannt.[9]

1/3 der Cybersicherheitsexperten geben an, dass sie aufgrund ihrer hohen Arbeitsauslastung keine Zeit für Fort- und Weiterbildung haben.[10]

VERBESSERTE KONTROLLE DER ZUNEHMENDEN ANGRIFFSFLÄCHE (UND IoT)

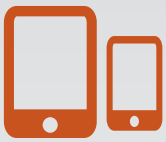
Dass sich Unternehmen auf das Unausweichliche – einen böswilligen Angriff oder einen Sicherheitsvorfall – vorbereiten müssen, liegt auch an der kontinuierlich größer werdenden Angriffsfläche, die es zu schützen gilt.[11] Egal, ob wir von Netzwerken, Software oder Menschen sprechen, die Angriffsfläche ist breiter und tiefer als jemals zuvor. Dadurch wird es für Cyberkriminelle einfacher, sich über eine wachsende Liste von Schwachstellen Zugang zu verschaffen.

IoT-Geräte sind einer der Gründe für die exponentielle Ausweitung der Angriffsfläche von Netzwerken und die damit verbundene Zunahme der Sicherheitsbedenken. In zahlreichen Unternehmenssegmente wächst die Anzahl der verbundenen IoT-Geräte jährlich um 50 Prozent – was zu 30,7 Mrd. Geräten im Jahr 2020 führen wird.[12] Und da die meisten dieser Geräte „headless“ sind, also keine Benutzeroberfläche haben, kann keine herkömmliche Sicherheitssoftware zum Blockieren von Viren auf ihnen installiert werden. Unternehmen müssen somit neue Wege finden, sie zu verwalten und zu schützen. IoT-Geräte haben außerdem schwache Autorisierungs- und Authentifizierungsprotokolle, da bei ihrer Entwicklung Sicherheitsaspekte nicht im Mittelpunkt standen. Es ist nicht verwunderlich, dass 25 Prozent der Angriffe auf Unternehmen auf das IoT gerichtet sein werden.[13]

Die verbesserte Kontrolle Ihrer größer werdenden Angriffsfläche, einschließlich des IoT, ermöglicht es Ihrem Unternehmen, seine Sicherheitsstrategie zu verbessern. **Ein Schritt** hierzu ist eine umfassende Bestandsaufnahme aller Geräte und Anwendungen, einschließlich des IoT, sodass Sie Ihre Risiken beurteilen können. Sie können somit sicherstellen, dass Ihre gesamte Angriffsfläche von Ihrer Cybersicherheitsstrategie abgedeckt ist. Dies umfasst auch die Fähigkeit, sie nach Vertrauenswürdigkeit einzustufen und zu segmentieren, um den Zugriff zu kontrollieren. Diese Strategie identifiziert zum einen IoT-Geräte, auf denen wichtige Daten gespeichert werden oder die auf wichtige Daten oder Funktionen zugreifen, und zum anderen auch kritische Funktionen, die geschützt werden müssen.

Ein **zweiter Schritt** ist die Verwendung von Bedrohungsüberwachung und -verwaltung in Echtzeit. Da IoT-Geräte aufgrund ihrer Verbreitung und mangelnden Sicherheit bevorzugte Ziele von Cyberkriminellen sind, ist die Echtzeitüberwachung des IoT ein Muss.

Ein **dritter Schritt** sind regelmäßige Penetration Tests der Firewalls und aller Hosts (einschließlich IoT). Dies erlaubt es Unternehmen, Sicherheitsprobleme auf der gesamten Bedrohungsfläche zu erkennen und zu beseitigen, noch bevor sie genutzt werden.



IoT-Geräte nehmen jährlich um **50 %** zu und werden bis zum Jahr 2020 die Zahl von 30,7 Mrd. erreichen.

25 % der Cyberangriffe werden in der Zukunft das IoT zum Ziel haben.

71 % der Cybersicherheitsexperten überwachen das IoT nicht in Echtzeit.[14]

51 % der Unternehmen mit SCADA/ICS haben im vergangenen Jahr einen Angriff verzeichnet, und 55 % dieser Incidents hatten Auswirkungen auf die Sicherheit von Mitarbeitern.[15]

BEI DER ERWEITERUNG IN DIE CLOUD FLEXIBILITÄT ERMÖGLICHEN

Cloud-Services nehmen rasant zu und ihre Nutzung folgt gleichen Schrittes. Die massiven Möglichkeiten für die Cloud liegen jedoch noch vor uns: Cloud-Services machen bislang weniger als 15 Prozent der IT-Gesamtausgaben aus. Das bedeutet auch, dass die Cybersicherheitsrisiken der Cloud ebenfalls an Umfang und Geschwindigkeit zunehmen werden. Da sich Cloud-Services außerhalb der traditionell definierten Netzwerksicherheitsgrenzen und natürlichen Sichtlinien befinden, bleiben Verwaltungsaufgaben und Verantwortlichkeiten der Cloud unklar.

Die Sicherheitsbedrohungen im Zusammenhang mit der Cloud sind sehr real. Die Cloud Security Alliance nennt 12 verschiedene Cybersicherheitsrisiken, die Cloud-Nutzer berücksichtigen müssen. Zu ihnen zählen Datendiebstähle, gestohlene Zugangsdaten und Umgehung der Authentifizierung, gehackte Schnittstellen und APIs (Application Protocol Interfaces).[16] Diese Risiken bremsen den Übergang zur Cloud: 49 Prozent der Unternehmen geben an, dass ihr Übergang zu Cloud-Services durch den Mangel an Cybersicherheitskenntnissen verlangsamt wird.[17]

Was können Unternehmen tun, um ihre Cloud-Investitionen zu schützen und ihren Unternehmen gleichzeitig die erforderliche Flexibilität zu bieten, ihre Cloud-Investition auszuweiten? Der **erste Schritt** ist die Erweiterung der traditionellen Netzwerkgrenzen, um den Cloud-Services – privaten, öffentlichen und hybriden – zu folgen. Dies umfasst nicht nur die Unternehmens-Firewalls, sondern auch Sicherheitsrichtlinien und -praktiken. Die Verwaltung der Netzwerksicherheit muss außerdem horizontal angelegt sein und Daten segmentieren, da sich verschiedene Benutzer, Transaktionen und Anwendungen im Netzwerk bewegen. Cloud-Services müssen – ebenso wie das IoT – über dieselbe zentrale Konsole sichtbar sein, die auch zur Überwachung und Verwaltung der Anlagen vor Ort genutzt wird.

Beim **zweiten Schritt** geht es darum, dass mehrere Unternehmen möglicherweise dieselbe öffentliche Cloud-Infrastruktur benutzen. Um potenzielle Cyberrisiken zu vermeiden, müssen Unternehmen einen Mikrosegmentierungsansatz implementieren, der den Datenverkehr auf der Kommunikationsebene zwischen zwei oder mehr Hosts, die sich in derselben Domäne befinden, prüft. Unternehmen sollten auch prüfen, ob die Cloud-Lösungsanbieter Cybersicherheitszertifizierungen besitzen, wie ISO 27001, SSAE 16, COBIT und die Cloud Controls Matrix[18] der Cloud Security Alliance, sowie solche, die Überwachungs- und mehrschichtige Sicherheitsmaßnahmen rund um die Uhr bereitstellen.

Ein **letzter Schritt**, den viele Unternehmen berücksichtigen müssen, ist der Einsatz von Schatten-IT. Das durchschnittliche Unternehmen nutzt 36 unterschiedliche Cloud-Anwendungen.[19] Unternehmen müssen dieses riesige, außer Kontrolle geratene Universum, das als „Schatten-IT“ bezeichnet wird, in den Griff bekommen, wenn sie erhebliche Cybersicherheitsrisiken vermeiden wollen.

Cloud-Services machen immer noch weniger als **15 %** der IT-Ausgaben aus.

93 % der Unternehmen nutzen Cloud-Services irgendeiner Form.[20]

79 % der Rechenlasten laufen derzeit in der Cloud ab.[21]

KONSOLIDIEREN DER SICHERHEITSLANDSCHAFT

Angesichts der sich entwickelnden Sicherheitslandschaft, der Einführung bahnbrechender Technologien und sowohl neuer als auch bestehender Vorschriften haben sich Cybersicherheitsunternehmen einer wachsenden Anzahl von Einzelprodukten zugewandt. Einige Unternehmen haben mittlerweile bis zu 50 Einzelprodukte für ihre Sicherheitsanforderungen.[22] Die Absicht dahinter ist, es den kriminellen Elementen so schwer wie möglich zu machen. Es tritt jedoch häufig der entgegengesetzte Effekt ein, da die zunehmende Komplexität Sicherheitsexperten daran hindert, Angriffe zu erkennen und zu verhindern, ganz zu schweigen von den zusätzlichen Kosten und Mitarbeiterressourcen zur Verwaltung der Lösungen.

Ein Problem der Einzelprodukte besteht darin, dass sie einen Überblick der Sicherheitsteams über das gesamte Übernehmen verhindern. Jedes Einzelprodukt arbeitet in seinem eigenen isolierten Bereich und interagiert nicht mit anderen Einzelprodukten in derselben Umgebung. Da die universale Richtlinienverwaltung unmöglich wird, ist eine einheitliche Durchsetzung von Richtlinien auf allen Einzelprodukten nicht möglich und es kommt zu Lücken. Ein zweites Problem besteht darin, dass Einzelprodukte keine Daten oder Befehle austauschen und Mitarbeiter (gewöhnlich mehrere) erforderlich sind, diese Lücke zu schließen. Die Entscheidung für die jeweils für die einzelnen Produkte vorzunehmenden Aktionen und das Koordinieren dieser Aktionen zwischen mehreren Bedienern verlangsamt die Reaktion und stellt eine Fehlerquelle dar.

Stattdessen sollten Unternehmen nach einer integrierten Security Fabric suchen, die es ihnen erlaubt, unterschiedliche Sicherheitsfunktionen zu nutzen, ohne Anforderungen, wie eine universale Richtlinienverwaltung, transparente Sichtbarkeit aller Sicherheitskomponenten und automatisierte intelligente Kommunikation und Aktionen, aufzugeben.

Wie sieht das aus? Im **ersten Schritt** stellen Sie sicher, dass Sie eine Unternehmens-Firewall für das gesamte Netzwerk haben. Die Implementierung mehrerer Netzwerksicherheitslösungen schafft Komplexität und führt zu Sicherheitslücken, die ausgenutzt werden können. Unternehmen müssen eine einzige Sicherheits-Firewall zum Schutz des gesamten Netzwerks nutzen. Diese Netzwerksicherheitslösung muss über die Grenzen der traditionellen IT-Infrastruktur hinausgehen, um die sich ausweitende Angriffsfläche zu schützen – einschließlich IoT und Cloud.

Im **zweiten Schritt** muss ein integriertes Modell für alle Ihre Anwendungen und Endgeräte implementiert werden. Diese in isolierten Bereichen zu verwalten, führt zu Sicherheitslücken und Schwachstellen, die ausgenutzt werden können.

Im **dritten Schritt** muss eine Sicherheitsinfrastruktur geschaffen werden, die als integriertes Ganzes arbeitet, gewöhnlich mittels mehrerer offener Application Programming Interfaces (APIs). Dies beginnt mit den Richtlinien zur Verwaltung von Daten und Kommunikation im Netzwerk, für Endgeräte, Anwendungen, Rechenzentren, Cloud und Zugriff.

Im **vierten Schritt** der Security Fabric muss eine 360-Grad-Ansicht der Bedrohungsdaten bereitgestellt werden. Durch das Anwenden derselben universalen Richtlinien in der gesamten IT-Infrastruktur und das Teilen von Informationen zwischen den verschiedenen Sicherheitskomponenten wird eine durchgängige Ansicht der Bedrohungsdaten geschaffen. Dies ist in einer Zeit, in der Zero-Day-Angriffe zum Alltag gehören, besonders wichtig.

Im **letzten Schritt** zur Erstellung des Security Fabric wird eine integrierte Kommunikation in Echtzeit zwischen den einzelnen Sicherheitskomponenten eingerichtet, die eine schnelle Reaktion auf Bedrohungen erlaubt. Sie ermöglicht auch das automatische Identifizieren und Isolieren von betroffenen Geräten, das Partitionieren von Netzwerksegmenten, das Aktualisieren von Regeln, das Inkraftsetzen neuer Richtlinien und das Entfernen von Malware.

Unternehmen haben bis zu **50** Sicherheits-Einzelprodukte.

Einzelprodukte führen zu gesteigerter Komplexität, was Sicherheitsexperten häufig daran hindert, Angriffe zu **erkennen** und zu **unterbinden**.

VERWALTEN DER RISIKOEXPOSITION

Wir leben in einer Welt unaufhörlichen Wandels. Die Möglichkeiten einer technischen Störung drängen die Cyberbedrohung häufig in den Hintergrund. Aber in den meisten Fällen besitzen Unternehmen gar nicht die Fähigkeit, die Risiken – weder aktuelle noch zu erwartende – zu bewerten oder sich ein Bild davon zu machen, wie ihre Risikotoleranz aussieht, selbst wenn sie das möchten.[23] Dadurch ist es äußerst schwierig, das Risiko der vorhandenen, implementierten Technologien zu beurteilen, geschweige denn Risiken neuer Lösungen zu antizipieren.

Eine treibende Kraft für Unternehmen, Cyberbedrohungen und Rendite (ROI) zu quantifizieren, geht auf ähnliche frühere Bemühungen von Finanzdienstleistern zurück, Finanzrisiken zu berechnen.[24] Angesichts einer jährlichen Zunahme der Ausgaben für Cybersicherheit um 15 Prozent[25] verlangen Unternehmen von ihren Sicherheitsteams Belege für die Rentabilität dieser Investitionen.

Unternehmen gelangen in zunehmendem Maße zu der Erkenntnis, dass das Team für Cybersicherheit nicht der IT-Abteilung unterstellt, sondern vielmehr eng in die Geschäftsprozesse integriert sein sollte. Das ermöglicht es Cybersicherheitsexperten, ein wesentlich breiteres und tiefergehendes Bild der Abläufe zu erhalten, Schwachstellen zu priorisieren und die Auswirkungen von Incidents aus Sicht des Geschäftsbetriebs zu bewerten. Cybersicherheitsexperten müssen hierzu u. a. folgende Fragen stellen:

1. **Was ist wichtig?** Bestimmte Datenressourcen sind wichtiger als andere. Sie basieren auf Unternehmenszielen, Leistungskennzahlen (KPIs) und anderen geschäftsbezogenen Fragen.
2. **Was wird bedroht?** Mit dieser Frage ermittelt ein Unternehmen, wo das höchste Risiko liegt – beispielsweise bei Daten, Cloud-Services, Geräten oder Benutzern.
3. **Was sind die potenziellen Auswirkungen?** Die finanziellen, betrieblichen und Markenauswirkungen der verschiedenen Bedrohungen sind unterschiedlich. Unternehmen müssen die Kosten für die Verwaltung eines Risikos (Technologie, Mitarbeiter, externe Ressourcen usw.) den potenziellen finanziellen, betrieblichen und/oder Markenauswirkungen für das Unternehmen gegenüberstellen.
4. **Wie können diese Lücken am besten geschlossen werden?** Nachdem die Bedrohungen identifiziert und eingestuft wurden, können Unternehmen entsprechende Lösungen einrichten, um sie abzuwehren. Die Lösungen bestehen aus Technologie, Personen und Prozessen, die alle mit gewissen Kosten verbunden sind.
5. **Wie hoch ist die Wahrscheinlichkeit?** Außer den potenziellen geschäftlichen Auswirkungen müssen Unternehmen die Wahrscheinlichkeit bewerten, mit der eine Bedrohung auftreten wird, wenn Abwehrmechanismen eingerichtet wurden, und mit welcher Wahrscheinlichkeit dies ohne solche Mechanismen der Fall ist. Wenn zum Beispiel die Wahrscheinlichkeit einer Instance durch Abwehrmechanismen von 50 Prozent auf 40 Prozent gesenkt wird, ist die Rendite deutlich niedriger als in einem Szenario, in dem die Wahrscheinlichkeit von 80 Prozent auf 10 Prozent gesenkt wird.

Die oben genannten Daten sind im Folgenden in Tabelle 1 zusammengefasst, wo die Cybersicherheitsmaßnahmen für die einzelnen Elemente basierend auf der jeweiligen Rentabilität priorisiert werden. Dank der neuen Technologien für künstliche Intelligenz (KI) und maschinelles Lernen (ML), die externe Daten und historische Trenddaten nutzen, besitzen Cybersicherheitsexperten heute die Fähigkeiten, prädiktive, datenbasierte Sicherheitsmodelle zu erstellen.[26] Diese können genutzt werden, um Risikotoleranzkurven zu entwickeln und zu identifizieren, welche Investitionen die höchste Rendite erzielen.

	Bedrohungs-wahrschein-lichkeit	Geschäftliche Auswirkungen der Bedrohung*	Abwehrkosten	Wirksamkeit der Abwehr (Wahrschein-lichkeit)	Abwehrrendite	Empfehlung
Bedrohung 1	75 %	2 Mio. bis 4 Mio. USD	750 000 USD	95 %	1,75 Mio. bis 3,25 Mio. USD	Fortfahren
Bedrohung 2	15 %	10 Mio. USD	3 Mio. USD	70 %	7 Mio. USD	Verfolgen
Bedrohung 3	50 %	500 000 USD	275 000 USD	98 %	225 000 USD	Verfolgen
Bedrohung 4	90 %	3 Mio. USD	1 Mio. USD	98 %	2 Mio. USD	Fortfahren

TABELLE 1. VERWALTEN DER RISIKOEXPOSITION
*Geschäftliche Auswirkungen = Finanzkosten, Betriebsunterbrechungen, Beschädigung der Marke

AUFBAU UND SCHUTZ IHRES CYBERSICHERHEITSPROFILS

Cybersicherheit ist kein einfaches Unterfangen. Die sich ständig verändernde Bedrohungslandschaft und die Hauptanliegen der Sicherheitsexperten sorgen dafür, dass es immer schwieriger wird, sie zu gewährleisten. Unternehmen, die in der Lage sind, diese Sicherheitsanforderungen zu lösen, schützen damit nicht nur ihr Geschäft, ihre Partner und ihre Kunden, sondern schaffen auch ein Framework, über das sie die Wirksamkeit ihrer Cybersicherheitsmaßnahmen beurteilen können. Es gibt keine Universalmethode, die für alle Fälle eingesetzt werden kann, da die Risikotoleranz von Unternehmen abhängig von Geschäftstyp und der jeweiligen potenziellen Bedrohungsexposition variiert.

[1] „Path to Cyber Resilience: Sense, Resist, React“, EY's 19th Global Information Security Survey 2016–17, 2016.

[2] Jon Oltsik, „Through the Eyes of Cyber Security Professionals: An Annual Research Report“, a Cooperative Research Project by ESG and ISSA, Dezember 2016.

[3] „Threat Landscape Report: Q4 2016“, Fortinet, Januar 2017.

[4] Kyle Torpey, „2016 Big Year for Ransomware – 70% Pays in This $1 Billion Industry“, Bitcoin, 29. Dezember 2016.

[5] „Path to Cyber Resilience: Sense, Resist, React“, EY's 19th Global Information Security Survey 2016–17, 2016.

[6] „Path to Cyber Resilience.“

[7] Michael Suby, et al., „The 2015 (ISC)2 Global Information Security Workforce Study“, Frost & Sullivan, 2015.

[8] „Path to Cyber Resilience.“

[9] „Cyber Threat Intelligence – How to Get Ahead of Cybercrime.“

[10] Jon Oltsik, „Through the Eyes of Cyber Security Professionals: An Annual Research Report“, a Cooperative Research Project by ESG and ISSA, Dezember 2016.

[11] Lily Hay Newman, „Hacker Lexicon: What Is An Attack Surface?“ Wired, 12. März 2017.

[12] Louis Columbus, „Roundup of Internet of Things Forecasts and Market Estimates, 2016“, Forbes.com, 27. November 2016.

[13] Ebd.

[14] „IoT Security: The Majority of IoT Devices Is Not Monitored in Real Time“, i-SCOOP, letzter Zugriff 10. April 2017.

[15] „2016 Industrial Control System Security Trends: Challenges and Strategies for Securing Critical Infrastructure“, Fortinet and Forrester, 14. September 2016.

[16] Fahmida Y. Rashid, „The Dirty Dozen: 12 Cloud Security Threats“, InfoWorld, 11. März 2016.

[17] „Building Trust in a Cloudy Sky.“

[18] „Cloud Security Standards: What to Expect & What to Negotiate: Version 2.0“, Cloud Standards Customer Council, August 2016.

[19] „Threat Landscape Report: Q4 2016.“

[20] „Building Trust in a Cloudy Sky: The State of Cloud Adoption and Security“, McAfee, Januar 2017.

[21] Ebd.

[22] Patrick Moorhead, „With a Few Surprises, Cisco Releases 2017 Annual Cybersecurity Report“, Forbes, 14. Februar 2017.

[23] Natalia Nelson, „How Companies Achieve Balance Between Technology Enabled Innovation and Cyber-Security“, MBA Thesis, Massachusetts Institute of Technology, Juni 2016.

[24] J.R. Reagan, et al., „Quantifying Risk: What Can Cyber Risk Management Learn from the Financial Services Industry?“ Deloitte University Press, 25. Juli 2016.

[25] „Cybersecurity Market Report“, Cybersecurity Ventures, Q1 2017.

[26] Douglas W. Hubbard and Richard Seiersen, How to Measure Anything in Cybersecurity Risk (New York: John Wiley & Sons, 2016).

DEUTSCHLAND
Feldbergstraße 35
60323 Frankfurt
Deutschland
Verkaufsabteilung:
+49 69 310 192 0

SCHWEIZ
Riedmuehlestr. 8
CH-8305 Dietlikon/Zürich
Schweiz
Verkaufsabteilung:
+41 44 833 68 48

ÖSTERREICH
Wienerbergstrasse 11
Tower A/9. OG
1100 Wien
Österreich
Verkaufsabteilung:
Tel: +43 1 3760013 - 0

HAUPTSITZ
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
USA
Tel.: +1 408 235 7700
www.fortinet.com/sales

VERTRIEBSBÜRO EMEA
905 rue Albert Einstein
06560 Valbonne
Frankreich
Tel.: +33 4 8987 0500

VERTRIEBSBÜRO APAC
300 Beach Road 20-01
The Concourse
Singapur 199555
Tel.: +65 6513 3730

LATEINAMERIKA ZENTRALE
Sawgrass Lakes Center
13450 W. Sunrise Blvd.,
Suite 430
Sunrise, FL 33323
Tel: +1 954 368 9990

76764-A-0-EN
Montag, 15. Mai 2017