www.pwc.at/gsiss

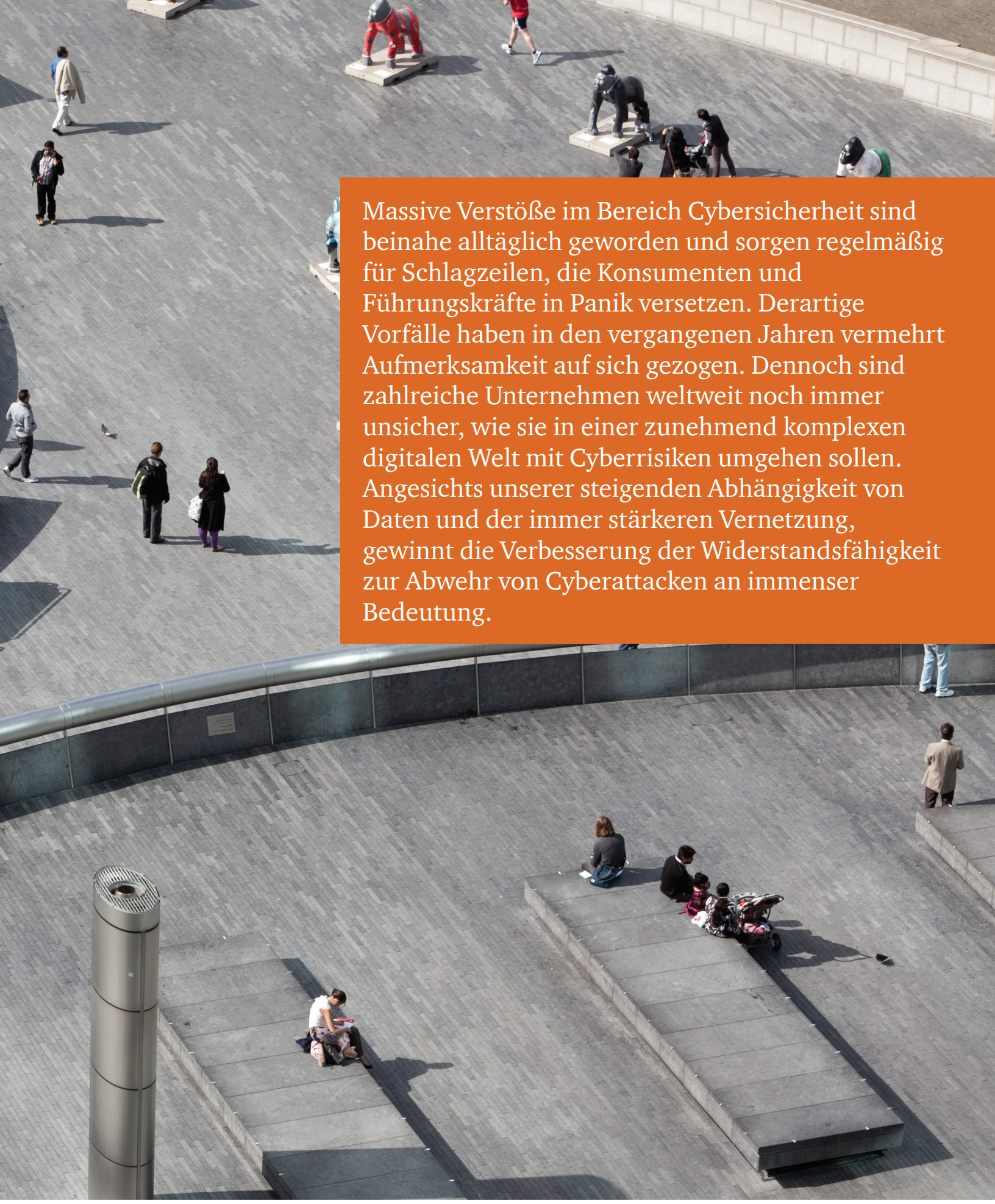
Cybersecurity und Privacy

Stärkung der digitalen Gesellschaft gegen Cyberattacken

Wesentliche Ergebnisse der Global State of Information Security® Survey 2018 für Österreich

pwc

Inhaltsverzeichnis

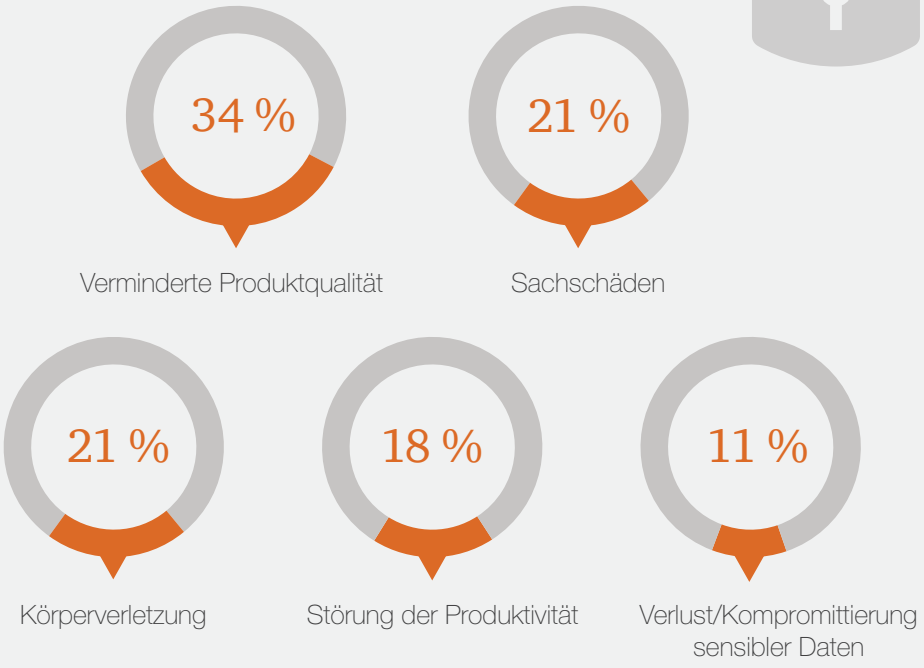


Massive Verstöße im Bereich Cybersicherheit sind beinahe alltäglich geworden und sorgen regelmäßig für Schlagzeilen, die Konsumenten und Führungskräfte in Panik versetzen. Derartige Vorfälle haben in den vergangenen Jahren vermehrt Aufmerksamkeit auf sich gezogen. Dennoch sind zahlreiche Unternehmen weltweit noch immer unsicher, wie sie in einer zunehmend komplexen digitalen Welt mit Cyberrisiken umgehen sollen. Angesichts unserer steigenden Abhängigkeit von Daten und der immer stärkeren Vernetzung, gewinnt die Verbesserung der Widerstandsfähigkeit zur Abwehr von Cyberattacken an immenser Bedeutung.

Einleitung

Bisher wurde im Zusammenhang mit Cyberattacken über keine Todesfälle berichtet bzw. verursachten diese nur relativ geringe Schäden.[1] Dennoch wird die destruktive Kraft solcher Angriffe immer deutlicher, vor allem im Hinblick auf geopolitische Bedrohungen. So beeinträchtigte zum Beispiel ein Cyberangriff im Dezember 2015 in der Türkei Netzwerke von türkischen Banken, Medien und der Regierung.[2] Noch im gleichen Monat kam es zur ersten bekannten Cyberattacke, die ein Stromnetz lahmlegen sollte und gezielt das ukrainische Stromversorgungsnetz im Visier hatte. 230.000 Einwohner waren damals von der Stromversorgung abgeschnitten.[3] Dieser Angriff hatte zudem das Telefonsystem des Landes zum Ziel, um Kunden an der Meldung dieser Ausfälle zu hindern und sabotierte damit Bemühungen zur Wiederherstellung der Stromversorgung.[4] Im Juni 2017 beeinträchtigte die Ransomware Petya, die eigentlich ukrainische Computer zum Ziel hatte, Geschäftsbetriebe auf der ganzen Welt. Massive Risiken im Bereich des Datenschutzes geben Anlass zur Sorge, dass Cyberattacken die Weltwirtschaft erschüttern werden.[5]

Erwartete Ergebnisse einer erfolgreichen Cyberattacke gegen Automatisierungs- bzw. Robotersysteme



Quelle: PwC, CIO und CSO, The Global State of Information Security® Survey 2018, 18. Oktober 2017.
Basis: 9.500 Befragte

1 The Cipher Brief, Cyber Deterrence Is Working – So Far, July 23, 2017
2 Harvard University Belfer Center for Science and International Affairs, Too Connected To Fail, May 2017
3 Wired, Inside the cunning, unprecedented hack on Ukraine's power grid, March 3, 2016
4 US Homeland Security Advisory Council, Final Report of the Cybersecurity Subcommittee: Part I - Incident Response, June 2016
5 The Wall Street Journal, The Morning Download, Sept. 11, 2017

Führungskräfte auf der ganzen Welt erkennen die immer größer werdenden Gefahren von Cyber-Insecurity. Im Rahmen unserer Studie „Global State of Information Security Survey® 2018“ (GSISS), geben Führungskräfte von Organisationen, die Automatisierung oder Roboter einsetzen, an, dass sie sich der potenziellen Bedeutung der Folgen von Cyberattacken bewusst sind.

34 % der Studienteilnehmer nennen die Beeinträchtigung der Produktqualität als größtmögliche Auswirkung einer Cyberattacke, 21 % etwaige Sachschäden, 21 % Schäden an menschlichem Leben, 18 % Betriebsstörungen und 11 % den Verlust bzw. die Kompromittierung sensibler Daten.

„Viele Organisationen müssen ihr digitales Risiko evaluieren und die Widerstandsfähigkeit im Hinblick auf das Unvermeidliche stärken.“

Dr. Christian Kurz, Leiter Forensic Technology Solutions und Cyberforensics, PwC Österreich

Trotz des Wissens um die Folgen von Cyberangriffen, bereiten sich viele bedrohte Unternehmen nicht entsprechend vor.

84 % der 42 Führungskräfte in Österreich, die an der GSISS 2018 teilgenommen haben, geben an, keine umfassende Informationssicherheitsstrategie zu verfolgen. 73 % verfügen über kein Programm zur Bewussteinsbildung ihrer Mitarbeiter zum Thema Cybersecurity und 86 % verfügen über keinen speziellen Prozess zur Reaktion auf etwaige Vorfälle.

„Viele Organisationen müssen ihr digitales Risiko evaluieren und die Widerstandsfähigkeit im Hinblick auf das Unvermeidliche stärken“, so Dr. Christian Kurz, Leiter Forensic Technology Solutions und Cyberforensics, PwC Österreich.

Geschäftsführer sind aktuell mit widersprüchlichen Expertenmeinungen konfrontiert. Die eine Seite prophezeit ein künftiges Cyber-Armageddon, während die andere Seite die meisten Cyberbedrohungen als unwichtig erachtet. Viel produktiver wäre ein sachlicher globaler Diskurs, der Geschäftsführern praktische Ratschläge gibt, um Unternehmen widerstandsfähig gegenüber Cyberattacken zu machen.

Auswirkungen von Cyberabhängigkeiten auf globale Risiken

Das Weltwirtschaftsforum (WWF) zählt die zunehmende Cyberabhängigkeit von IT-Netzen zu einem der größten Risikofaktoren weltweit. Der Global Risks Bericht 2017 des WWF hält fest, dass Cyberattacken, Softwarefehler und andere Faktoren zu Systemausfällen führen könnten, welche sich über Netzwerke hinweg verbreiten und die Gesellschaft in ungeahnter Weise beeinträchtigen könnten.[6]

Der jüngste Bericht des US National Intelligence Council zu globalen Trends warnte ebenfalls vor der „immanenten" Bedrohung aus dem Netz – möglicherweise im großen Stil mit „tödlichen Konsequenzen" – aufgrund der Anfälligkeit kritischer Infrastrukturen.[7] Fallstudien zu Katastrophen (non-cyber) haben ergeben, dass diese Vorfälle oft mit Stromausfällen beginnen und viele Systeme davon sofort, oder innerhalb eines Tages, betroffen sind. Das bedeutet, dass zumeist wenig Zeit bleibt, das ursprüngliche Problem zu beheben, bevor es sich ausbreitet.[8] Wechselwirkungen zwischen kritischen und nicht-kritischen Netzwerken bleiben oft so lange unbemerkt, bis ein Schaden eintritt.[9]

Viele Menschen weltweit – vor allem in Japan, den USA, Deutschland, Großbritannien und Südkorea – haben Angst vor Cyberattacken aus anderen Ländern.[10] Werkzeuge zur Durchführung von Cybeangriffen verbreiten sich zunehmend auf der ganzen Welt. Kleinere Länder wollen ähnlich große Kapazitäten wie jene in größeren Ländern entwickeln. Die Veröffentlichung von National Security Agency (NSA) Hacking Tools macht diese hochentwickelten Werkzeuge für gefährliche Organisationen und böswillige Hacker verfügbar.[11]

6 World Economic Forum, 2017 Global Risks Report, January 2017
7 US National Intelligence Council, Global Trends: Paradox of Progress, January 2017
8 CascEff, Cascading effects: What are they and how do they affect society? July 31, 2017
9 Internet outages after the Sept. 11, 2001, terrorist attacks were caused by a chain of events: lack of electric power required a major data center to use backup generators that relied on fuel; poor air quality in the city due to the attack hindered data-center cooling, hastening fuel consumption; normal fuel delivery was blocked by emergency traffic limits; and without fuel, the generators could not function. See Harvard University Belfer Center for Science and International Affairs, Too Connected To Fail, May 2017
10 The Pew Research Center, Spring 2017 Global Attitudes Survey, August 2017
11 PwC, Bold Steps to Manage Geopolitical Cyber Threats, 2017

Ein Großteil der betroffenen Unternehmen kann die Täter bei Cyberattacken nicht eindeutig identifizieren. In unserer GSISS 2018 geben nur 14 % der Studienteilnehmer an, sie hätten großes Vertrauen in ihre Fähigkeit, die Täter eindeutig zu bestimmen.

Die zunehmende Produktion unsicherer Internet of Things (IoT) Geräte generiert weit verbreitete Sicherheitsschwachstellen im Cyberbereich.[12] Eine weitere Gefährdung der Datenintegrität könnte das Vertrauen in zuverlässige Systeme untergraben und physische Schäden durch die Beeinträchtigung kritischer Infrastrukturen verursachen.[13]

Nur 14 % geben an, sie hätten großes Vertrauen in ihre Fähigkeit, die Täter von Cyberattacken zu identifizieren.

Quelle: PwC, CIO und CSO, The Global State of Information Security® Survey 2018, 18. Oktober 2017

12 PwC, Uncovering the Potential of the Internet of Things, 2017

13 Then-US Director of National Intelligence James Clapper told Congress in 2016, "Future cyber operations will almost certainly include an increased emphasis on changing or manipulating data to compromise its integrity (i.e., accuracy and reliability) to affect decision-making, reduce trust in systems, or cause adverse physical effects. Broader adoption of IoT devices and AI—in settings such as public utilities and health care—will only exacerbate these potential effects."

Vorbereitung auf Cyberangriffe als Geschäftsanforderung

Für den US National Intelligence Council haben jene Staaten gute Zukunftsaussichten, die in Infrastruktur, Wissen und Beziehungen investieren, die widerstandsfähig gegen Angriffe sind – egal ob wirtschaftliche, ökologische, gesellschaftliche oder Cyberangriffe. Das Gleiche gilt für die erfolgreichen Unternehmen von morgen. Widerstandsfähige Unternehmen werden am besten aufgestellt sein, um den Geschäftsbetrieb aufrecht zu erhalten, Vertrauen bei Kunden aufzubauen und hohe wirtschaftliche Leistungen zu erzielen.

Wie können Unternehmen demnach die Widerstandsfähigkeit gegen Cyberattacken erhöhen? Die Ergebnisse der GSISS 2018 bieten entsprechende Antworten.

Führungskräfte müssen im Hinblick auf die Förderung der Cyberabwehr mehr Verantwortung übernehmen.

In der Privatwirtschaft müssen jene, die den Unternehmenserfolg vorantreiben, auch für die Geschäftsrisiken zur Verantwortung gezogen werden. Die Bereitstellung eines effizienten Kontrollsystems und eines proaktiven Risikomanagements unterliegt der Unternehmensleitung. Strategien für Business-Continuity, Nachfolgeplanung, strategische Ausrichtung und Datenanalyse sind dabei von zentraler Bedeutung. Dennoch geht aus der GSISS 2018 hervor, dass die Unternehmensleitung die Sicherheitsstrategien bzw. Investitionspläne eines Unternehmens zumeist nicht proaktiv in die Hand nimmt.

Nur 24 % der Studienteilnehmer geben an, dass die Unternehmensleitung proaktiv an der Gestaltung einer Gesamtsicherheitsstrategie des Unternehmens mitarbeitet.

Laut Matt Olsen, Mitbegründer und Vorsitzender für Geschäftsentwicklung und Strategie von IronNet Cybersecurity sowie ehemaliger Leiter des US National Counterterrorism Center, wird das Thema Cybersicherheit auf Ebene der Unternehmensleitung nach wie vor als ein IT-Problem wahrgenommen.

Gemäß den von der National Association of Corporate Directors' 2016 – 2017 erschienenen Studien über Unternehmensleiter von börsennotierten und privaten Unternehmen, sehen nur wenige Vorstandsmitglieder ihr Unternehmen gegen Cyberattacken gut aufgestellt[14]. Diese Zweifel verwundern nicht, berücksichtigt man die mangelnde Einbindung der Befragten bei Sicherheitsmaßnahmen. 42 % der österreichischen Studienteilnehmer sind sich einig, dass die Ausgaben für Sicherheit lediglich durch Bedrohungen vorangetrieben werden. Zugleich gibt es eine genau so große Gruppe, die dieser Aussage widerspricht. Die restlichen Befragten sind unentschlossen.

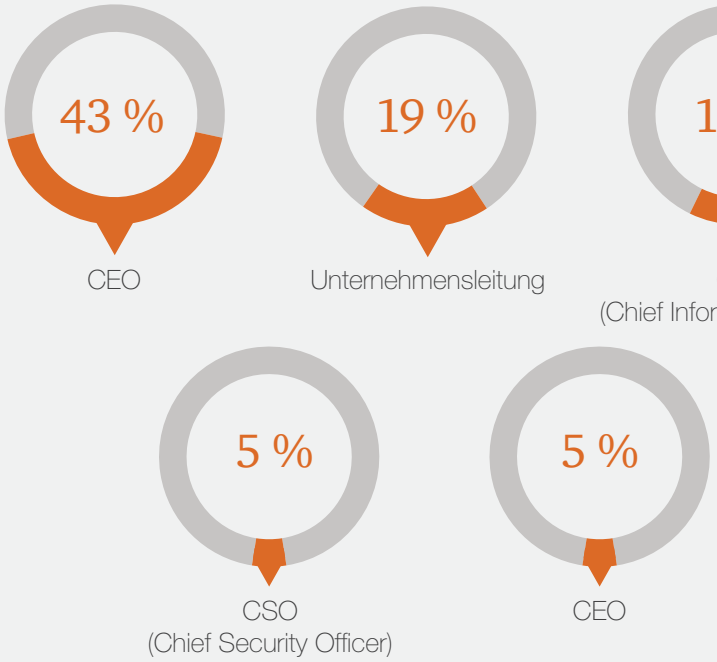
Der Großteil der Studienteilnehmer (68 %) gibt an, dass die Ausgaben ihrer Unternehmen hinsichtlich Sicherheitsmaßnahmen von den Erlösen des jeweiligen Geschäftszweiges abhängen. Die restlichen Teilnehmer (32 %) geben an, dass dies nicht so ist bzw. sind sich dabei unsicher.

Die Funktion des Chief Information Security Officers (CISO) gewinnt zunehmend an Bedeutung. Der GSISS 2018 zufolge, berichten in Österreich rund 43 % der CISOs (oder CSOs) an den Chief Privacy Officer, 24 % an die Unternehmensleitung und 14 % jeweils an den CIO (Chief Information Officer), den CTO (Chief Technology Officer) bzw. an den COO (Chief Operating Officer).

Laut Keith Alexander, Gründer und CEO von IronNet Cybersecurity sowie ehemaliger Leiter und Viersternegeneral des US Cyber Command und der National Security Agency, hat der CISO der Unternehmensleitung den aktuellen Status quo der Cybersecurity-Strategie aufzuzeigen. Die zur Verfügung gestellte Information solle auch jegliche bereits stattgefundenen Cyberangriffe, Defizite bezüglich Trainings, Ausstattung und Cyber-Tools umfassen. Der CISO hat Sicherheitslücken aufzudecken und hervorzuheben, damit die Unternehmensleitung ihre Verpflichtungen im Hinblick auf das Verständnis für und die Auseinandersetzung mit potentiellen Risiken für das Unternehmen wahrnehmen kann.

14 United Nations International Telecommunication Union, Global Cybersecurity Index report, 2017

An wen berichtet der CISO und CSO direkt?



Quelle: PwC, CIO und CSO, The Global State of Information Security® Survey 2018, 18. Oktober 2017.
Basis: 9.500 Studienteilnehmer

Organisationen müssen tiefer graben, um Risiken aufzudecken. Soll die Gesellschaft robust gegen Cyberattacken werden, braucht es gebündelte Bemühungen, um jene Risiken aufdecken zu können, die mit neuen Technologien entstehen. Mit dem digitalen Fortschritt brauchen Organisationen entsprechende Führung und Prozesse zur Umsetzung notwendiger Sicherheitsmaßnahmen. Viele Unternehmen stehen dabei erst am Anfang.

Beispielsweise geben nur wenige Studienteilnehmer an, dass ihre Organisation plant, IoT-Risiken quer über das Geschäftsfeld zu erfassen. Wer im Unternehmen für die IoT-Sicherheit verantwortlich ist, hängt von der Organisation ab – 15 % sehen dies im Verantwortungsbereich des CISO, während hingegen 31 % dies im Aufgabenbereich des Engineering Teams, 21 % beim Production Development und 13 % beim Chief Risk Officer sehen. Führungskräfte im Bereich Cybersecurity sind in vielen Organisationen noch immer rar. Etwa ein Drittel (30 %) der Studienteilnehmer gibt an, dass ihre Organisation einen CISO beschäftigt; 5 % geben an, dass sie einen Chief Security Officer einsetzen und 11 % bestätigen, dass sie Sicherheitsspezialisten zur Unterstützung der internen Geschäftstätigkeiten beschäftigen.

Viele Organisationen könnten proaktiver mit Cyberrisiken umgehen. Nur 19 % der Befragten geben an, dass ihre Organisation Background Checks durchführt. Nur ein Viertel der Studienteilnehmer (25 %) hat Schlüsselprozesse zur Aufdeckung von Cyberrisiken in Geschäftssystemen eingeführt – darin inbegriffen Penetration Tests, Threat Assessments, Monitoring von Sicherheitsinformationen sowie Sicherheits- und Schwachstellenanalysen.

Es bedarf mehr Informationsaustausch und Koordination zwischen den Stakeholdern. Nur 49 % der Studienteilnehmer geben an, dass sie formell mit anderen in ihrer Branche, einschließlich Mitbewerbern, zusammenarbeiten, um die Sicherheit zu erhöhen und potentielle zukünftige Bedrohungen zu verringern. Glaubwürdige, zeitgerechte und verwertbare Informationen zu Cyberbedrohungen sind entscheidend für eine rasche Reaktionsfähigkeit bzw. um die Widerstandsfähigkeit zu stärken. Um auf Cyberattacken zu reagieren, bedarf es über alle Organisationen, Branchen, Länder und Regionen hinweg gemeinsamer Anstrengungen, deren Effektivität von der Bereitschaft zur Zusammenarbeit abhängt.

Die geteilten Informationen müssen auch nützlich sein. Von jenen GSISS-Studienteilnehmern, die mit anderen zusammenarbeiten, geben lediglich 32 % an, ihre Bemühungen hätten dazu beigetragen, dass auch vonseiten ihrer Branchenkollegen mehr verwertbare Informationen geteilt bzw. ausgetauscht wurden.

22 %

geben an, dass ihre Organisationen planen, IoT-Risiken quer über das Geschäftsfeld zu erfassen.

Quelle: PwC, CIO und CSO, The Global State of Information Security® Survey 2018, 18. Oktober 2017

Die nächsten Schritte für Führungskräfte

C-Suites müssen Verantwortung übernehmen – die Unternehmensleitung muss involviert sein. Führungskräfte müssen Verantwortung für die Widerstandsfähigkeit gegen Cyberattacken übernehmen. Das Festlegen einer Top-down-Strategie zur Bewältigung von Cyber- und Privacy-Risiken über das gesamte Unternehmen hinweg ist entscheidend. Die Risikomanagement-Strategie eines Unternehmens sollte über ein solides Verständnis potentieller Cyberbedrohungen der Organisation verfügen. Zudem erfordert sie ein Bewusstsein dafür, welche Vermögenswerte den größten Schutz benötigen. Dafür braucht es eine konsequente grundlegende Struktur für den Umgang mit Risiken. Die Unternehmensleitung hat die Entwicklung einer Cyber-Risikokultur auf allen Organisationsebenen zu etablieren und voranzutreiben.

Widerstandsfähigkeit als Weg zum Erfolg – nicht nur zur Risikovermeidung. Die Erhöhung der Widerstandsfähigkeit gegenüber Risiken ist ein Weg hin zu einer stärkeren, langfristigen wirtschaftlichen Leistung. So waren beispielsweise Unternehmen, die noch vor dem Tsunami in Japan 2011 Prozesse zur Business-Continuity in ihren Risikomanagement-Programmen verankerten, in der Lage, ihren Betrieb schneller als ihre Mitstreiter wieder aufzunehmen. Damit konnten sie sich einen Marktanteil nach der Katastrophe sichern.[15]

Durch gezielte Zusammenarbeit und gewonnene Erkenntnisse profitieren. Führungskräfte in Industrie und Wirtschaft müssen über Organisationen, Sektoren und nationale Grenzen hinweg zusammenarbeiten, um Risiken identifizieren, erfassen und testen zu können. Nur so lassen sich die Widerstandsfähigkeit und das Risikomanagement branchenweit nachhaltig stärken. Auch an heiklen Themen, wie Verantwortung, Haftung, Zugehörigkeiten, Bewältigung von Folgen und Normen kann gemeinsam gearbeitet werden.

Stresstests mit Bezug auf Wechselwirkungen. Alle Schlüsselsektoren der Wirtschaft auf der ganzen Welt sind gut beraten, ihre Wechselbeziehungen anhand von simulierten Cyberattacken einem Stresstest zu unterziehen. Dan Geer, Chief Information Security Officer bei In-Q-Tel, empfiehlt die Entwicklung von Cybersecurity Stresstestszenarien mit dem Ziel, folgende Frage zu beantworten: „Bin ich gegenüber Ausfällen von anderen, von denen ich abhängig bin, widerstandsfähig?“[16] Eine im Mai 2017 vom Belfer Center for Science and International Affairs der Harvard University veröffentlichte Studie hat diese Idee aufgegriffen und den potenziellen Vorteil unterstrichen, der sich mit der Durchführung solcher Tests durch Aufsichtsbehörden in kritischen Infrastrukturen erzielen lässt.[17]

---

15 The report ranked Singapore, the United States, Malaysia, Oman, Estonia, Mauritius, Australia, France, Georgia, and Canada as the most committed member states
16 The Pew Research Center, Spring 2017 Global Attitudes Survey, August 2017
17 World Economic Forum, 2017 Global Risks Report shareable infographics, January 2017

Freiwillige Bemühungen, die aktuell im Finanzbereich unternommen werden, umfassen die jüngsten Maßnahmen des Financial Services Information Sharing and Analysis Center (FS-ISAC) zur Einrichtung des Financial Systemic Analysis & Resilience Center (FSARC) und der Global Resilience Federation. Bemühungen wie diese könnten einschlägige Cybersecurity-Modelle für andere Sektoren schaffen.

Die FS-ISAC untersucht aktuell einen Ansatz für eine Machbarkeitsstudie zur Schaffung eines virtuellen Cyber Testgeländes, das so gestaltet ist, dass Organisationen in einem sicheren Umfeld Cyberattacken simulieren können. Mit diesen simulierten Angriffen soll die Widerstandsfähigkeit getestet werden, so Bill Nelson, Präsident und CEO der Organisation. Im Energiebereich wird alle zwei Jahre eine GridEx-Übung durchgeführt, die eine Cyberattacke bzw. einen physischen Angriff auf das Stromnetz, sowie auf weitere kritische Infrastruktur in ganz Nordamerika simuliert. Diese Form des realistischen Kriegsspiels ist für Matt Olsen von IronNet Cybersecurity durch nichts zu ersetzen.

Verstärkter Fokus auf Risiken im Hinblick auf Manipulation und Zerstörung von Daten. In einem Gespräch im April 2017 sagte Dan Geer voraus, dass Integrität die Vertraulichkeit als wichtigstes Ziel von Cybersicherheit in der Privatwirtschaft ablösen werde. Zudem meinte er, dass im Militärsektor Waffen, die auf Integrität abzielen, bereits weiter verbreitet seien als jene, die auf Vertraulichkeit abzielen.[18] Die Sheltered Harbor Initiative im Finanzbereich könnte ein Modell im Umgang mit diesen aufkommenden Risiken für andere Sektoren bieten. Diese Initiative hat Standards entwickelt, um Banken bei der Wiederherstellung von Kontodaten im Falle einer großen Cyberattacke zu unterstützen, führte Nelson aus. Der neue Praxisleitfaden des National Institute of Standards and Technology mit dem Titel „Data Integrity: Recovering from Ransomware and Other Destructive Events“, der als Entwurf im September 2017 veröffentlicht wurde[19], bietet Hilfestellung für die effiziente Wiederherstellung im Falle einer Beschädigung von Daten. Darüber hinaus könnte der Einsatz von Blockchain-Technologie vor allem dann relevant sein, wenn die Integrität von Transaktionen oder Daten kritisch ist, wie das US National Security Telecommunications Advisory Committee im Vorjahr in einem Entwurfsbericht anmerkte.[20]

Das Fazit lautet: Führungskräfte sollten jetzt die Gelegenheit nutzen und sinnvolle Maßnahmen in die Wege leiten, um die Widerstandskraft ihrer Organisationen zu stärken, Cyberrisiken standzuhalten und eine nachhaltig sichere digitale Gesellschaft zu schaffen.

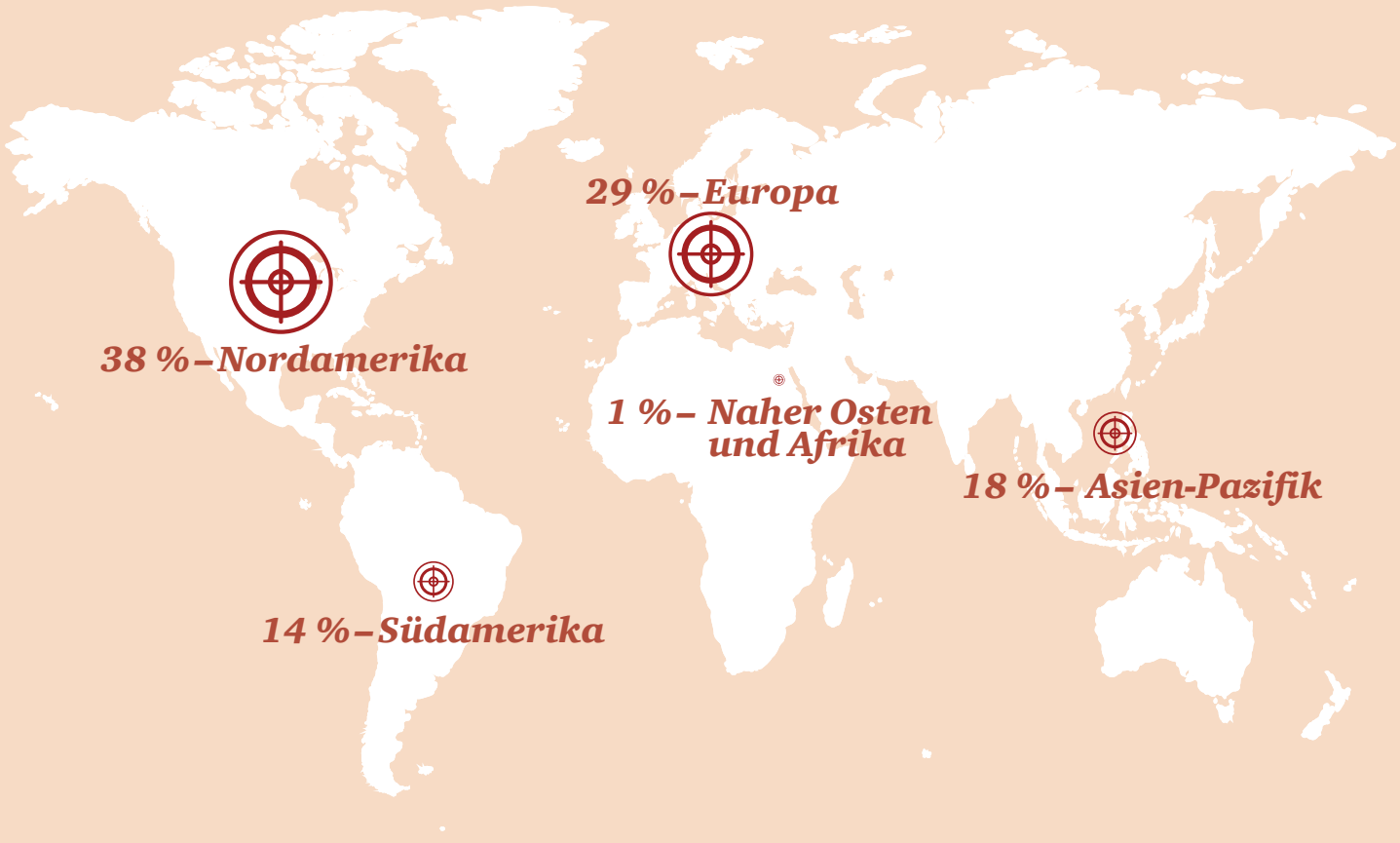
18 World Economic Forum, 2017 Global Risks Report, January 2017
19 “Additional views” statement by Sen. Susan Collins (R-ME) in US Senate Report 114-32, April 15, 2015
20 Black Hat, The 2017 Black Hat Attendee Survey: Portrait of an Imminent Cyberthreat, July 2017

Methodik

The Global State of Information Security® Survey 2018 ist eine weltweite Studie, die von PwC, CIO und CSO online vom 24. April bis 26. Mai 2017 durchgeführt wurde. Die Leser von CIO und CSO sowie Klienten von PwC wurden weltweit via E-Mail eingeladen, an dieser Studie teilzunehmen.

Die in diesem Bericht dargelegten Ergebnisse basieren auf den Antworten von über 9.500 CEOs, CFOs, CIOs, CISOs, CSOs, VPs und IT-Führungskräften sowie auf Sicherheitsmaßnahmen in mehr als 122 Ländern.

38 % der Studienteilnehmer kamen aus Nordamerika, 29 % aus Europa, 18 % aus dem asiatisch-pazifischen Raum, 14 % aus Südamerika und 1 % aus dem Nahen Osten und Afrika.



Die Schwankungsbreite beträgt weniger als 1 %; auf Grund von Rundungsdifferenzen ergibt die Basis nicht immer 100 %. Sämtliche Zahlen und Grafiken in diesem Bericht beziehen sich auf die Studienergebnisse.

Ansprechpersonen zu Cyberforensics

Steffen Salvenmoser
Partner
Tel.: +43 1 501 88-1104
Mobil: +43 676 833 77 1104
E-Mail: steffen.salvenmoser@pwc.com

Christian Kurz
Senior Manager
Tel.: +43 1 501 88 -1407
Mobil: +43 699 1630 5047
E-Mail: christian.kurz@pwc.com

www.pwc.at/gsiss
www.pwc.at/forensics

www.pwc.com/gsiss
www.pwc.com/cybersecurityandprivacy

Autoren

Christopher Castelli, Barbara Gabriel, Jon Yates,
and Philip Booth