DIGITAL INSIGHT Feb/22

EDITORIAL

Liebe Leserinnen und Leser,

Cybersicherheit ist die Voraussetzung für die digitale Transformation. Ohne eine sichere IT-Infrastruktur ergibt die fortschreitende Digitalisierung keinen Sinn, denn wir steigern nur unsere Angreifbarkeit als Gesellschaft. In Sachen Cybersicherheit sind wir in Deutschland nicht hinreichend gewappnet. Mit der Digitalisierung steigen auch Anzahl und Schwere der Hackerangriffe. Bei kritischen Infrastrukturen wurde der Handlungsbedarf erfreulicherweise erkannt; entsprechende behördliche Prozesse stehen bei Angriffen auf beispielsweise Krankenhäuser oder Stromanbieter bereit. Kleine und mittelständische Unternehmen hingegen sind meist sich selbst überlassen; viele von ihnen sind machtlos angesichts der Professionalität der Hacker. Dabei sind KMUs das wirtschaftliche Rückgrat unserer Gesellschaft. Die existentielle Bedrohung, die von systematischen Cyberattacken auf die deutsche Wirtschaft ausgeht, wird nicht ausreichend erkannt.

Daher widmet sich die erste Ausgabe der *Digital Insight* im Jahr 2022 dem Thema Cybersicherheit: Im *Comment* erörtert der Vorstandsvorsitzende der msg Dr. Stephan Frohnhoff, warum Cloud- und Netzanbieter zum Schutz vor Cyberattacken mehr zur Verantwortung gezogen werden sollten. In den *InBriefs* können Sie lesen, wie die Bilanz des Global Risks Report des Weltwirtschaftsforums für das Jahr 2022 ausfällt und warum es sich für Deutschland lohnen könnte, bei der Cybersicherheit dem Beispiel Israels zu folgen. In der Rubrik *InPerson* führen wir ein Interview mit Professor Dr. Pohlmann. Der Professor für Informationssicherheit und geschäftsführende Direktor des Forschungsinstituts für Internet-Sicherheit plädiert für eine gesamtgesellschaftliche Anstrengung, um der Cyberbedrohung entgegenzuwirken. In der Rubrik *InFocus* legen Frank Christian Sprengel und Andreas Höher dar, wie Cyber Security Exercises und ein “train as you fight“-Ansatz zum besseren Schutz vor Cyberangriffen beitragen.

Schließlich führt Anna Kassautzki, MdB der SPD-Fraktion, in der Rubrik *Political Voice* aus, was eine sichere Digitalisierung ausmacht.

Ich wünsche Ihnen viel Freude beim Lesen!

Regina Welsch
Redaktionsleitung *Digital Insight*,
Abteilungsleiterin Digitalpolitik, msg

INQUOTE

Olaf Scholz, SPD:
„Liebe Mitbürgerinnen und Mitbürger, wir stehen am Beginn eines neuen Jahrzehnts. Wir brechen auf in eine neue Zeit. Eine Zeit, die gut wird, wenn wir sie aktiv gestalten."
Am 31.12.2021 in der Neujahrsansprache

Volker Wissing, FDP:
„Mit dem G7-Vorsitz wird Deutschland in der Digitalisierung ein starkes Signal setzen für offene Standards und Diversität, für digitale Innovation sowie für unternehmerische und gesellschaftliche Initiative."
Am 13.01.2022 im Bundestag

Kevin Kühnert, SPD:
„Das, was bei der Digitalisierung getan werden muss, ist keine Raketenphysik mehr. Wir brauchen einen handlungsfähigen Staat, der zügig in der Lage ist zu handeln."
Am 29.01.2022 beim Tag der jungen Wirtschaft

Detlef Müller, SPD:
„Wir wollen, dass die Verwaltung in Deutschland endlich ein Niveau bei der Digitalisierung erreicht, wofür man sich international nicht mehr schämen muss."
Am 13.01.2022 im Bundestag

Tabea Rößner, Grüne:
„Die Digitalisierung bietet viele Chancen für die ökologisch-soziale Transformation in einer lebendigen Demokratie, für den Wirtschaftsstandort, für einen fairen Wettbewerb, diskriminierungsfreie Plattformen und einen gemeinwohlorientierten Ordnungsrahmen für neue Technologien. Zeit, sie endlich zu nutzen."
Am 25.06.2021 im Bundestag

Anna Kassautzki, SPD:
„Wir brauchen nicht nur sichere Verschlüsselung, sondern auch sichere Hard- und Software. Deswegen wollen wir zusätzlich eine HerstellerInnen-Haftung für Schäden auf den Weg bringen, die durch fahrlässig oder vorsätzlich verursachte IT-Sicherheitslücken entstehen."
Am 13.01.2022 im Bundestag

Renaud Deraison, CTO und Mitgründer von Tenable:
„Die Büchse der Pandora wurde geöffnet und Organisationen sind überall Cyber-Schwachstellen ausgesetzt: Kritische Infrastrukturen, Lieferketten, Unternehmen – alle haben das Potential schwerwiegende Folgen zu haben für Menschen, Wirtschaft und ganze Länder."
Am 19.01.2022 in Lanline

Nancy Faeser, SPD:
„Ich werde alles daransetzen, dass wir unsere Digitalisierungsprojekte mit voller Kraft vorantreiben. Die IT-Sicherheit ist immer Priorität."
Am 01.02.2022 auf dem Deutschen IT-Sicherheitskongress

Arne Schönbohm, BSI:
„Deswegen arbeiten wir intensiv an Initiativen wie der Allianz für Cybersicherheit oder dem Cybersicherheitsnetzwerk. Netzwerke, die dem kooperativen Austausch dienen und auch digitale Ersthelfer zur Verfügung stellen werden."
Am 06.11.2021 in der WirtschaftsWoche

msg COMMENT

Cyberattacken auf KMUs in Deutschland

Dr. Stephan Frohnhoff,
Vorstandsvorsitzender der msg

Das Jahr 2021 hat eindeutig gezeigt: Kein Unternehmen ist gegen Cyberattacken immun! Von den deutschen Unternehmen gaben 43 Prozent an, dass sie im Jahr 2021 mindestens eine Cyberattacke erleiden mussten. Laut einer Studie des Bitkomverbands sind neun von zehn Unternehmen von Cyberangriffen betroffen und jedes zehnte Unternehmen steht einer existenziellen Bedrohung gegenüber. Besonders die Gefahr sogenannter DDoS-Angriffe (engl. Distributed Denial of Service) nimmt zu. So stieg der Anteil von DDoS-Angriffen an der Gesamtzahl aller Cyberattacken von 18 Prozent im Jahr 2019 auf 27 Prozent im Jahr 2021. Die Schäden belaufen sich auf mehrere Milliarden Euro. Einige Staaten verwenden Cyberangriffe zudem als nationales Druckmittel; die Grenze zum Cyber-War ist schwer auszumachen.

Kleine und mittelständische Unternehmen (KMU) müssen sich bis dato selbst helfen, wenn sie angegriffen werden. Der Staat fokussiert seine Aufmerksamkeit auf Kritische Infrastrukturen (KRITIS) und KRITIS-Unternehmen. Daher stellen sich viele Unternehmen des Mittelstands die Frage, wann die Politik endlich ihre kritische Lage begreift und ihnen eine adäquate Unterstützung zusagt. Angriffsmuster und Intensität, zum Beispiel bei DDoS-Attacken im hohen Gigabit-Bereich, deuten darauf hin, dass auch diese Unternehmen Opfer sind; entweder sind sie Opfer international organisierter Kriminalität oder gar von gezieltem staatlich gefördertem Handeln geopolitisch aggressiver Staaten. Als Antwort auf die Cyberattacken der letzten Jahre erwähnen SPD, Grüne und FDP an zahlreichen Punkten im Koalitionsvertrag die Neuordnung der IT-Sicherheitspolitik. Ob das ausreicht oder ob KMUs ihre Cyber-Angelegenheiten weiter selbst regeln müssen, wird sich zeigen. Zur wirksamen Prävention von Cyberattacken sind Regularien erforderlich, welche die Eindämmung der für viele Unternehmen existenziellen Bedrohung gewährleisten. Dies gilt vor allem für die Abwehr von DDoS-Angriffen. Welche Lösungsstrategien sind zu erwägen?

Netz- und Cloud-Provider in die Verantwortung nehmen

Netz- und Cloud-Provider haben in der (digitalen) Welt eine besondere Stellung. Ohne sie funktioniert im Prinzip nichts mehr. Gerade deswegen ist es entscheidend, dass für diese Dienstleister hohe Sicherheitsstandards gelten. So ist es zum Beispiel nötig, allgemeine Sicherheitsstandards zur Abwehr von DDoS-Angriffen einzuführen. Um die Einfallstore für DDoS-Angriffe zu schließen, sollten Netz- und Cloud-Provider verpflichtet werden, Schutz- und Qualitätsstandards einzuhalten.

Bisherige Bestrebungen reichen nicht aus, um DDoS-Angriffe angemessen zu bekämpfen. So sieht zwar der im August 2021 hervorgebrachte Katalog der Sicherheitsanforderungen der Bundesnetzagentur vor, dass Internet-Service-Provider verpflichtet werden, sich gegen DDoS-Angriffe zu schützen und Maßnahmen zur Abwehr (Mitigation) zu treffen. Jedoch müssen die Kapazitäten nur so ausgelegt sein, dass die Funktionsfähigkeit bei einer mittelschweren Attacke ohne weitere Maßnahmen gewährleistet werden kann. Fraglich bleibt, bei welcher Datenmenge ein Angriff unter die Definition mittelschwerer Angriff fällt.

Auch für Cloud-Provider gab es erste Regulierungsversuche. Diese beschränkten sich allerdings oft auf Anbieter, die für KRITIS-Unternehmen oder Behörden arbeiten. So ist die Erkennung und angemessene Reaktion auf DDoS-Angriffe sowie der Einsatz eines Security-Information-and-Event-Management-Systems nur für Cloud-Provider verpflichtend, die für Behörden arbeiten (als Teilkriterium für die C5-Zertifizierung). Dabei gibt es Möglichkeiten, den Sicherheitsstandard zu verbessern und zu vereinheitlichen. Die Verantwortung liegt bei der Politik, die entsprechenden Rahmenbedingungen zu schaffen und für die Provider durchzusetzen.

Staatliche Unterstützung für nicht KRITIS-Unternehmen

Laut IT-Sicherheitsgesetz 2.0 und der Cybersicherheitsstrategie 2021 beziehen sich staatliche Cyberschutzmaßnahmen nur auf KRITIS-Unternehmen. Die Cybersicherheitsstrategie sieht jedoch vor, die regulatorischen Rahmenbedingungen mit Blick auf KMUs weiterzuentwickeln. Ziel ist dabei, die digitale Souveränität und Wettbe-

werbsfähigkeit der Unternehmen im Bereich Cybersicherheit auszubauen. KMUs sind im Angriffsfall auf konkrete Hilfe des Bundesamts für Sicherheit in der Informationstechnik: BSI oder anderer staatlicher Stellen angewiesen. Weiter muss die (inter-)nationale Zusammenarbeit zur Bekämpfung von Cyberkriminalität gestärkt werden. Mittelfristiges Ziel sollte eine klare Koordinierung der Vorgehen zur Abwehr von Cyberattacken sein. Die momentan bestehende Vielzahl an Gremien könnte eine effektive Kommunikation im Falle eines Angriffs erschweren.

Computer Emergency Response Teams (CERTs) aufrüsten

Strukturelle Probleme, wie etwa der IT-Fachkräftemangel, führen dazu, dass sich viele KMUs im Falle einer Cyberattacke nicht selbst helfen können. Daher ist es unbedingt notwendig, die staatlichen Hilfen auch für Nicht-KRITIS-Unternehmen zugänglich zu machen. Einen Ansatzpunkt bieten CERTs, die als zentrale Anlaufstelle für präventive und reaktive Maßnahmen auf Bundes- und Länderebene angesiedelt sind. Um zuverlässige, flächendeckende Hilfen für betroffene Unternehmen zu gewährleisten, benötigen die CERTs jedoch sehr viel umfassendere personelle und finanzielle Ressourcen als sie im Moment haben.

Staatliche Meldestelle und/oder Register für Cyberangriffe schaffen

Auf staatlicher Seite fehlt es bislang an Ressourcen zur effektiven Cyberabwehr; zudem existiert kein zentrales Register zur Erfassung von Cyberangriffen auf Unternehmen. Um das Ausmaß der Cyberangriffe auf KMUs zu erfassen, muss eine staatliche Meldestelle oder ein Register geschaffen werden. Ein zentrales Melderegister ist unerlässlich, um sich ein flächendeckendes, differenziertes Bild über die Cyberbedrohungslage in Deutschland zu machen und adäquate Maßnahmen zu ergreifen.

Cyberangriffe bedürfen eindeutiger politischer Antworten

Die Professionalisierung der Cyberangriffe hat ein Ausmaß erreicht, das den deutschen Mittelstand existentiell bedroht. Um dieser Bedrohung etwas entgegenzusetzen, bedarf es neben technischen und wirtschaftlichen Ressourcen einer eindeutigen innen- und außenpolitischen Antwort.

INBRIEF

Bilanz des Global Risks Report 2022: Cyberbedrohungen gehören zu den weltweit größten Risiken

In der 17. Ausgabe des Global Risks Reports[1] erarbeitet das Weltwirtschaftsforum in Kooperation mit Partnern wie der Zurich Insurance Group und der University of Oxford Prognosen zu den global akutesten Bedrohungen. Für das Jahr 2022 ist darunter auch das zunehmende Risiko, das von Cyberbedrohungen ausgeht.

Die Digitalisierung stellt laut Bericht besonders Entwicklungs- und Schwellenländer vor die Herausforderung, eine effektive Verteidigung gegen Cyberangriffe auf kritische Infrastrukturen sowie den Schutz persönlicher Daten und der Privatsphäre zu gewährleisten. Doch auch Industrienationen sind gegen großangelegte Cyberangriffe nicht immer ausreichend gewappnet. Laut dem Global Risks Perception Survey werden Cyberbedrohungen in diesen Ländern als besonders gefährlich eingestuft. Der Bericht diagnostiziert einen weltweiten Führungskräftemangel von ca. drei Millionen Cyberfachleuten und einen rapiden Anstieg von Ransomware-Angriffen, der sich im Jahr 2020 auf 435 Prozent belief. Außerdem seien 95 Prozent der Cybersicherheitsrisiken auf menschliche Fehler zurückzuführen, was die Relevanz einer umfassenden, universellen digitalen Bildung hervorhebt. Die Zunahme neuer Angriffspotentiale, welche mit der Fortentwicklung von Zukunftstechnologien einhergeht, übertrifft demnach die Fähigkeit von Regierungen und Gesellschaften, Schritt zu halten. Auch länderübergreifende Maßnahmen reichen bislang nicht aus, um internationale Cyberkriminalität und gesellschaftliche Bedrohungen wie die Verbreitung von Falschinformationen effektiv zu bekämpfen. Die weitere Zunahme von Cyberoffensiven birgt die Gefahr, dass internationale Konflikte in Zukunft neben dem physischen auch im digitalen Raum ausgetragen werden.

Der Global Risks Report hebt wissenschaftlich fundiert hervor, welche akuten Bedrohungen heute und in Zukunft im Cyberraum bestehen. Politische Weichenstellungen sind nun nötig, um die Cybersicherheit von Individuen, Unternehmen und Staatsapparaten effektiv zu gewährleisten.

Cybersicherheit: Israel als mögliches Vorbild für die Bundesrepublik

Die Corona-Jahre haben in Deutschland auf politischer und gesellschaftlicher Ebene zu der Erkenntnis geführt, dass beim Thema Cybersicherheit dringender Handlungsbedarf besteht. Um diesen zu realisieren, mag die Orientierung an Ländervorbildern wie Israel hilfreich sein.

Aber warum Israel? Schließlich führen andere Global Player wie die USA, das Vereinigte Königreich oder Estland die Cybersicherheits-Weltrangliste an.[2] Nun, das hightechaffine Land Israel bietet viele Argumente: Schließlich hat sich die israelische Regierung bereits im Jahr 2011 per Resolution das Ziel gesetzt, zum globalen Vorreiter in Sachen Cybersicherheit zu werden.[3] Eine Bilanz über das vergangene Jahrzehnt zeigt: Das ehrgeizige Vorhaben scheint Realität geworden zu sein. Die Höhe der in israelische Cybersecurity-Startups

getätigten Investments stieg im Jahr 2021 von 2,74 Milliarden (2020) auf 8,84 Milliarden US-Dollar. 45 Prozent der weltweiten privaten Cyberinvestments fließen heute in israelische Unternehmen; israelische Cyberexporte haben einen Gesamtanteil von zehn Prozent am globalen Markt.[5] Cyberexpertise zu vermitteln hat bei den israelischen Streitkräften und an den Universitäten des Landes eine hohe Priorität. Israel ist somit – im Gegensatz zu den meisten anderen Staaten – kaum vom Cyberfachkräftemangel betroffen.

Diese Cyberkompetenz veranlasste die Baden-Württembergische Landesregierung, sich Israel zum Vorbild zu nehmen. Im Rahmen der Verabschiedung der Cybersicherheitsstrategie zum Jahresende 2021 äußerte der Innen- und Digitalisierungsminister Thomas Strobl (CDU): „Diese Kompetenzen müssen wir uns erschließen, indem unsere Hochschulen, Behörden und staatlichen Einrichtungen die intensive Zusammenarbeit mit israelischen Einrichtungen suchen."[6]

Ein Blick auf Israel zeigt also: Große Fortschritte sind in kurzer Zeit möglich; ehrgeizige Ziele lohnen sich. Länder wie Israel als Vorbild beim Thema Cybersicherheit zu begreifen und deren ambitionierte Herangehensweise zu übernehmen, könnte auch für Deutschland erfolgsentscheidend sein.

Von der Redaktion

1 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
2 https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/
3 https://www.jpost.com/israel-news/cyber-week-how-israel-became-a-leader-in-cyber-tech-and-investment-674168
4 https://techcrunch.com/2022/01/04/israels-cybersecurity-startups-post-another-record-year-in-2021/
5 https://www.jpost.com/israel-news/cyber-week-how-israel-became-a-leader-in-cyber-tech-and-investment-674168
6 https://www.stuttgarter-nachrichten.de/inhalt.cybersicherheit-strategie-fuer-die-sicherheit-des-digitalen-baden-wuerttembergs.ec9225a8-50b2-44fd-8f63-c8c4c99669dc.html

INPERSON

Interview mit Herrn Professor Dr. Norbert Pohlmann

Die Cybersicherheitslage in Deutschland und die Verantwortung der Internet- und Cloud-Provider

Dr. Norbert Pohlmann ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit an der Westfälischen Hochschule. Zudem ist Professor Pohlmann Vorstandsvorsitzender des Bundesverbands IT-Sicherheit TeleTrusT und Vorstandsmitglied des Verbands der Internetwirtschaft eco. Weitere Engagements bilden seine Mitgliedschaft im Steuerkreis der BMWK-Initiative „IT-Sicherheit in der Wirtschaft" sowie in der Advisory Group der European Union Agency for Cybersecurity – ENISA.

Jonathan Ostertag: Herr Professor Pohlmann, die Cybersicherheitslage ist laut BSI-Bericht von 2021 prekär. Wie steht es aus Ihrer Sicht um die Cybersicherheit in Deutschland und was sind die Ursachen für die gestiegenen Cyberangriffe?

Professor Dr. Norbert Pohlmann: Wir stellen immer wieder fest, dass auch mit der Digitalisierung die Cybersicherheitsprobleme jedes Jahr größer werden. Daraus lässt sich unter anderem ableiten, dass unsere heutige IT nicht sicher genug konzipiert und aufgebaut ist, um den Angriffen intelligenter Hacker erfolgreich entgegenzuwirken. Insbesondere, da die Komplexität der IT-Systeme und -Infrastrukturen immer größer wird, die Methoden der Angreifer ausgefeilter und die Angriffsziele kontinuierlich lukrativer werden. Entsprechend steigen die Risiken sehr stark, was zu hohen Schäden führt. Auf der anderen Seite werden Cyberkriminelle immer erfolgreicher und können als kriminelles

Ökosystem ihre Leistungsfähigkeit steigern, was unsere digitale Zukunft gefährdet. Also, die Wortwahl „Alarmstufe Rot" des BSI-Präsidenten im BSI-Cybersicherheitslagebericht bringt es auf den Punkt.

J. O.: In einem Artikel für das dotmagazin schreiben Sie gemeinsam mit Ulla Coester von xethix Empowerment, dass eine erfolgreiche Digitalisierung das Vertrauen der Nutzer und Nutzerinnen gegenüber den IT-Lösungen erfordert. Dabei nennen Sie die Cybersicherheit als zentralen Bestandteil der Vertrauenswürdigkeit. Was meinen Sie damit?

N. P.: Cybersicherheit und Vertrauenswürdigkeit sind Grundvoraussetzung für den Erfolg der Digitalisierung. Ohne Cybersicherheit ergibt Digitalisierung keinen Sinn – denn, wenn wir in hohem Maße die IT-Systeme und -Dienste mit den vielen Anwendungen und Daten nutzen und davon abhängig sind, muss auch sichergestellt sein, dass diese kontinuierlich einsatzbereit sind. Dazu müssen sie adäquat geschützt werden.

Zusätzlich bringt die Digitalisierung für Nutzer und Nutzerinnen einen hohen Grad an Komplexität mit sich. Für sie wird es zunehmend schwieriger, die Technologie und deren Hintergründe zu verstehen. Daher ist es unbedingt notwendig, dass die Unternehmen vertrauenswürdig agieren. Dazu gehören auf jeden Fall die Bereitstellung und Umsetzung eines hohen Maßes an Cybersicherheit sowie eine passende Werteorientierung, damit Nutzer und Nutzerinnen Vertrauen aufbauen können. Gelingt dies nicht, werden sie neue Technologien nicht akzeptieren und Digitalisierung kann nicht gelingen.

Auf der Forschungsebene beschäftigen wir uns auf Basis eines Vertrauenswürdigkeitsmodells damit, aufgrund welcher Kriterien IT-Lösungen, Unternehmen und Branchen mithilfe einer sogenannten wahrgenommenen Vertrauenswürdigkeit Vertrauen beim Nutzer und der Nutzerin aufbauen können. Also, die Themen Cybersicherheit und Vertrauenswürdigkeit sind für die digitale Zukunft extrem wichtig.

J. O.: Vor allem Cloud-Provider haben in der digitalen Welt eine besondere Stellung. Welche Verantwortung haben diese Akteure hinsichtlich des benötigten Vertrauens in die IT-Branche?

N. P.: Wir hängen in Deutschland bezüglich der Nutzung von Cloud-Diensten hinterher. Das liegt vor allem an Sicherheitsbedenken und an fehlendem Vertrauen. Völlig zu Unrecht, denn wenn heute ein Mittelständler die eigene IT im Unternehmen mit eher wenig erfahrenem IT- und IT-Sicherheitspersonal betreibt, ist das im Prinzip schlechter, weil dies absolut nicht dem Stand der Technik entsprechen kann.

Es ist völlig klar: Die Zukunft liegt in der Cloud. Viele Aspekte sprechen für die Cloud – vor allem die Cybersicherheit und Verfügbarkeit von IT-Diensten sowie Daten. Auf der anderen Seite geben Unternehmen die Hoheit über ihre wertvollen Unternehmensdaten ab, denn diese sind dann nicht mehr auf den eigenen Servern gespeichert, sondern in der Cloud. Unter diesem Aspekt wiederum ist die Vertrauenswürdigkeit des Cloud-Anbieters entscheidend. Dies zeigt die Notwendigkeit, dass Cloud-Anbieter einen sehr hohen Stand an Cybersicherheit umsetzen und besonders vertrauenswürdig agieren.

INTERNET-PROVIDER UND CLOUD-PROVIDER

Während Internet-Provider eine Internetanbindung zur Verfügung stellen (wie die Telekom) bieten Cloud-Provider (wie Microsoft, Google oder Amazon Web Services) IT-Services online an, die normalerweise intern gehostet werden. Unterteilt wird hierbei in Infrastruktur, Plattform und Software. Zu den Services der Cloud-Provider zählen die dezentrale Speicherung und Verwaltung von Daten, der direkte Zugriff auf Software und Anwendungen ohne vorherige Installation sowie das Bereitstellen von Inhalten und Diensten.

J. O.: Kann die Zertifizierung von IT-Lösungen eine Vermittlerrolle für Vertrauen darstellen?

N. P.: Zertifizierung ist erst mal eine Vertrauenswürdigkeitsmaßnahme, die sehr hilfreich ist, um Vertrauen aufzubauen. Wenn Unternehmen ihre IT-Lösung zertifizieren lassen, ist das per se positiv. Allerdings stellt sich dann die Frage, wie weit die Zertifizierung geht. Bei vielen Zertifizierungen wird nur das zertifiziert, was tatsächlich umgesetzt worden ist. Werden beispielsweise Daten nicht verschlüsselt, dann lässt sich dieser Aspekt auch nicht zertifizieren, was dazu führt, dass dieses Kriterium komplett entfällt.

Im Bereich Cloud-Dienste sind einige Sicherheitsmaßnahmen wie „Confidential Computing" teilweise noch auf einer Forschungs- und Umsetzungsebene. Daher können wir davon ausgehen, dass sich der Level an Cybersicherheit in der Zukunft noch verbessern wird.

CONFIDENTIAL COMPUTING

Confidential Computing schützt Daten während der Nutzung, indem es Berechnungen in einer vertrauenswürdigen Ausführungsumgebung (engl. Trusted Execution Environment) durchführt. Diese sicheren und isolierten Umgebungen verhindern den unbefugten Zugriff oder die Änderung von Anwendungen und Daten während der Nutzung.

J. O.: Was ist mit den Schutzmaßnahmen, die Cloud-Provider bereits treffen können? Hier gibt es oft Abstufungen hinsichtlich der Sicherheit, was auch mit den Kosten zusammenhängt. Gibt es Möglichkeiten, eine Standardisierung nach dem Stand der Technik herzustellen, um so eine höhere Cybersicherheit zu erzeugen?

N. P.: Ja, das ist eine komplizierte Frage. Die Bereitschaft der Unternehmen mehr Geld für die Cybersicherheit auszugeben, ist im Allgemeinen nicht groß. Die Cloud-Anbieter bieten daher oft einen günstigen Grundpreis, um konkurrenzfähig zu bleiben. Sie argumentieren, dass für mehr Sicherheit auch mehr gezahlt werden muss. Das ist eben so, wie sich der Markt entwickelt hat. Da können wir im Prinzip nichts tun, denn jeder Geschäftsführer von Cloud-Diensten muss diese Entscheidung selber treffen.

Auf der anderen Seite haben wir Gesetze wie die Datenschutzgrundverordnung oder das IT-Sicherheitsgesetz. Diese schreiben vor, dass der Stand der Technik im Bereich Cybersicherheit zum Schutz der Daten und IT-Systeme eingesetzt werden muss. Doch dieser wird nicht immer umgesetzt. So setzen mehr als 90 Prozent der Cloud-Provider Passwörter für die Authentifizierung ihrer Nutzer und Nutzerinnen ein, was natürlich nicht dem Stand der Technik entspricht. Hier wäre Multifaktor-Authentifikation auf der Basis einer kryptografischen Grund-Authentifikation deutlich risikoärmer. Insgesamt besteht also ein großer Nachholbedarf, passende Cybersicherheitsmechanismen einzusetzen.

J. O.: Wie kommen wir zu einer passenden Cybersicherheit, die eine gute Basis für unsere Zukunft darstellen kann?

N. P.: Der größte Handlungsbedarf besteht darin, im Sinne unserer zukünftigen Wohlstandsabsicherung alle Voraussetzungen für eine souveräne, sichere und vertrauenswürdigere digitale Zukunft zu schaffen.

Politisch muss dafür gesorgt werden, dass wir Vorreiter beim Thema Cybersicherheit werden: Wir müssen IT-Security Made in Germany oder Made in Europe fordern und fördern, um uns angemessen und souverän heute und in Zukunft schützen zu können. Wir brauchen eine Stärkung der Cybersicherheit insgesamt ohne Wenn und Aber durch ein stringentes, konsistentes Vorgehen. Wir müssen die wichtigsten Maßnahmen, die zur Stärkung der Cybersicherheit führen, konsequent umsetzen. Staat, Industrie und Forschung müssen deutlich enger zusammenarbeiten, damit wirklich eine Verbesserung der Cybersicherheit stattfindet, und wir geeignete IT-Sicherheitstechnologien und Vorgehen zusammen umsetzen. Die Unternehmen in Deutschland geben im Schnitt ein Promille ihrer Umsätze für IT-Sicherheit aus. Wenn dieses Geld im Rahmen einer gemeinsamen Cybersicherheitsstrategie ausgegeben würde, könnten wir deutlich mehr und vor allem zusammen umsetzen, um eine gute Basis für die digitale Zukunft aufzubauen.

J. O.: Um ein Praxisbeispiel anzuführen: Wie könnte das in Bezug auf Schutzmaßnahmen gegenüber DDoS-Angriffen, auch im Hinblick auf die Kosten, gelingen?

DISTRIBUTED DENIAL OF SERVICE-ANGRIFFE

Bei Distributed Denial of Service (DDoS)-Angriffen werden mit Hilfe von verschiedenen Systemen (meist kompromittierte IT-Systeme) ausgesuchte Ziel-IT-Systeme mit so vielen Anfragen bombardiert, dass die Ziel-IT-Systeme die Anfragen nicht mehr verarbeiten können und aus Erschöpfung der Ressourcen zusammenbrechen. Prominente Angriffe dieser Art gab es auf Web-Server von Amazon oder eBay.[7]

N. P.: Bei DDoS-Angriffen ist die Idee, dass die Ressourcen von zentralen IT-Diensten im Cyberraum ausgeschöpft werden. Hierbei geht es um Bandbreite, CPU- und RAM-Kapazitäten. Der Angriff hat das Ziel, dass IT-Dienste nicht mehr verfügbar sind. Dies ermöglicht den Angreifenden Erpressungsgeld zu fordern, damit sie den Angriff stoppen.

Zur Abwehr gibt es sogenannte On-Site- und Off-Site-Mechanismen. On-Site-Mechanismen machen IT-Systeme robuster, können aber DDoS-Angriffe nicht gänzlich verhindern. Bei Off-Site-Möglichkeiten wird im Prinzip die Internetanbindung anders strukturiert, sodass Redundanzen geschaffen werden, mit denen sich eine Ausschöpfung der Ressourcen verhindern lässt.

Es gibt also Möglichkeiten, besseren DDoS-Schutz umzusetzen. Dabei geht es jedoch um eine Vorsorgesicherheit, die nur für den Fall eines DDoS-Angriffs benötigt wird. Vorausgesetzt, dass alle Unternehmen in Deutschland diese Vorsorgesicherheit verlangen würden, wären Cloud- und Internet-Provider eher bereit, dahingehend mehr zu investieren und so ein höheres Schutzniveau und damit eine höhere Robustheit unserer IT-Dienste zu erzeugen. Wenn sich aber momentan nur drei Prozent der Unternehmen auf diese Weise schützen, wird das im Einzelfall relativ teuer sein. Nur durch gemeinsame zielgerichtete Investitionen könnten die Kosten verteilt werden.

BANDBREITE, CPU UND RAM

Mit der Bandbreite wird die Geschwindigkeit der Datenübertragung über Internetverbindungen beschrieben. Der Hauptprozessor (engl. Central Processing Unit (CPU)) eines Computers / Servers ist dessen Kernstück und für alle Berechnungen der Anfragen über das Internet zuständig. Der Arbeitsspeicher (engl. Rapid Access Memory (RAM)) eines Computers / Servers ist der Speicher, der für die auszuführenden Programme und auszulesenden Daten bei einer Internetanfrage benötigt wird.

OPEN-SOURCE-TECHNOLOGIE, BUNDESTROJANER UND MULTI-FAKTOR-AUTHENTIFIZIERUNG

Open-Source-Technologien sind Programme, die im Prinzip alle, meist kostenlos, einsehen, ändern und nutzen können.[8] Als Bundestrojaner bezeichnet man in Deutschland die Online-Durchsuchung von Endgeräten durch die Ermittlungsbehörden mithilfe einer Software (eines sogenannten Trojaners).[10] Eine Multi-Faktor-Authentifizierung prüft die Zugangsberechtigung (z.B. zu Cloud-Diensten) durch mehrere, unabhängige Faktoren.[10]

J. O.: Abschließend noch ein Ausblick auf die nächsten Jahre: Was muss im Bereich Cybersicherheit gesamtgesellschaftlich getan werden und welche Entwicklungen gibt es bereits?

N. P.: Positiv ist, dass die Politik das Thema Cybersicherheit auf der Agenda hat. Im Koalitionsvertrag lässt sich relativ viel dazu finden: Das Recht auf Verschlüsselung, Schwachstellen-Management, Souveränität in Open-Source-Technologien oder die Abschaffung von Bundestrojanern. Entsprechende Diskussionen mit Politikern und Politikerinnen in diesem Bereich sind jedoch oft zu kleinteilig. Aus meiner Sicht müssten wir es zum Beispiel schaffen, den Grad an E-Mail-Verschlüsselung deutlich zu erhöhen. Zudem brauchen wir eine bessere Verifizierung von Web-Servern und Cloud-Anwendungen oder eine gemeinsame starke Multi-Faktor-Authentifizierung für alle Dienste. Auch müssen wir kleinere Unternehmen dabei unterstützen, dies umzusetzen. Gleichzeitig ist es notwendig, dass Unternehmen sich vertrauenswürdig darstellen, damit für die Nutzer und Nutzerinnen transparent wird, in welchen Bereichen Unternehmen wie agieren. Diese Transparenz lässt sich zum Beispiel über Reputationssysteme darstellen. Das eröffnet die Möglichkeit, positives Verhalten zu belohnen, um so die Unternehmen zu motivieren, sich zu verändern.

Ich bin davon überzeugt, dass der Staat die Möglichkeit hat, über Regulierungen, Anforderungen und Förderungen all diese Beispiele für einen höheren Level an Cybersicherheit zu motivieren.

Ziel muss es sein, dass wir die Cybersicherheit gemeinsam in den Griff bekommen. Historische Beispiele zeigen, dass es funktionieren kann, ein Problem gesamtgesellschaftlich zu lösen: Vor 30 Jahren hatten wir etwa 12.000 Tote im Straßenverkehr. Um diese Zahl zu minimieren, haben sich alle relevanten Akteure zusammengetan – Automobilhersteller, Straßenbauer, gesellschaftliche Organisationen, Wissenschaft und Politik. Mit einem guten Resultat: Die Straßen wurden verbreitert, die Verkehrsschilder deutlich sichtbarer, die Führerscheine optimiert und nicht zuletzt die Menschen auf wichtige Punkte aufmerksam gemacht – zum Beispiel mit der Sendung „Der 7. Sinn“. Heute haben wir weniger als 3.000 Tote. Durch die gemeinsame Anstrengung der Gesellschaft wurde also ein wichtiges Ziel erreicht – und zwar ohne die Mobilität einzuschränken. Genau das steht jetzt auch für die Cybersicherheit an. Wir werden keine hundertprozentige Sicherheit erzielen – das ist klar. Aber wir müssen deutlich besser werden.

J.O.: Herr Professor Pohlmann, vielen Dank für das Gespräch und Ihre Zeit.

Das Interview führte Jonathan Ostertag, Coordinator Digitalpolitik, msg

7 Weitere Informationen finden Sie z.B. unter: BSI - Denial-of-Service (DoS) und Distributed Denial-of-Service (DDoS) (bund.de), Distributed Denial of Service (DDoS) - Glossar - Prof. Pohlmann (norbert-pohlmann.com)

8 Weitere Informationen finden Sie z.B. unter: Technologische Souveränität im Cyber-Raum - Glossar (norbert-pohlmann.com)

9 Weitere Informationen finden Sie z.B. unter: Staatstrojaner / Bundestrojaner - Glossar - Prof. Dr. Pohlmann (norbert-pohlmann.com)

10 Weitere Informationen finden Sie z.B. unter: Authentifikation - Glossar - Prof. Dr. Norbert Pohlmann (norbert-pohlmann.com)

INFOCUS

Cyber Security Exercises: Cybersicherheitsplanspiele als Mittel die Resilienz in Unternehmen zu steigern

Andreas Höher, Head of Defense Consulting, msg

Frank Christian Sprengel, Repuco Unternehmensberatung GmbH

„Train as you fight" heißt es im militärischen Sprachgebrauch, wenn es darum geht, sich auf Herausforderungen in möglichen Einsatzlagen der Cybersicherheit aktiv vorzubereiten. In konventionellen bzw. historisch gewachsenen Einsatzräumen, so genannten Domänen (Land, See und Luft), wird dies seit jeher im Rahmen militärischer Übungen (Manövern) getan. Dabei verwendet man in der Regel das Material und Personal, das auch im realen Szenario zum Einsatz kommen würde.

In den „neuen" Domänen Weltraum sowie Cyber- und Informationsraum sind entsprechend neue Wege der Übung zu gehen, da sie hochdynamisch sind und durch ihre Digitalität eigenen Gesetzmäßigkeiten unterliegen. Daher bieten „Cyber Security Exercises" auf speziellen IT/OT-Systemumgebungen den idealen Raum, um das eigene Personal, Material, Verfahren und Taktiken in Aktion zu testen, ohne dabei ungewollte Spuren zu hinterlassen.

Cyber Security-Übungen sind am besten im internationalen Rahmen durchzuführen. Sie berücksichtigen dabei Szenarien, aus denen heraus sich ein relevantes „Drehbuch" für die Übungsanlage erarbeiten lässt. Die real-verantwortlichen Akteure sollten im Übungsverlauf, ihrem Tagesgeschäft entsprechend, die für die Cyber Security bereitstehende Infrastruktur nutzen und auf dieser ihre Aktionen umsetzen. Unterstützt werden die Übungseinlagen durch realitätsgetreue filmische Einspieler, die Realität und Fiktion für die handelnden Akteure verschwimmen lassen.

Das Besondere an diesen Übungen: Die Teilnehmenden üben auf einer physisch-digitalen Übungsplattform, die einen virtuellen/digitalen Zwilling einer IT/OT-Umgebung simuliert. Die Spielenden können im Verlauf der Übung über eine eigene Workstation bzw. über einen Remote-Access teilnehmen. Dabei können sie die Aufgaben mithilfe von bekannten und vertrauten Softwareprodukten analysieren, mediale und technische Entwicklungen monitoren, miteinander und mit Behörden kommunizieren sowie geeignete Interventions- bzw. Mitigationsmaßnahmen setzen.

Die Teams der jeweiligen Security Operation Center (SOC) arbeiten im Rahmen des Spiels autark, sind jedoch, wie in der realen Welt auch, miteinander verbunden. In Konferenzen und schriftlichen Abstimmungen werden dann Erkenntnisse ausgetauscht und mögliche Operationsweisen abgestimmt.

Neben den spielenden Teilnehmenden, die ein betroffenes internationales Unternehmen darstellen, spielen nationale und internationale Behörden-Vertretende mit, die den NIS-Regeln[11] entsprechende Meldungen entgegennehmen und auf diese reagieren. Die Übungsleitung beobachtet den Übungsverlauf und betreibt mit entsprechenden Einspielern den Fortschritt der Übung.

Internationale Beobachtende sowie Entscheiderinnen und Entscheider haben zudem die Möglichkeit, passiv (physisch als auch digital) am Übungsgeschehen teilzunehmen und informieren sich so über die Rahmenbedingungen, das Szenario und die Umsetzungsschritte, mit denen die Übenden die Aufträge erfüllen bzw. die ihnen gestellten Herausforderungen meistern.

Damit dieses Vorhaben gelingt, ist ein „Einschulungstermin" nötig. An diesen Übungstermin werden die Übenden mit allen Rahmenbedingungen, Rollen und Prozessen vertraut gemacht; so kann dem postulierten Credo „train as you fight" in der Tat entsprochen werden.

Als wesentliche Erkenntnisse des „train as you fight"-Ansatzes stehen zum Schluss die Einsichten, dass nur durch solche Übungslagen eine realitätsnahe Vorbereitung auf reale Einsatzlagen möglich ist.

Auch ist davon auszugehen, dass ein Großteil der Teilnehmenden die Übungsteilnahme als Bereicherung empfindet, da die SOC-Teams interdisziplinär mit fixierten Rollen zusammengesetzt sind und sie außerhalb der gewohnten Denkmuster und ohne gravierende Konsequenzen befürchten zu müssen, üben können. Gemeinsam wird es den Teams somit gelingen, die gesetzte Lage zu meistern und für den eigenen realen Betrieb wertvolle Erfahrungen zu sammeln. Durch den Austausch wird zudem das individuelle Netzwerk an Kompetenzträgerinnen und -trägern erweitert und damit ein Beitrag zur Vernetzung der Security Community gewährleistet.

Eine State-of-the-art-Übungsplattform: Der physische und digitale Austausch sowie die Untermalung durch ein realistisches, interessantes Szenario sind dabei erfolgskritisch und unabdingbar, um effektive Cybersicherheitsübungen durchzuführen. Nur der „train as you fight"-Ansatz in Verbindung mit regelmäßig durchzuführenden Cybersicherheitsplanspielen kann die Resilienz von Organisationen wirkungsvoll steigern.

Von Andreas Höher, Head of Defense Consulting, msg und Frank Christian Sprengel, Repuco Unternehmensberatung GmbH

11 Regeln der Richtlinie zur Netz- und Informationssicherheit

POLITICAL VOICE

mit MdB Anna Kassautzki, Ordentliches Mitglied im Ausschuss für Digitales und Mitglied der SPD-Fraktion im Deutschen Bundestag

Digitalisierung – aber sicher!

Was früher die Postkarte aus dem Urlaub war, ist heute ein Bild, eine Text-, Sprach-, oder Videonachricht. Wir verlassen uns darauf, dass unsere Chats privat sind, ohne das mit Gewissheit sagen zu können. Ob nun absichtlich oder auch unbewusst, zum Beispiel durch Metadaten, wir teilen mehr sensible Informationen als je zuvor. Im digitalen Raum sind Datenschutz und Informationssicherheit kein Expert*innenproblem mehr, sondern gehen uns alle an. Um private Kommunikation zu gewährleisten, auch die der technisch Unbedarften, benötigen wir standardmäßig sichere Verschlüsselung – ohne Hintertüren und Schlupflöcher. Ein Recht auf Verschlüsselung für alle werden wir einführen.

Die Softwareprodukte, die wir nutzen, bestehen häufig zumindest in Teilen aus Open-Source-Projekten, die – oft in ehrenamtlicher Arbeit – hergestellt und öffentlich zur Verfügung gestellt werden. Während also Produkte, die auf Open-Source-Software basieren, oftmals Millionen erwirtschaften, so findet die Entwicklung selbst immens wichtiger Komponenten viel zu oft als personell und finanziell schlecht ausgestattetes Freizeitprojekt engagierter Programmierer*innen statt. Damit möchte ich mich explizit nicht dagegen aussprechen, ganz im Gegenteil: Open-Source-Software kann von unabhängigen Sicherheitsexpert*innen jederzeit überprüft werden. Das schafft Transparenz und Vertrauen, hilft Lücken schnell zu schließen und erhöht damit die Sicherheit für uns alle. Das bedeutet aber, dass Open-Source-Entwicklung ordentlich gefördert werden muss. Das passiert zukünftig beispielsweise darüber, dass Hard- und Software, die mit öffentlichen Mitteln finanziert oder gefördert wird und dem keine relevanten Sicherheitsinteressen entgegenstehen, auch als Open-Source-Projekte der Allgemeinheit zur Verfügung gestellt werden: Public Money, Public Code.

Starke Verschlüsselung und aktuelle Software schützen uns alle. Wenn in Open-Source-Projekten Lücken gefunden werden, gibt es zumeist schnell Patches, um diese zu beheben. Sobald Sicherheitslücken gefunden werden, müssen diese umgehend in allen Produkten geschlossen werden. Dafür wollen wir die Hersteller*innenhaftung einführen: Wer fahrlässig oder mutwillig Sicherheitslücken verursacht, muss für entstandene Schäden auch haften.

Solche Lücken als Einfallstore für Cyberangriffe sind insbesondere bei kritischer Infrastruktur fatal. Dem öffentlichen Sicherheitsinteresse stehen hier viele unbesetzte IT-Stellen in Behörden gegenüber. Mich persönlich freut es deswegen besonders, dass es die Flexibilisierung der Einstellungsvoraussetzungen in den Koalitionsvertrag geschafft hat. Damit wird Erfahrung auch ohne einschlägiges Studium wertgeschätzt – viele ITler*innen, die ich kenne, sind Quereinsteiger*innen aber deshalb nicht weniger kompetent. In Kombination mit sicheren Jobaussichten, Aufstiegschancen und einer guten Altersvorsorge kann der öffentliche Dienst eine echte Alternative sein. Und hochqualifizierte und -motivierte IT-Expert*innen, sind neben starker Verschlüsselung und robuster Hard- und Software unser bester Schutz gegen Cyberangriffe.

Auch Unternehmen sind davon betroffen. Dabei stehen Unternehmen, die ihr Geschäft in der digitalen Welt ausweiten wollen vor der Herausforderung, nicht nur sichere und technisch einwandfreie Systeme zu implementieren und stetig zu pflegen, sondern diese auch für ihre Mitarbeiter*innen und User*innen einfach nutzbar zu machen. Dabei sollte bei der Konzeption immer die Frage im Raum stehen: Welche Daten und Datensätze müssen tatsächlich mit dem Internet verbunden sein und wie können wir diese sicher schützen? Neben der technischen Sicherung und guten Konzeption muss allerdings auch die Awareness für Sicherheit im Netz steigen – nicht nur bei Unternehmen, sondern bei uns allen.

Viele von uns nutzen Systeme, ohne zu wissen, wie sie funktionieren. Wie die Menschen im Mittelalter der Kirche, müssen die meisten von uns den Programmen glauben, dass sie wirklich das tun, was sie behaupten. Häufig ist der Einstiegspunkt für Cyberangriffe keine Softwarelücke, sondern Mitarbeiter*innen (Chef*innen nicht ausgenommen), die auf Links in einer E-Mail klicken und ihre Zugangsdaten eingeben. Ich fordere nicht, dass alle Menschen programmieren lernen – das ist illusorisch. Ich fordere aber, dass Unternehmen, die öffentliche Hand und wir alle die Wichtigkeit der Sicherheit im digitalen Raum verstehen, uns fortbilden und gemeinsam daran arbeiten, dass der “Risikofaktor Mensch” in der IT-Security kleiner wird. Die Digitalisierung und damit der weitere Einstieg in die Digitalität geht stetig voran und das ist gut so. Dabei ist mir allerdings wichtig, dass wir nicht “Digitalisierung first – Bedenken second” fahren, sondern die wichtigen Sicherheitsaspekte von Anfang an mitdenken.

VERANSTALTUNGSHINWEISE

24.02.2022, FZI Open House 2022
Open-House-Veranstaltung zur Veranschaulichung des dezentralen Technologie- und Wissenschaftstransfers.
Veranstalter: FZI Forschungszentrum Informatik
Ort: Online
Anmeldung unter: https://www.fzi.de/veranstaltungen/fzi-open-house/

23.03.2022, eGovernment Kommunal 2022
Plattform für den Wissensaustausch mit Panel-Diskussionen, Best Practices und Networking über die Digitalisierung in der kommunalen Verwaltung.
Veranstalter: Vogel IT-Akademie
Ort: Online
Anmeldung unter: https://www.egovkommunal.de/anmeldung

14.03.2022, Data Debates #21: „Die digitale Aufholjagd"
Paneldiskussion über die Digitalisierungsmaßnahmen und -pläne der neuen Bundesregierung.
Veranstalter: Tagesspiegel, Telefónica Deutschland/o2
Ort: Online
Anmeldung unter: https://www.basecamp.digital/event/data-debates-21-die-digitale-aufholjagd/

STELLVERTRETENDE REDAKTIONSLEITERIN:

Antonia Dittrich

MITWIRKENDE AUTOREN UND AUTORINNEN:

Julia Gronenberg

Jonathan Ostertag

Emil Schenkyr

IMPRESSUM

Herausgeber
msg systems ag
Robert-Bürkle-Straße 1
85737 Ismaning/München
Deutschland

Verantwortlich:
Dr. Stephan Frohnhoff (Vorsitzender),
Rolf Kranz,
Dr. Aristid Neuburger,
Karsten Redenius,
Dr. Frank Schlottmann,
Dr. Jürgen Zehetmaier
Aufsichtsratsvorsitzender:
Johann Zehetmaier

Redaktionsleitung:
Regina Welsch
msg systems ag
Friedrichstraße 120, 10117 Berlin
Mobil: +49 1520 238 5842
E-Mail: public-affairs@msg.group