Mehr Digitalisierung, höhere Cyberrisiken: Status Quo und Trends

Michael Waidner

Michael Kreutzer

Stefan Wunderlich

Die Chancen der Digitalisierung in Wirtschaft, Staat und Gesellschaft gehen mit grossen Herausforderungen in den Bereichen IT-Sicherheit und Privatsphärenschutz einher. Angesichts der steigenden Verbreitung und Komplexität von Software, Hardware und Internetdiensten sowie der Entwicklung immer neuer Angriffstechniken wächst die Gefahr von Cybervorfällen. Unternehmen sollten daher regelmässig Risikoanalysen durchführen und Massnahmen ergreifen, um mögliche Schäden abzuwenden oder zu mildern. Eine Erhöhung des Gesamtsicherheitsniveaus erfordert jedoch auch strategische Massnahmen und staatliches Handeln wie zum Beispiel die Erarbeitung und Durchsetzung auditierbarer Mindeststandards.

Die digitale Transformation hat heute faktisch alle Bereiche der Wirtschaft erfasst, von Finanz- und Versicherungswesen, über industrielle Fertigung und Maschinenbau, Mobilitätswirtschaft, Logistik oder Gesundheitswirtschaft bis hin zur Agrarindustrie. Hochgradig vernetzte Geräte, datengestützte Dienstleistungen und Geschäftsmodelle, neue Technologien wie 5G, maschinelles Lernen und autonomes Fahren treiben Innovationen, die den gesellschaftlichen und wirtschaftlichen Fortschritt voranbringen und für ein Plus an Lebensqualität und Wohlstand sorgen. Die Chancen der Digitalisierung in Wirtschaft, Staat und Gesellschaft gehen mit grossen Herausforderungen in den Bereichen IT-Sicherheit und Privatsphärenschutz einher. Je mehr Bereiche des gesellschaftlichen Zusammenlebens, der Wirtschaft und der öffentlichen Verwaltung von der Digitalisierung erfasst werden, desto grösser wird die Angriffsfläche und desto stärker steigt das Risiko von Cybervorfällen, sei es durch Einwirkung von aussen – durch gezielte Angriffe, breit gestreute Phishing- oder Malware-Kampagnen oder Social Engineering – oder verursacht von Innentätern. Vielfach haben die Angreifer leichtes Spiel, weil sie Fehlkonfigurationen und Fehlbedienungen ausnutzen können.

Die wirtschaftlichen Schäden durch Cybervorfälle sind enorm: Allein für die deutsche Wirtschaft geht der Branchenverband Bitkom für den Zeitraum 2018 bis 2019 von einem Gesamtschaden von mehr als 100 Milliarden Euro pro Jahr aus; das ist eine Verdopplung gegenüber dem Zeitraum 2016 bis 2017 (Bitkom, 2019). Neben Produktionsausfällen und dem Abfluss geistigen Eigentums schlagen dabei insbesondere auch die Kosten für Krisenmanagement, Vorfallbehandlung, die Wiederherstellung der Betriebsfähigkeit und Imageschäden zu Buche. Die Motive der Angreifer sind ebenso vielfältig wie die Angriffsszenarien. Sie sind nicht auf finanziellen Gewinn beschränkt, sondern reichen bis hin zu Cyberspionage und -sabotage sowie der Destabilisierung von Staaten. So stehen zum Beispiel auch kritische Infrastrukturen, also Einrichtungen, deren Ausfall zu Versorgungsengpässen oder erheblichen Beeinträchtigung des gesellschaftlichen Lebens führen können, immer häufiger im Visier. 2015 führte ein Angriff auf Stromversorger in der Ukraine zum ersten grossflächigen Blackout durch einen Hackerangriff (Süddeutsche Zeitung, 2016). 2018 missglückte ein Angriff auf eine petrochemische Anlage in Saudi-Arabien, die eine beträchtliche Zahl an Menschenleben hätte kosten können, nur knapp aufgrund eines Programmierfehlers des Angreifers.[1] Selbst Angriffe mit Bereicherungsabsicht können Menschen töten. Nach einem Cybervorfall im Universitätsklinikum Düsseldorf in diesem Jahr stand der Tod einer Patientin, deren Rettungswagen aufgrund des Vorfalls umgeleitet werden musste, in direktem Zusammen-

Die Autoren

Prof. Dr. Michael Waidner ist Direktor des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE, Professor an der Technischen Universität Darmstadt, Institutsleiter des Fraunhofer-Instituts für Sichere Informationstechnologie SIT und Chief Digital Officer (CDO) der Wissenschaftsstadt Darmstadt.

Dr. Michael Kreutzer ist zuständig für Internationalisierung und strategische Industriebeziehungen am Fraunhofer-Institut für Sichere Informationstechnologie SIT.

Dr. Stefan Wunderlich ist Referent für Cybersicherheit mit dem Schwerpunkt Wirtschaft beim Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE.

hang mit einem Cyberangriff (Handelsblatt, 2020).

Unsere IT ist fundamental unsicher

Ein hohes Niveau an Cybersicherheit ist eine notwendige Voraussetzung für eine zukunftssichere Digitalisierung von Wirtschaft, Staat und Gesellschaft. Eine der tragenden Säulen von Cybersicherheit ist die Informationstechnologie, die nicht nur funktioniert, sondern die auch überprüfbar sicher ist. Tatsächlich sehen wir aber in der Sicherheitsforschung Sicherheitslücken und Schwachstellen in praktisch allen Bereichen von IT-Infrastrukturen:

- Das Internet, als Rückgrat der Digitalisierung und zweifellos wichtigste Kommunikationsinfrastruktur unserer Zeit, basiert auf Basis-Technologien und -Protokollen, die grösstenteils bereits viele Jahrzehnte alt sind und oftmals verblüffend einfach manipuliert und anschliessend angegriffen werden können.[2]
- Software ist heute umfangreich und kompliziert und wird unter dem Druck einer immer schnelleren Time-to-Market so schnell und agil entwickelt, dass eine angemessene Qualitätsprüfung oft als «zu aufwändig» erscheint. Häufig findet noch nicht einmal eine automatisierte Schwachstellenanalyse vor dem Go-live statt. Spezialistinnen und Spezialisten für Softwaresicherheit am Fraunhofer-Institut für Sichere Informationstechnologie SIT fanden in allen Softwareprodukten, die sie untersuchten, Schwachstellen allein schon mittels automatisierter Scans; und dies nur bei Betrachtung des Binärcodes.[3]
- Mobile Apps spielen eine immer bedeutendere Rolle in Wirtschaftsleben und Gesellschaft. Eine kürzlich publizierte Studie der Technischen Universität Darmstadt weist nach, wie eine grosse Zahl der untersuchten Android-Apps durch die Verschleierung von Quellcode unsichere Internetzugriffe, unsichere Verwendungen von Kryptografie und Missbräuche von Zugriffsrechten verdeckten (Glanz et al., 2020). Die jährliche Analyse der 2 000 am häufigsten installierten kostenlosen Apps mit dem Analysetool Appicaptor des Fraunhofer SIT deckte 2019 auf, dass 53 Prozent der iOS- und 66 Prozent der Android-Apps HTTP-Verbindungen nutzen, um Inhalte wie HTML-Seiten und JavaScript-Code zu laden. Diese Verbindungen sind nicht verschlüsselt und vielfach fehlerhaft implementiert (Fraunhofer SIT, 2019).
- Auch Hardwarekomponenten, Vernetzungshardware und Endgeräte sind angreifbar. Im Sommer 2018 wurde die Hardwaresicherheitslücke Meltdown in einer weit verbreiteten Prozessorfamilie entdeckt und konnte zunächst nicht geschlossen werden. Geräte zur Anbindung der «letzten Meile» zu kleinen und mittelständischen Unternehmen sowie zu Privathaushalten erweisen sich vielfach als unsicher (Rotenberg et al., 2017). Bei einer Analyse von 33 VoIP-Telefongeräten verschiedener Hersteller haben Forscher des Fraunhofer SIT 40 teils gravierende Schwachstellen gefunden, deren Ausnutzung es Angreifern ermöglicht hätte, Gespräche abzuhören, das Telefon ausser Betrieb zu setzen oder sich sogar Zugriff auf das Firmennetzwerk zu verschaffen.[4]

Hyperkonnektivität, Hyperkonvergenz und dynamische Informationsökosysteme

Anders als bei physischen Risiken handelt es sich bei der «IT-Sicherheitslage» um eine hochgradig dynamische Bedrohungssituation, die sich permanent weiterentwickelt. Der technische Fortschritt und neue Anwendungen befeuern hier drei «Meta»-Trends, die eine Vervielfachung der Angriffsfläche bewirken: Heutige und künftige Schlüsseltechnologien der Digitalisierung weisen einen immer höheren Grad an Vernetzung auf (Hyperkonnektivität), die Übergänge zwischen IT-Systemen werden immer nahtloser (Hyperkonvergenz), und die Dynamik der Informationsökosysteme steigt auf eine quantitative und qualitative Weise.

Hyperkonnektivität: Aktuell werden Kommunikationsnetzwerke für Spezialzwecke wie Long Range Wide Area Network (LoRaWAN), Bluetooth LE, HiFlecs, Zigbee, Z-Wave und Industrial Ethernet eingeführt. Diese interagieren im Hintergrund mit anderen innovativen Infrastrukturkomponenten wie beispielsweise Cloud-basierten Back-end-Systemen. Die Installation und Steuerung von Hardwarevernetzungskomponenten erfolgt zunehmend mittels Network Function Virtualization (NFV), was das Herstellen von Konnektivität zwischen diversen Komponenten weiter erleichtert.

Die International Data Corporation (IDC), eine Dienstleisungs- und Beratungsagentur im Bereich Informationstechnologien, rechnet für das Jahr 2025 mit 41,6 Milliarden vernetzten IoT-Geräten.[5] Statista prognostiziert sogar 75 Milliarden vernetzte Geräte bis 2025.[6] Gleichzeitig wird das Breitbandnetz ausgebaut und die Einführung der fünften Mobilfunkgeneration, 5G, die eine performante Kommunikation zwischen diesen Geräten ermöglichen soll, läuft an. Insgesamt entstehen so stark untereinander verbundene Netze von Netzen, über die immer mehr Komponenten miteinander verbunden werden.

Hyperkonvergenz: Der von der OECD 1997 beschriebene Trend zur Konvergenz der globalen Informationsinfrastruktur (Committee for Information, Computers and Communications Policy, 2017) ermöglicht einen nahtlosen Übergang zwischen Technologien oder Infrastrukturen sowie zwischen Inhalten, Diensten und Anwendungsebenen. Leicht zu erkennen ist dies beispielsweise bei Endgeräten: Quasi alle Büroarbeitsplätze sind mit Laptops als universelles Arbeitswerkzeug ausgestattet. Ein Smartphone stellt heute eine Plattform für mehrere Anwendungen wie Telefonie, Internet-Surfen und Social Networks bereit. Ein modernes Kombigerät im Büro vereint Telefon, Fax, Drucker und Scanner.

Konvergenz und Digitalisierung haben synergetische neue IT-, Kommunikations- und Unterhaltungsdienste geschaf-

fen. Betriebssystemübergreifende Onlinedienste wie Webshops und Internettools sind heute allgegenwärtig. Kommunikations- und Kollaborationsinfrastruktur sowie Geschäftsanwendungen wie CRM- und ERP-Lösungen werden von Unternehmen und Behörden mehr und mehr als Dienstleistung über die Cloud (Software as a Service (SaaS)) bezogen, in der Regel per Abonnement. Darüber hinaus wurden neuartige weltweite Plattformen wie App-Stores, Messenger und Social Networks eingeführt, die nahtlos von allen vernetzten Endgeräten genutzt werden können. Kommunikationsanwendungen wie Telefonie, Videokonferenz, E-Mail, SMS und Instant Messaging gehen ineinander über und auf. Multimodalität gehört somit inzwischen zum Alltag, die Konvergenz hat sich zur Hyperkonvergenz ausgeweitet.

Informationsökosysteme: Die grossen digitalen Techkonzerne aus den USA wie Apple, Amazon, Alphabet/Google, Facebook und Microsoft entwickeln statt Einzelanwendungen mehr und mehr geschlossene Plattformökosysteme – auch und gerade für Informationen. Die aktuellen Entwicklungen im Bereich von Big-Data-Analysen, insbesondere mit Hilfe maschinellen Lernens, ermöglichen eine Vielzahl von Strukturierungen, Auswertungen, die Erkennung von Vorgängen in der realen Welt sowie Analysen bis hin zu Interpretationen und Schlussfolgerungen. Eine offensichtliche Anwendung ist die Verarbeitung natürlicher Sprache, die zunehmend akkurater wird. Ein weiteres Beispiel sind wissensbasierte Systeme, die Analysemöglichkeiten in vielen Sektoren erweitern, wie etwa in der Produktion oder im Gesundheitswesen.

Neue Gefährdungstrends

Aus den beschriebenen Trends resultiert eine Erhöhung der Angriffsfläche. Die wachsende IT-Durchdringung unseres Alltags schafft immer neue Angriffsziele für eine Vielzahl von Aggressoren – darunter ressourcenmächtige Angreifer wie Staaten, quasi-staatliche Akteure und das organisierte Verbrechen. Gleichzeitig lässt sich eine zunehmende Professionalisierung der Angreifer konstatieren, denen zudem immer ausgereiftere Tools zur Verfügung stehen (Waidner et al., 2017, S. 11).

Cyberkriminelle agieren heute nicht mehr nur als Einzeltäter, sondern gehen zunehmend organisiert und arbeitsteilig vor. So ist es beispielsweise möglich, über das Darknet Botnetze zu mieten, um mit deren Hilfe einen DDoS-Angriff auszuführen (Süddeutsche Zeitung, 2019). Durch die Verfügbarkeit solcher Dienstleistungen sowie immer leistungsfähigerer Tools für die Automatisierung von Angriffen sinken die Anforderungen an die technischen Kenntnisse und Fähigkeiten von Angreifern.

Angreifern stehen heute eine Vielzahl von manuellen, halbautomatisierten und vollautomatischen Angriffswerkzeugen zur Verfügung, deren Zahl in Zukunft noch zunehmen dürfte. Technische Innovationen wie zum Beispiel das maschinelle Lernen tragen zwar zur Verbesserung der Verteidigung gegen Cyberbedrohungen bei, etwa bei der Detektion von Anomalien in Netzwerken oder der Erkennung von Angriffsmustern. Dieselben Innovationen führen jedoch auch auf der Gegenseite zu Durchbrüchen bei den Angriffstechniken (Waidner et al., 2017, S. 11). So können beispielsweise neuronale Netze so trainiert werden, dass sie auf Basis von automatisiert erhobenen Informationen über Zielpersonen Phishing-E-Mails erzeugen – dies geht in die Richtung eines vollautomatischen Spear-Phishings (Forbes, 2018). Auch Blockchain-Technologien wie zum Beispiel Blockchain DNS, ein Adressdienst ohne zentrale Registrierungsstelle wie ICANN oder DENIC, können so genutzt werden, dass sie die Aktivitäten von Cyberkriminellen schützen.[7]

Cyberrisiken regelmässig analysieren

Da sich sowohl die Bedrohungslage als auch die zu schützende IT-Infrastruktur kontinuierlich wandelt, sollten Unternehmen regelmässige Risikoanalysen zur Sicherheit ihrer IT-Systeme durchführen (Kraft und Stöwer, 2017) und basierend auf dem Ergebnis entsprechende Massnahmen umsetzen. Im initialen Schritt gilt es dabei, diejenigen IT-Komponenten zu identifizieren, die für die Aufrechterhaltung der kritischen Geschäftsprozesse in Bezug auf das Kerngeschäft des Unternehmens essenziell sind und die daher im Fokus der Analyse stehen sollten. Die eigentliche Risikoanalyse kann dabei grob in drei Phasen unterteilt werden:

In Phase 1 wird für die zuvor identifizierten kritischen Komponenten in Abhängigkeit vom möglichen Schadensausmass das Risiko bestimmt und bewertet. Mögliche Schäden resultieren beispielsweise aus Produktionsausfällen, Compliance-Verstössen, Vertrauens- und Reputationsverlusten oder der Nichterfüllung anderer externer Verpflichtungen.

In Phase 2 werden die erfassten potenziellen Schäden hinsichtlich ihrer Risiken für das Unternehmen bewertet. Hier bieten sich Risikomatrizen an, in denen unternehmensspezifisch Eintrittswahrscheinlichkeit und Schadensausmass abgebildet werden. Da in der Regel keiner der beiden Werte quantitativ geschätzt werden kann, bieten sich hier mehrstufige qualitative Kategorien an.

In Phase 3, der Risikobehandlung, ist zunächst für jedes betrachtete Risiko grundlegend zu entscheiden, ob es akzeptiert, durch Umstrukturierung des risikobehafteten Prozesses oder Verzicht auf problematische Technik und sensitive Daten vermieden, durch Outsourcing oder Abschluss von Versicherungen verlagert oder durch geeignete Massnahmen verringert werden soll oder muss. In der Regel sollte das Augenmerk darauf gerichtet sein, die Risiken mit geeigneten Massnahmen zu minimieren, also die Wahrscheinlichkeit von Sicherheitsverletzungen und deren Auswirkungen zu verringern.

Strategien zur Erhöhung des Gesamtsicherheitsniveaus

Individuelle Massnahmen von Unternehmen oder Organisationen zur Minderung von Cyberrisiken sind notwen-

dig, können jedoch das Gesamtniveau der Cybersicherheit nur punktuell verbessern. Hierfür sind strategiegetriebene Aktivitäten auf nationaler wie internationaler Ebene erforderlich (Waidner et al., 2017, S. 13).

In allen Branchen führen risikoadäquate Mindeststandards bezüglich Cybersicherheit zu einem erheblichen Vertrauenszuwachs. Standards und Zertifizierungen bieten die Grundlage für die Bewertung der Qualität digitaler Produkte und Dienste und müssen immer auch Kriterien für IT-Sicherheitsmechanismen enthalten.

Das Aufdecken, Melden und Schliessen von Sicherheitslücken in digitalen Produkten und Diensten ist eine der zentralen Aufgaben im Bereich IT-Sicherheit. Der Staat sollte entsprechende Aktivitäten fördern und verbindliche Richtlinien für den Prozess der Offenlegung von Schwachstellen definieren.

Dringend werden aktuell Bildungs- und Weiterbildungsangebote für Cybersicherheit benötigt, die Fachkräfte schnell und bedarfsspezifisch in der Thematik qualifizieren. Diese müssen breit angelegte Programme für verschiedene Empfängergruppen sein, die zudem einen möglichst hohen Praxisbezug haben, damit das Gelernte unmittelbar in der Arbeitsumgebung angewendet werden kann. Für Lehrkräfte müssen verstärkt Angebote geschaffen werden, sich im Bereich Informationstechnologie, Digitalisierung und Cybersicherheit weiterbilden zu können, ohne dass diese Weiterbildungen eine Zusatzbelastung für sie bedeutet. Neben der Schule gewinnen zunehmend ausserschulische Lernräume für Schülerinnen und Schüler an Bedeutung. Entsprechende Angebote gilt es flächendeckend auszubauen.

Anmerkungen

1 Vgl. https://www.heise.de/newsticker/meldung/Saudi-Arabien-Cyberangriff-haette-Explosion-ausloesen-koennen-Ermittler-sind-alarmiert-3996010.html.
2 Vgl. https://www.heise.de/security/meldung/Zer tifikate-fuer-beliebige-Domain-Forscher-demo nstrieren-kritisches-DNS-Problem-4156868.html.
3 Vgl. https://www.sit.fraunhofer.de/de/vusc/.
4 Vgl. https://www.sit.fraunhofer.de/de/presse/details/news-article/show/gefahr-uebers-telefon/.
5 Vgl. https://www.idc.com/getdoc.jsp?containerId=prUS45213219.
6 Vgl. https://news.sap.com/germany/2019/10/iot-chance-moeglichkeiten/.
7 Vgl. https://www.securityweek.com/how-cybercriminals-are-using-blockchain-their-advantage.

Referenzen

Bitkom. (2019). Wirtschaftsschutz in der digitalen Welt. Abgerufen von: https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019_0.pdf.

Committee for Information, Computers and Communications Policy. (1997). Global Information Infrastructure – Global Information Society (GII-GIS): Policy Recommendations for Action.

Forbes. (2018). Seven Ways Cybercriminals Can Use Machine Learning. Abgerufen von: https://www.forbes.com/sites/forbestechcouncil/2018/01/11/seven-ways-cybercriminals-can-use-machine-learning/?sh=1cff084b1447.

Fraunhofer SIT. (2019). Appicaptor Security Index 9/2019. Abgerufen von: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Appicaptor-Security-Index-2019_FraunhoferSIT.pdf.

Glanz, L., Müller, P., Baumgärtner, L., Reif, P., Amann, S., Anthonysamy, P., und Mezini, M. (2020). Hidden in Plain Sight: Obfuscated Strings Threatening Your Privacy. Proceedings of the 15th ACM Asia Conference on Computer and Communications. Abgerufen von: https://dl.acm.org/doi/ 10.1145/3320269.3384745.

Kraft, R., und Stöwer, M. (2017). IT-Risikomanagement im Produktionsumfeld – Herausforderungen und Lösungsansätze. HMD Praxis der Wirtschaftsinformatik, 54, 84–96.

Handelsblatt. (2020). Todesfall nach Hackerangriff auf Uni-Klinik Düsseldorf. Abgerufen von: https://www.handelsblatt.com/technik/sicherheit-im-netz/cyberkriminalitaet-todesfall-nach-hackerangriff-auf-uni-klinik-duesseldorf/26198688.html.

Rotenberg, N., Shulman, H., Waidner, M., und Zeltser, B. (2017). Authentication-bypass Vulnerabilities in SOHO Routers. In Proceedings of the SIGCOMM Posters and Demos (pp. 68–70).

Süddeutsche Zeitung. (2016). Bundesamt geht von Hackerangriff auf ukrainisches Stromnetz aus. Abgerufen von: https://www.sueddeutsche.de/digital/ukraine-bundesamt-geht-von-hackerangriff-auf-ukrainisches-stromnetz-aus-1.2830197.

Süddeutsche Zeitung. (2019). Deutschland ist ein attraktives Ziel für Cyberkriminelle. Abgerufen von: https://www.sueddeutsche.de/digital/cyberkriminalitaet-internet-kriminalitaet-deutschland-1.4677158.

Waidner, M., Backes, M., und Müller-Quade, J. (2017). Positionspapier: Cybersicherheit in Deutschland. Fraunhofer Verlag.