Cyberattacken auf kritische Infrastrukturen

IT-Krisenmanagement kontinuierlich in der Praxis optimieren

Die Zahl kriminell motivierter Cyberattacken auf die kritische Infrastruktur ist auf einem Rekordhoch. Ursache dafür ist nicht nur die zunehmende Digitalisierung in der Gesellschaft, sondern auch die immer stärkere Professionalisierung der Angreifergruppen. Unternehmen der Kommunal-, Energie- und Wasserwirtschaft sind gut beraten, IT-Sicherheit als kontinuierlichen Verbesserungsprozess zu verstehen, ganzheitliche Cybersecurity-Strategien zu entwickeln und das eigene IT-Krisenmanagement immer wieder selbstkritisch zu hinterfragen.

Schwelbrände gehören zu den heimtückischsten ihrer Art. Sie können jederzeit als offenes Feuer auflodern und sich schlimmstenfalls zum Flächenbrand ausweiten. Wenn immer neue Glutnester unkontrolliert aufflammen, bringt das selbst die erfahrensten Feuerwehrteams schnell an die Grenze der Belastbarkeit.

Ähnlich »angespannt bis kritisch« beschreibt der im Oktober 2021 vom Bundesamt für Sicherheit in der Informationstechnik (BSI) vorgestellte »Bericht zur Lage der IT-Sicherheit in Deutschland« die Bedrohung durch Cyberkriminelle für die digitale Gesellschaft und die vernetzte Arbeitswelt. Die Zahlen sprechen dabei für sich: Allein gegenüber dem Jahr 2020 stieg die Zahl neuer Schadprogrammvarianten um 22 % auf 144 Mio. Mit täglich bis zu 553 000 neuen Varianten ist das der höchste jemals gemessene Wert je Tag.

Der Bitkom e. V. geht davon aus, dass der deutschen Wirtschaft durch Diebstahl, Spionage und Sabotage jährlich ein Gesamtschaden von 223 Mrd. € entsteht – das Doppelte der Schadenssumme von 2018/2019. Insgesamt 88 %, also neun von zehn Unternehmen, waren 2020/2021 von Cyberattacken betroffen. Zunehmend nutzen die Angreifer Ransomware auch für neue Formen der Cybererpressung und drohen ihren Opfern nicht nur mit der Vernichtung beziehungsweise Verschlüsselung, sondern auch mit der Veröffentlichung und missbräuchlichen Nutzung von Identitätsdaten. Nicht selten wird die Höhe des Lösegelds dabei individuell an Unternehmensgröße und -bedeutung (zum Beispiel im Rahmen kritischer Infrastrukturen) festgemacht – ein Phänomen, das gemeinhin als »Big Game Hunting« (Großwildjagd) bezeichnet wird. Stéphane Nappo, Vice President und CISO der Groupe SEB, bringt es auf den Punkt: »Es dauert 20 Jahre, um einen guten Ruf aufzubauen, und nur ein paar Minuten eines Cybervorfalls, um ihn zu ruinieren.«

Vor dem Hintergrund des »ersten digitalen Katastrophenfalls» stellte Sascha Lobo im Juli 2021 seine Kolumne im Spiegel unter die ebenso prägnante wie provokative Überschrift »Die nächste Pandemie wird digital: Der Landkreis Anhalt-Bitterfeld ist nach einem Hackerangriff handlungsunfähig. Deutschland ist auf so etwas miserabel vorbereitet: Die öffentliche IT-Infrastruktur wurde kaputtgespart, ein digitales Mindset fehlt.«

Leider ist Anhalt-Bitterfeld kein Einzelfall. Allein in Mecklenburg-Vorpommern stieg nach Angaben des LKA die Zahl der Vergehen, die sich gegen Internet, Datennetze und informationstechnische Systeme richten, um fast 10 % gegenüber dem Vorjahr. Zu den prominenten Opfern gezielter Cyberattacken gehörten im Jahr 2021 nicht nur große Konzerne wie Aida Cruises – Deutschlands größte Kreuzfahrtreederei –, sondern auch kommunale Energieversorger wie die Stadtwerke Wismar sowie Verwaltungsbehörden und -institutionen wie die Landeshauptstadt Schwerin und der Landkreis Ludwigslust-Parchim.

Längst geht es nicht mehr darum, ob ein Cyberangriff auf die eigene IT-Infrastruktur stattfinden wird. Es geht vielmehr darum, wann dies passiert und wie schnell dieser erkannt und erfolgreich abgewehrt werden kann.

Zunehmende Digitalisierung und Professionalisierung der Tätergruppen

Dass nahezu alle Branchen zunehmend von Cyberkriminalität betroffen sind, hat grundsätzlich zwei Ursachen: die immer stärkere Digitalisierung in der Gesell-

schaft (mit Einfallstoren wie Remote Working, Smart Home und Smart Governance) sowie die steigende Professionalisierung der Tätergruppen – bis hin zu einer ausgeklügelten Arbeitsteilung und »Industrialisierung« in weltweit agierenden kriminellen Netzwerken, die es den Ermittlungsbehörden zunehmend erschweren, personell und technologisch hinterherzukommen. Die Cyberkriminalität hat sich zu einem lukrativen Geschäftsmodell entwickelt, das gerade in Entwicklungs- und Schwellenländern topausgebildete IT-Spezialisten auf die dunkle Seite der Macht zieht.

Hinzu kommt auf internationaler Ebene ein weiterer gefährlicher Trend: Zwischen- und innerstaatliche Konflikte werden zunehmend auch auf den Schlachtfeldern des Cyberspace ausgetragen, wobei die Grenzen zwischen privaten und staatlichen Hackergruppen immer weiter verschwimmen. Das Spektrum hybrider Kriegsführung und staatlich gesteuerter Cyberangriffe reicht dabei von klassischer Spionage bis hin zu Sabotage und gezielter Aushöhlung demokratischer Strukturen durch Lieferengpässe, Desinformation, Aufstachelung und Verunsicherung einzelner Bevölkerungsgruppen.

Kontinuierliches IT-Sicherheitsmanagement verhindert Flächenbrand

Dass sich die kritischen Infrastrukturen als Rückgrat der Gesellschaft hier als besonders vulnerabel erweisen, liegt auf der Hand. Realistisch betrachtet, stellen Angriffe auf einzelne Anlagen jedoch noch keine ernst zu nehmende Bedrohung für das Gemeinwohl dar. Erst wenn großflächig strukturelle Sicherheitslücken ausgenutzt werden, die Reaktionsfähigkeit der Systeme nicht mehr gewährleistet ist oder wie kürzlich im Fall von Log4j zu viele Softwarekomponenten angegriffen werden, brennt es buchstäblich.

Wird die Kommunal-, Energie- und Wasserwirtschaft als Ganzes betrachtet, bietet sich ein durchaus heterogenes Bild. Nur wenige, vorwiegend kleinere Strukturen, verlassen sich auch heute noch mit vorhandener Alttechnik und einem von verschiedenen Abteilungen gehäkelten Flickenteppich darauf, dass ein Cyberangriff sie schon nicht treffen werde. Die Mehrzahl ist bereits stark sensibilisiert für die unterschiedlichen Facetten der Cyberkriminalität und entsprechend gut aufgestellt – sowohl personell als auch technologisch. Jede erfolgreich getroffene Maßnahme bildet hier für sich genommen im Optimalfall ein eigenes Schutzniveau. Erst wenn die Angreifer mehrere dieser Schutzwälle durchbrechen können, ist der Tipping Point (Wendepunkt) erreicht, der ein kleines, noch beherrschbares Feuer in einen unkontrollierbaren, nicht mehr zu löschenden Großbrand verwandelt.

Gefahr durch gezielte Software-Supply-Chain-Angriffe

Ein IT-Sicherheitssystem ist nur so stark wie das am wenigsten abgesicherte Glied der Lieferkette. Kriminelle Hacker gehen dabei immer öfter die »Extrameile« über IT-Dienstleister – zum Beispiel Beratungshäuser und Softwareanbieter wie im Jahr 2021 Kisters oder SolarWinds. Mit Colonial Pipelines wurde im Jahr 2021 sogar die Betreiberfirma des größten Öl-Pipelinesystems in den USA erpresst, was wiederum erhebliche Auswirkungen auf die Öl- und Benzinlieferketten an der amerikanischen Ostküste hatte.

Systematisch werden durch Ransomware-Angriffe so viel Informationen wie möglich gesammelt – zum Beispiel mit online verfügbaren Demosystemen oder Testanwendungen. Diese Methode ist besonders perfide, da sie das langjährig aufgebaute Vertrauensverhältnis zu den eigenen Servicepartnern zerstört und bewusst zu kriminellen Zwecken ausnutzt. Solche Software-Supply-Chain-Angriffe werden im Jahr 2022 noch zunehmen, da spezialisierte Bedrohungsakteure in der Lage sein werden, ganze Softwareentwicklungspipelines zu infiltrieren und ihr kriminelles Know-how nach dem Vorbild des Ransomware-as-a-Service-Modells weiterzuverkaufen.

Und leider wird 2022 weltweit neben Fragen der Sicherheit in der Cloud (Stich-

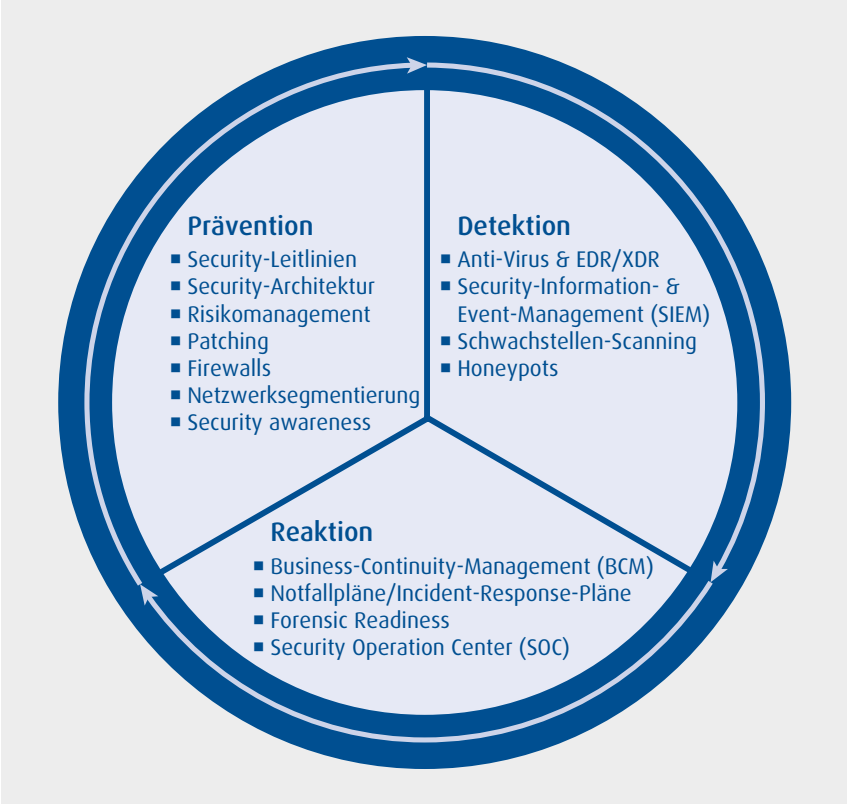

Bild 1. IT-Sicherheit als kontinuierlicher Verbesserungsprozess

wort: Management von Maschinenidentitäten) auch eine mögliche Manipulation der IoT-Infrastruktur in modernen Smart-Home- und Smart-City-Umgebungen ein Thema sein. Beispiele sind der Diebstahl von Geräteidentitäten und die Übernahme von Messgeräten, Kameras oder Monitoren zu kriminellen Zwecken.

Umso wichtiger ist daher ein effektives IT-Asset-Management (IAM) für mehr Sicherheit, Transparenz und Produktivität. Es gewährleistet, dass jedes Asset von Wert über seinen gesamten Lebenszyklus hinweg sorgfältig dokumentiert, bereitgestellt, gewartet, aktualisiert und bei Bedarf stillgelegt werden kann. So haben zum Beispiel Windenergieanlagen mit 10 bis 15 Jahren eine deutlich höhere Lebensdauer als die zugrunde liegenden Betriebssysteme, die bereits nach 8 bis 10 Jahren ihr End of Life erreichen. Diese Diskrepanz birgt gefährliche Sicherheitslücken in sich, die zunehmend auch den Gesetzgeber auf den Plan rufen werden.

Ein IT-Asset-Management ist eine wichtige Grundlage, wenn besser bewertet werden soll, welche Komponenten im Einsatz sind, welchen Sicherheitsstand diese haben und wann diese gegebenenfalls durch neue Komponenten abgelöst werden müssen.

Ganzheitliche Sichtweise: IT-Sicherheit ist Chefsache

Was also kann noch getan werden? Fakt ist: IT-Sicherheit sollte ganzheitlich betrachtet werden und grundsätzlich Chefsache sein. Doch was, wenn sich gerade kleinere Unternehmen den »Luxus« einer einheitlichen, konsolidierten IT- und IT-Sicherheitsstrategie nicht leisten können? Immerhin vermissen laut einer europaweiten Umfrage von Forrester Research vom Februar 2020 sechs von 10 IT-Entscheidern (57 %) eine durchgängige End-to-End-Sicherheit ihres Netzwerks. Hier hat es sich in der Praxis bewährt, analog zum Datenschutz und unter klarer Definition der Verantwortlichkeiten, einen externen IT-Informationssicherheitsbeauftragten (ISB) hinzuzuziehen – und das nicht erst im Rahmen einer geplanten Zertifizierung gemäß ISO 27001 und IT-Grundschutz. Auch lassen sich häufig mit anderen Unternehmen Synergien in der Zusammenarbeit nutzen, zum Beispiel durch den Aufbau gemeinsamer IT-Sicherheitsstrukturen. Das reduziert eigene Personal-, Anschaffungs- und Administrationskosten.

Der Umgang mit Log4j hat gezeigt, wie wichtig es ist, die zu schützenden Bereiche und die dazugehörigen Verantwortlichkeiten unmissverständlich vorab zu definieren und deren Umsetzung systematisch zu kontrollieren. Während viele Unternehmen durchaus vorbildlich im Bereich der Prävention dastehen (zum Beispiel Firewalls, Antivirusprogramme), wird nicht selten der mindestens ebenso wichtige Bereich der Reaktion sträflich vernachlässigt.

Ein krisensicheres Business-Continuity-Management ist daher dringend erforderlich, damit der reguläre Betrieb nach störungsbedingter Unterbrechung in kürzestmöglicher Zeit wieder aufgenommen werden kann. So lassen sich Schäden reduzieren und existenzielle Bedrohungen vermeiden, die zum Beispiel durch unterbrochene Lieferketten schnell auch für weitere Unternehmen zu einem Flächenbrand werden können.

Häufig wird es kriminellen Hackern zu leicht gemacht. So fehlt es nicht selten

immer noch zum Beispiel an einem professionellen Release-, Patch-, Berechtigungs- und Identitätsmanagement, an sicheren Passwörtern oder einer konsequenten Trennung privater und beruflicher Mailaccounts beziehungsweise der kaufmännischen und technischen Systeme.

IT-Krisenmanagement kontinuierlich in der Praxis optimieren

Im Zusammenhang mit der Pandemie wird oft von der Erstellung geeigneter Notfall- und Katastrophenpläne gesprochen. Meist signalisieren kommunale Unternehmen, Wasser- und Energieversorger dann, dass sie diese schon lange in der Schublade haben. Unternehmen der kritischen Infrastruktur sind allerdings gut beraten, ihre Krisenmanagementplanung nicht nur als schriftliche Dokumentation vorzuhalten, sondern diese kontinuierlich praxisnah zu erproben und mögliche Schwachstellen systematisch auszubessern. Auch hier ist eine ganzheitliche Herangehensweise gefragt, da die Gesamtsicht zum Beispiel auch Aspekte der internen und externen Kommunikation umfasst (bei der Information der Mitarbeiter, bei juristischen Bewertungen, bei der Beantwortung von Ad-hoc-Presseanfragen oder im Umgang mit Aufsichtsbehörden, Polizei und weiteren Stakeholdern). Es ist sinnvoll, diverse Krisenszenarien im Vorfeld ehrlich durchzuspielen und entsprechend abzusichern.

Wieder einmal macht der Faktor Mensch hier den Unterschied. Kontinuierlich up to date zu bleiben und für Sicherheitslücken sensibilisiert zu sein, ist daher auch, aber nicht nur, Aufgabe gezielter Awareness-Trainings. Dabei kommt die Bedrohung nicht immer nur von externen Angreifern. Durch eine sorgfältige Personalauswahl, eine offene, wertschätzende Unternehmenskultur und die gezielte Nutzung effektiver Security-Information- und Event-Management-Systeme (SIEM) kann maliziösem Verhalten Einzelner erfolgreich entgegengesteuert werden.

IT-Sicherheit ist ein kontinuierlicher Prozess, der regelmäßig ehrlich auf den Prüfstand gestellt werden sollte. Laut Stéphane Nappo sind die fünf effektivsten Cyber Defender:

- Anticipation
- Education
- Detection
- Reaction
- Resilience.

Die Oetker Daten- und Informationsverarbeitung KG (OEDIV) unterstützt ihre Kunden auf der gesamten Bandbreite der Cybersecurity und entwickelt gemeinsam mit ihnen ganzheitliche IT-Strategien und IT-Sicherheitsstrategien.

Tim Philipp Schäfers,
Information Governance (ING), Cyber Security Consultant,
OEDIV Oetker Daten- und Informationsverarbeitung KG, Bielefeld

Dr. **Anke Schäfer**,
Dr. Schäfer PR- und Strategieberatung, Rostock

>> info@secusys.de
>> www.oediv.de