Markus Schneider, Thomas Dexheimer, Elias Heftrig, Sinisa Dukanovic

Cybertraining auf einer Cyber Range

Eine Pflichtaufgabe für Organisationen

Wenn Organisationen heute Opfer eines Cyberangriffs werden, bemerken sie dies meist erst, wenn es zu spät ist – nämlich an den Auswirkungen: Die Angreifer haben ihr Ziel erreicht und die Opfer erhalten Lösegeldforderungen. Da Cyberangriffe üblicherweise über längere Zeit in mehreren aufeinander aufbauenden Schritten ablaufen, könnte man sie auch früher entdecken und abwehren. Hierfür benötigen die für die operative Cybersicherheit Verantwortlichen Wissen und Erfahrung. Dazu dienen Cybertrainings auf einer Cyber Range.

Dr.-Ing. Markus Schneider

ist stv. Institutsleiter und Leiter Cybertraining & Weiterbildung bei Fraunhofer SIT & Nationales Forschungszentrum für Angewandte Cybersicherheit ATHENE
E-Mail:
markus.schneider@sit.fraunhofer.de

Dipl.-Inform. Thomas Dexheimer

ist Trainer der ATHENE Cyber Range am Fraunhofer SIT & Nationales Forschungszentrum für Angewandte Cybersicherheit ATHENE

E-Mail:
thomas.dexheimer@sit.fraunhofer.de

M.Sc. Elias Heftrig

ist Trainer der ATHENE Cyber Range am Fraunhofer SIT & Nationales Forschungszentrum für Angewandte Cybersicherheit ATHENE

E-Mail: elias.heftrig@sit.fraunhofer.de

Dipl.-Inform. Sinisa Dukanovic

ist Trainer der ATHENE Cyber Range am Fraunhofer SIT & Nationales Forschungszentrum für Angewandte Cybersicherheit ATHENE

E-Mail:
sinisa.dukanovic@sit.fraunhofer.de

1 Einleitung

Cybersicherheit stellt Organisationen, wie Unternehmen oder Behörden, vor große Herausforderungen. Die hohe Zahl an erfolgreichen Angriffen belegt, dass technische Schutzmaßnahmen zwar wichtig sind, dass sie jedoch für einen effektiven Schutz nicht genügen. Technik ist in der Praxis nie perfekt, z. B. wegen Fehlern in der Implementierung oder Konfiguration von Software oder bei der Bedienung. Die organisierte Cyberkriminalität nutzt dies insbesondere für Ransomwareangriffe aus – mit erheblichem Schaden für Opfer, etwa durch Ausfall von IT-Systemen und Unterbrechungen betrieblicher Abläufe oder durch Veröffentlichung von vertraulichen Unternehmensdaten, Lösegeldforderungen, Einnahmeverlusten und Reputationsschäden. Angesichts der Bedrohungslage und des Ökosystems der Angreifer stellt sich Organisationen heute nicht die mehr Frage, ob sie angegriffen werden, sondern eher wann dies geschieht und wie sie den Schaden möglichst klein halten können.

Wenn man davon ausgehen muss, dass es keinen perfekten Schutz gibt und IT-Infrastrukturen angreifbar sind, dann geht es für Organisationen darum, dass die für die operative Sicherheit Verantwortlichen die Angriffe entdecken und sie rechtzeitig vereiteln können, bevor Angreifer ihr Ziel erreicht haben. Mit diesen Personen sind hier nicht durchschnittliche Anwender, sondern Akteure mit ausgeprägten technischen Kompetenzen wie in der IT-Administration oder in einem Security Operation Center gemeint. Reale Angriffe bestehen üblicherweise aus einer Folge einzelner Schritte, entlang derer sich die Angreifer zu ihren Angriffszielen vorarbeiten. Ziel ist, dass Opfer an den Spuren und Auffälligkeiten einzelner Schritte einen sich anbahnenden Angriff möglichst früh erkennen. Hierfür benötigen diese Personen Cybertrainings, also Situationen, in denen sie alleine oder mit anderen Personen aus ihrer Abteilung lernen, realistische Cyberangriffe im operativen Betrieb zu entdecken und abzuwehren.

Da man Cybertrainings wegen der Risiken durch Kollateralschäden nicht in der Produktivumgebung der jeweiligen Organisation durchführen kann, braucht man dafür eine spezielle Trainingsumgebung: eine Cyber Range. Ohne Cyber Range können die sicherheitsverantwortlichen Personen die Erkennung und Abwehr von Cyberangriffen praktisch nicht trainieren. Solche prak-

tischen Übungen sind jedoch für den Schutz unerlässlich. So sei hier auf die Übung von Reaktionen in kritischen Situationen in anderen Bereichen verwiesen, wie etwa Übungen auf Flugsimulatoren in der Luftfahrt oder Feuerlöschübungen. Dort hat man erkannt, dass rein theoretisches Wissen ohne praktische Erfahrung für die Bewältigung kritischer Situationen nicht genügt, insbesondere wenn auch Stress als weiterer belastender Faktor hinzukommt.

Angesichts der beschriebenen Ausgangslage und rechtlicher Anforderungen wird in diesem Beitrag die Auffassung vertreten, dass Cybertrainings aus mehreren Gründen, wie etwa zur Sorgfalt und zur Risikovorsorge, für Organisationen verpflichtend sind. Hinzu kommen Verpflichtungen aus weiteren spezifischen Rechtsakten, z. B. für kritische Infrastrukturen.

2 Ausgangssituation

2.1 Risiken und Kosten durch Cyberangriffe

Das Versicherungsunternehmen Allianz hat Cyberangriffe im Jahr 2025 erneut zum weltweit größten Geschäftsrisiko für Unternehmen erklärt.[1] Die Schäden für die deutsche Wirtschaft durch Cybercrime lagen gemäß dem Digitalverband Bitkom im Jahr 2024 bei 178,6 Mrd. Euro.[2] Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) bewertete die Lage der IT-Sicherheit in Deutschland im Jahr 2024 wiederholt als sehr angespannt.[3] Gemäß einer Studie von IBM sind die Durchschnittskosten für einen Cyberangriff im Jahr 2024 im Vergleich zum Vorjahr weltweit um 10% auf 4,88 Millionen US-Dollar gestiegen. Die durchschnittlichen Kosten je Cyberangriff liegen in Deutschland im Vergleich dazu bei 5,31 Millionen US-Dollar, ein Anstieg um 13,7%. Bei den durchschnittlichen Kosten je Cyberangriff steht Deutschland weltweit an vierter Stelle.[4]

Die Kosten eines Cyberangriffs setzen sich aus unterschiedlichen Komponenten zusammen, wie etwa den Kosten aus entgangenem Geschäft, zusätzlichen Kosten für investigative Maßnahmen und die Kommunikation nach Innen und Außen, und die Kosten für die technischen Maßnahmen zur Wiederherstellung. Hinzu kommen noch Kosten, die schwierig zu erfassen sind, wie etwa die negativen Effekte für Reputation und Schwierigkeiten bei der Akquise von Neukunden. Auch Schäden aus abgeflossenen Unternehmensdaten sind schwierig zu beziffern. Dies gilt beispielsweise für Dokumente, die nach Angriffen zu Wettbewerbern gelangen (z. B. Strategiedokumente, Erfindungen für Patentanmeldungen), wodurch Wettbewerbsvorteile verloren gehen können.

2.2 Angriffe und das Ökosystem der Cyberkriminalität

Cyberangriffe werden immer mehr zum Massengeschäft, insbesondere Ransomwareangriffe. Laut BSI haben diese Angriffe im Jahr 2024 weiter stark zugenommen.[5] Je schlechter Organisationen auf den Umgang mit Cyberangriffen vorbereitet sind, desto eher sind Angriffsversuche erfolgreich.

Die am weitesten verbreiteten Varianten dieser Angriffe bestehen darin, dass der Zugang zu Daten und IT-Infrastruktur bis zur Zahlung eines Lösegeldes unterbunden wird, z. B. durch Verschlüsselung der Daten, oder Verbreitung vertraulicher Geschäftsdaten bei ausbleibender Lösegeldzahlung, z. B. durch Veröffentlichung im Internet. Es besteht jedoch keine Garantie, dass Angreifer nach der Lösegeldzahlung ihre Drohung nicht dennoch umsetzen.

Für Angriffe werden oft Schwachstellen in IT-Produkten ausgenutzt, die noch nicht geschlossen sind, oder sogenannte „Zero Day Exploits", für welche noch keine Patches zur Verfügung stehen. Dies ist keine Seltenheit. Laut BSI wurden im Jahr 2023 durchschnittlich 78 solcher Schwachstellen pro Tag bekannt.[6] Die Ausnutzung erbeuteter Zugangsdaten ist ein anderer Weg.

Es ist auch festzustellen, dass Angreifer häufig IT-Dienstleister ins Visier nehmen. Über diese können sie Zugang zu den IT-Infrastrukturen und Daten von deren Kunden bekommen und somit einen Multiplikatoreffekt erzielen. IT-Dienstleister können auf den Systemen ihrer Kunden mit besonderen Rechten agieren, z. B. mit Administrator-Rechten.

Es wurde auch festgestellt, dass Angreifer die Funktion von Programmen zur Angriffsdetektion (z. B. Endpoint Detection & Response) in den angegriffenen IT-Infrastrukturen deaktivieren, sodass Angriffe ungestört fortgesetzt werden können.[7] Deshalb ist es nicht hinreichend, sich auf die Alarme von Detektionssystemen allein zu verlassen, sondern es bedarf auch gut ausgebildeter Personen, die Angriffe entdecken können. Es besteht ebenso ein Trend, dass Angreifer auf den angegriffenen IT-Systemen immer wieder vorhandene Standardwerkzeuge (z. B. Komponenten von Betriebssystemen) für ihre Angriffe trickreich einsetzen, da deren Nutzung von Detektionssystemen nicht als Angriff klassifiziert wird.[8]

Angreifer haben sich in den vergangenen Jahren stark professionalisiert und im internationalen Rahmen ein eigenes Ökosystem ausgebildet. Im Darknet hat sich inzwischen eine regelrechte Schattenwirtschaft für kriminelle Leistungen zur Durchführung von Cyberangriffen entwickelt, die ein Massengeschäft umfasst. So gibt es beispielsweise Angebote zur Miete von Angriffswerkzeugen; in diesem Zusammenhang spricht man bereits von „Ransomware as a Service (RaaS)" oder „Cybercrime as a Service (CCaaS)".[9]

1 Allianz: Allianz Risk Barometer - Identifying the major business risks for 2025. Januar 2025, https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2025.pdf

2 Bitkom: Wirtschaftsschutz 2024. https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf

3 BSI: Die Lage der IT-Sicherheit in Deutschland 2024. 2024, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html

4 IBM: Cost of Data Breach Report 2024. https://www.ibm.com/de-de/reports/data-breach

5 BSI: Die Lage der IT-Sicherheit in Deutschland 2024. 2024, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html

6 BSI: Die Lage der IT-Sicherheit in Deutschland 2024. 2024, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html

7 MITRE: Endpoint Denial of Service. 2025, https://attack.mitre.org/techniques/T1499/, https://attack.mitre.org/

8 Check Point: Cyber Security Report 2023. https://www.checkpoint.com/resources/report-4fd2/report-cyber-security-report-2023

9 Martin Dukek: Ransomware-as-a-Service. DuD 3/2024, S. 153-157.

2.3 Reaktionszeiten bei Cyberangriffen

Wenn Organisationen angegriffen wurden, dann sichern IT-Forensiker üblicherweise die Angriffsspuren und werten diese aus. Anhand dieser Daten kann man dann einzelne Angriffsschritte rekonstruieren und sehen, wie lange Angreifer bereits in die IT-Infrastruktur von Organisationen eingedrungen sind und welche Schritte sie in Richtung ihres Ziels unternommen haben. Gemäß einer Studie von IBM war die durchschnittliche Zeit zur Erkennung eines Angriffs im Jahr 2024 mit 194 Tagen sehr hoch; in den Jahren zuvor war sie ähnlich hoch.[10] Für die Behebung eines Angriffs wurden im vergangenen Jahr durchschnittlich noch zusätzliche 64 Tagen benötigt.

Laut der Studie von IBM führen betroffene Organisationen die langen Reaktionszeiten auf eine bestehende personelle Unterbesetzung und Qualifikationsdefizite zurück. Es ist naheliegend, dass Defizite zu längeren Reaktionszeiten führen. Solche Defizite führen auch dazu, dass die Aufgaben nicht effizient erfüllt werden können, wodurch die Wahrnehmung einer Unterbesetzung nochmal verstärkt wird.

Die Charakteristiken von Reaktionszeiten in Abhängigkeit von Variablen, auf welche Organisationen direkten Einfluss nehmen können, wurden bisher unseres Wissens nach nicht umfassend untersucht. Es sind lediglich ältere Untersuchungen bekannt, bei welchen Abhängigkeiten zwischen Reaktionszeit einerseits und Angriffsmethode bzw. Angriffszielen andererseits bestehen.[11] Allerdings basieren diese Untersuchungen auf Daten aus den Jahren 2010–2017, für die in vielerlei Hinsicht andere Rahmenbedingungen galten.

2.4 Bedarf zur Stärkung des Personals

Die in Organisationen für die operative Cybersicherheit Verantwortlichen sollten in besserer Weise dazu befähigt werden, sich adäquat für die Ziele ihrer Organisation einzusetzen. Hierfür ist es notwendig, dass sie Hinweise auf Cyberangriffe möglichst früh erkennen und Maßnahmen zum Schutz ergreifen, um Risiken und Schäden für ihre Organisation zu verringern. Dazu tragen Cybertrainings bei.

Diese Fähigkeiten umfassen sowohl Inhalte als auch Aspekte zur Stärkung der Prozessetablierung in Organisationen zur effektiven und effizienteren Behandlung von Vorfällen. Inhaltlich geht es bei den Trainings darum, die Erkennung und Verteidigung verschiedener Angriffe und den Umgang mit Werkzeugen zu üben. Beispielsweise sind in Abhängigkeit von den eingesetzten Techniken unterschiedliche Typen von Angriffen maßgeblich. Mit der Verwendung neuer Techniken ist davon auszugehen, dass weitere Angriffsarten oder -vektoren relevant werden. Hinzu kommt, dass Angreifer agil arbeiten und immer wieder neue Typen von Angriffen entwickeln; in deren Ökosystem verbreiten sich Werkzeuge und Wissen rasant. Darüber hinaus werden auch Werkzeuge auf der Verteidigerseite weiterentwickelt, deren adäquater Einsatz für jeweilige Angriffe trainiert werden muss. Für den Ernstfall ist es wichtig, dass in Organisationen aktuelles Wissen und Erfahrung mit dem praktischen Einsatz vorliegen.

Cybertrainings bereiten das Personal auf Notfallprozesse und deren praktische Umsetzung vor. Wenn es in Trainingssituationen mit echten Cyberangriffen konfrontiert wird, lernt es, Prozessabläufe für die Angriffserkennung und Verteidigung einzuüben, um dann später unter Stress die richtigen Entscheidungen treffen zu können. Werden Trainings in Gruppen durchgeführt, lernen die Teilnehmenden darüber hinaus, wie sie mit anderen Personen aus ihrer Organisation möglichst effektiv und effizient zusammenarbeiten können, indem sie gemeinsam dieselbe Verteidigungsstrategie befolgen. Solche Fähigkeiten und Routinen kann man durch praktische Trainings ausbilden, in denen Trainingsinhalte und Trainingsablauf den Ernstfall möglichst realistisch darstellen.

Cybertrainings sind für alle Personen relevant, die operativ in Organisationen zur Cybersicherheit beitragen. Das ist unabhängig davon, welche Strukturen eine Organisation hierfür eingerichtet hat und wie tiefgehend die Fachkenntnisse der Personen sind, z. B. aus der IT-Administration oder einem Security Operation Center. Die Trainingsziele bestehen darin, die Teilnehmer zu befähigen und dabei zu unterstützen, dass sie kritische Schäden für ihre Organisation vermeiden können. Für die Verteidigung geht es darum, dass bei irgendeinem Angriffsschritt Hinweise oder Spuren wahrgenommen werden, damit Maßnahmen zur Analyse und ggf. zur Abwehr eingeleitet werden können. Ob diese weiteren Maßnahmen dann organisationsintern oder unter Einbeziehung externer Spezialisten durchgeführt werden, ist für das übergeordnete Organisationsziel der Vermeidung kritischer Schäden nachrangig.

Die Zielsetzung praktischer Cybertrainings zeigt deutlich, dass diese sich von üblichen Awareness-Trainings unterscheiden, die sich hauptsächlich an durchschnittliche Benutzer von Anwendungssoftware richten und deren Wirksamkeit gelegentlich bezweifelt wird.[12] Synergien zwischen *Business Continuity Management* (BCM) und *Information Security Management* (ISM), dem Cybertrainings als eine mögliche Maßnahme zugeordnet werden, sind bekannt.[13] Andere Arbeiten setzen die technische oder digitale Resilienz in den Zusammenhang mit psychischer Resilienz von Mitarbeitenden im Zusammenhang mit Belastungs- und Gesundheitsfragen am Arbeitsplatz.[14] Da die hier behandelten Cybertrainings Personen für Ernstfälle vorbereiten, ist davon auszugehen, dass Cybertrainings positive Auswirkungen bei psychischen Belastungen am Arbeitsplatz haben. Zur Stärkung der Abwehrfähigkeiten steht auch Red Teaming zur Diskussion.[15] Aufgrund der zu befürchtenden Kollateralschäden scheinen Cybertrainings mit Cyber Ranges jedoch besser geeignet.

10 IBM: Cost of Data Breach Report 2024. https://www.ibm.com/de-de/reports/data-breach

11 Yaman Roumani: Detection time of data breaches. Computers & Security, Volume 112, January 2022

12 Martin Brehmer, Vanessa Steinherr, Raphaela Stöckl: Toward A Higher Resilience Against Cyberattacks. Datenschutz und Datensicherheit (DuD) 1/2024

13 Lucas Daus, Philipp Przybylski: Business Continuity Management und Informationssicherheit. Datenschutz und Datensicherheit (DuD) 7/2023

14 Anja S. Göritz, Robin Bührle, Jefrey Wimmer: Möglichkeiten und Grenzen digitaler Resilienztrainings. Datenschutz und Datensicherheit (DuD) 6/2024

15 Fabian M. Teichmann, Sonia R. Boticiu: An overview of the benefits, challenges, and legal aspects of penetration testing and red teaming. International Cybersecurity Law Review (2023) 4

3 Cyber Ranges

3.1 Was ist eine Cyber Range?

Eine Cyber Range ist eine interaktive Plattform, die Netzwerke, Systeme, Werkzeuge und Softwareanwendungen in einer virtuellen Umgebung simuliert. Diese kann für verschiedene Zwecke genutzt werden, wie etwa zum Lernen und Trainieren, auch zum gemeinsamen Trainieren, aber auch zur Überprüfung des Leistungsstands von Personen und Teams.[16] Insbesondere kann man auf einer Cyber Range als simulierte und abgeschottete Umgebung zu Trainingszwecken echte Angriffe durchführen, welche die Teilnehmer genauso wie in einem Produktivsystem wahrnehmen.[17],[18],[19] Zu diesem Zweck sind auf der Cyber Range die typischen Systeme vorhanden, die Organisationen üblicherweise in ihren IT-Infrastrukturen einsetzen, z. B. Firewalls, Endpoint Security, SIEM-Systeme. Darüber hinaus kann man in der simulierten Umgebung IT-Infrastrukturen nachbilden, wie man sie in realen Unternehmensnetzen einsetzt, z. B. Datenbanken, Mailserver, Webserver.

Um eine Analogie zu bemühen: Was ein Flugsimulator Piloten bietet, nämlich Reaktionen in kritischen Situationen zu trainieren, das bietet eine Cyber Range den Verantwortlichen für die operative Cybersicherheit in Unternehmen. So wie im Flugsimulator schwierige Wetterbedingungen oder technische Defekte wie ein Triebwerksausfall simuliert werden können, werden Trainingsteilnehmer auf einer Cyber Range mit Cyberangriffen konfrontiert. Trifft man in einer kritischen Trainingssituation eine falsche Entscheidung, entsteht – wie im Flugsimulator – kein (realer) Schaden.

Cyber Ranges werden für Training und Weiterbildung von Berufstätigen eingesetzt, um praktische Fähigkeiten für Ernstfälle zu erlernen und zu üben; auch in der universitären Ausbildung werden sie in einfacheren Ausführungen genutzt.

3.2 Welchen Nutzen hat eine Cyber Range?

Mit Hilfe von Cybertrainings auf einer Cyber Range können sowohl weniger erfahrene Personen ihren Umgang mit Cyberangriffen erlernen als auch erfahrene IT-Spezialisten sich kontinuierlich weiterbilden. Trainings in einer solchen Umgebung tragen zur Risikovorsorge von Unternehmen bei, da die Teilnehmer danach im Ernstfall besser reagieren können.

Die Verbesserung der Reaktionsfähigkeit hat mehrere Facetten: Angriffe können besser und schneller erkannt werden, Prozesse für den Ernstfall können besser geprobt werden und die Handlungs- und Entscheidungssicherheit im Ernstfall wird gesteigert. Mitarbeitende können sich in Angriffe einarbeiten, die sie sonst nur aus Beschreibungen kennen.

All dies führt für Unternehmen zur Reduktion von Risiken, was folgende Aspekte beinhaltet: geringere Ausfallzeiten bei Angriffen, Vermeidung von Schäden bei Angriffen, geringere finanzielle Verluste, Schutz der Reputation und Verringerung von Datenschutzrisiken. Ein Training auf einer Cyber Range kann auch aufzeigen, wo noch Defizite und Nachbesserungsbedarfe bestehen.

Darüber hinaus tragen moderne Cybertrainings auf einer Cyber Range auch zur Erfüllung von Anforderungen im Zusammenhang mit Compliance und Governance bei, wie etwa zur Erfüllung regulatorischer Anforderungen, dem Nachweis von Sicherheitsmaßnahmen nach dem Stand der Technik oder der Reduktion von Haftungsrisiken.

In einer Studie zum Nutzen von Cybertrainings auf Cyber Ranges durch praktische Übungen in der akademischen Lehre wurde insbesondere die Gamifizierung hervorgehoben, die das Lernen positiv unterstützt.[20]

4 Cybertrainings als Pflicht

4.1 Allgemeine Anforderungen für Unternehmen

Die Ergreifung von geeigneten Maßnahmen zur Abwehr von Organisationsrisiken, also auch implizit zur Abwehr von Cyberangriffen, und die Verpflichtung zur Durchführung von Cybertrainings lässt sich aus verschiedenen Rechtsvorschriften ableiten. Üblicherweise hat nach diesen Vorschriften die obere Leitungsebene in Organisationen, z. B. der Vorstand oder die Geschäftsführung die Verpflichtung, Schäden für ihre Organisation abzuwehren, wofür sie entsprechende Sorgfaltspflichten erfüllen muss. Beispiele sind etwa § 93 Aktiengesetz[21] oder § 43 GmbH-Gesetz[22].

Darüber hinaus bestehen organisationsinterne Regularien, aus welchen sich konkrete rollenabhängige Verpflichtungen für einzelne Personen ergeben können, wie z. B. Geschäftsordnungen oder Gesellschaftsverträge. Aufgrund der zunehmenden Abhängigkeit von IT-Systemen und der Bedrohungslage gehören adäquate Cybersicherheit und Risikovorsorge zu den Kernpflichten einer sorgfältig handelnden Geschäftsführung.

Welche Maßnahmen als adäquat zur Erfüllung dieser Kernpflichten verstanden werden, hängt von dem jeweiligen Stand der Technik und der kanonischen Auslegung ab. Cybertrainings sind bereits als adäquate Maßnahme zur Risikoreduktion von Cyberangriffen anerkannt.[23] Unternehmen brauchen Maßnahmen für den Fall, dass Angreifer erste Verteidigungslinien überwunden haben. Hierbei helfen Cybertrainings.

4.2 Anforderungen aus spezifischen Rechtsakten

Neben den genannten allgemeinen Anforderungen, aus denen man in impliziter Weise eine Verpflichtung für Cybertrainings

16 National Institute of Standards and Technology (NIST): „The Cyber Range – A Guide". 2023, https://www.nist.gov/system/files/documents/2023/09/29/The%20Cyber%20Range_A%20Guide.pdf

17 Karel Kuchar, Petr Blazek, Radek Fujdiak: From Playground to Battleground: Cyber Range Training for Industrial Cybersecurity Education. ACM ICCNS 2023

18 M.N. Katsantonis, A. Manikas, I. Mavridis,·D. Gritzalis: Cyber range design framework for cyber security education and training. International Journal of Information Security (2023) 22

19 Muhammad Mudassar Yamin, Basel Katt, Vasileios Gkioulos: Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security 88 (2020)

20 Willi Lazarov, Tiina Schafeitel-Tähtinen, Joseph Squillace, Zdenek Martinasek, Aneta Coufalikova, Marko Helenius,·Petr Gallus, Radek Fujdiak: Lessons Learned from Using Cyber Range to Teach Cybersecurity at Diferent Levels of Education. Technology, Knowledge and Learning, Springer, April 2025

21 Bundesministerium für Justiz: Aktiengesetz (AktG). https://www.gesetze-im-internet.de/aktg/

22 Bundesministerium für Justiz: Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG). https://www.gesetze-im-internet.de/gmbhg/

23 Fabian M. Teichmann, Sonja R. Boticiu: Adequate responses to cyber-attacks. International Cybersecurity Law Review (2024) 5

ableiten kann, existieren auf Basis anderer Rechtsakte konkretere Anforderungen.

Für den Bereich der kritischen Infrastrukturen besteht nach Art. 21 Abs. 1&2 der NIS-2-Richtlinie[24] die Anforderung, dass Einrichtungen sicherzustellen haben, dass geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergriffen werden. Cybertrainings helfen, die Risiken für die Sicherheit der Netz- und Informationssysteme zu beherrschen, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

Gemäß DSGVO Art. 32(1)[25] haben die für die Verantwortlichen und auch deren Auftragsdatenverarbeiter die Sicherheit der Verarbeitung zu gewährleisten, was neben geeigneten technischen auch organisatorische Maßnahmen umfasst, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dies schließt auch die hierfür notwendigen Fähigkeiten ein, um Angriffe auf Daten zu erkennen und abzuwehren.

Wenn Hersteller von Software Funktions- und Sicherheitsaktualisierungen über das Internet verteilen, dann sind diese Systeme attraktive Ziele für Lieferkettenangriffe, über die man manipulierte Softwarekomponenten an viele Nutzer verteilen kann. Hierfür ist der Cyber Resilience Act (CRA)[26] einschlägig. So besteht die Verpflichtung gemäß CRA Anhang I, Teil I, Ziffer 2a, dass Softwareprodukte ohne ausnutzbare Schwachstellen auf dem Markt bereitgestellt werden und nach Anhang I, Teil II, Ziffer 2 Sicherheitsaktualisierungen bereitgestellt werden, nach Anhang I, Teil II, Ziffer 7 ggf. auch durch automatisierte Prozesse. Es liegt somit in der Verantwortung der Hersteller sicherzustellen, dass die Softwareverteilung sicher ist.

5 Die ATHENE Cyber Range

Als Mitwirkender im Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE betreibt das Fraunhofer SIT die ATHENE Cyber Range. Auf dieser wird Personen von externen Organisationen die Möglichkeit geboten, ihre defensiven Fähigkeiten in Bezug auf Cyberangriffe zu trainieren.

Jeder Trainingskurs besteht aus mehreren Trainingseinheiten, in denen jeweils ein komplexer Angriff behandelt wird. Jeder komplexe Angriff ist auf ein größeres Ziel in der angegriffenen Organisation ausgerichtet, wie z. B. ein Spionageangriff auf eine Unternehmensdatenbank. Das Erreichen dieses Ziels würde üblicherweise einen größeren Schaden verursachen, wie z. B. Datenverlust, Geschäftsprozessunterbrechung oder Publikation von Geschäftsinformationen kombiniert mit Erpressung. Jeder behandelte Angriff besteht aus mehreren Schritten, die zwischen dem initialen Eindringen in die IT-Infrastruktur der Organisation und dem Angriffsziel liegen. Aktuell kann man auf der ATHENE Cyber Range insgesamt 22 verschiedene komplexe Angriffe in 9 Trainingskursen trainieren (*https://www.athene-center.de/cyber-range-trainings*).

Das Angebot der Cybertrainings auf der ATHENE Cyber Range wird kontinuierlich ausgebaut, so dass neue Trainingskurse mit weiteren Cyberangriffen hinzukommen.

6 Fazit

Die hohe Zahl erfolgreicher Angriffe und Schäden für Organisationen macht deutlich, dass die üblichen Schutzmaßnahmen offensichtlich nicht genügen. Aus Post-mortem-Analysen ist bekannt, dass Angriffe während ihrer oftmals monatelangen Anbahnung hätten erkannt und verhindert werden können, wenn die an der operativen Cybersicherheit arbeitenden Personen hierfür besser vorbereitet gewesen wären. Für diese Vorbereitung wurden Cyber Ranges entwickelt, auf denen die notwendigen spezialisierten Fähigkeiten ausgebildet und trainiert werden können. Cybertrainings sind wichtig, denn im Ernstfall muss schnell reagiert werden.

Da Cybertrainings einen wichtigen Beitrag zur Risikovorsorge für Unternehmen leisten und die Ebene der Entscheider für die Abwendung von Schäden in Unternehmen verantwortlich ist, besteht eine implizite Verpflichtung zur Durchführung von Cybertrainings. Für andere Trainings in kritischen Bereichen, wie z. B. in der Luftfahrt, sind die Häufigkeiten und Zeiträume für Trainings explizit vorgeschrieben.

Für Cybertrainings in besonders regulierten Bereichen wie etwa kritische Infrastrukturen wären explizite Vorschriften von Vorteil. Aber auch in anderen Bereichen sollten Aufsichtsgremien bei ihrer Überprüfung der verwendeten Maßnahmen zur Cyberresilienz in Unternehmen auf Cybertrainings achten. Für die Angebote von Versicherungen zu Cyberschäden ist die Durchführung von Cybertrainings ebenfalls ein relevantes Kriterium für die Bemessung von Versicherungsprämien oder des Deckungsumfangs.

24 Europäische Union: Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

25 Europäische Union: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

26 Europäische Union: Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung)