IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Trendkategorie: Digitalisierung und Konnektivität

Cyberkriminalität

Der Begriff Cyberkriminalität ist ein Kunstwort, das missverständlich sein kann. Daher spricht man idealerweise von „Angriffen auf Steuerungen“, „Straftaten, die aus dem Internet heraus begangen werden“ oder „Straftaten, die mit einem Computer durchgeführt werden“. Die Ziele sind Informationsgewinnung, Identitätsdiebstahl, Sabotage, Spionage, Erpressung, Raub von Kryptowährungen, Zerstörung physischer Systeme, Desinformation oder terroristische Akte.

Top-Trend

Hierzu gehören beispielsweise:

- Angriffe auf Fernsteuerungen etwa per Schmalband-Funk, WLAN oder optischer Verbindung,
- Angriffe auf Steuerungen oder Angriffe auf Computersysteme, z. B. über Schadprogramme (Ransomware), DDoS-Angriffe (mutwillige Überlastung der IT-Infrastruktur) oder Spam und Phishing (gefälschte und schadhafte E-Mails),
- Taten, die das Persönlichkeitsrecht, Urheberrecht oder Markenrecht verletzen, z. B. durch Datenleaks und Doxing (Sammlung personenbezogener Daten),
- Diebstahl von digitalen Werten (Non-Fungible Token oder Token in einer Kryptowährung),
- Vorbereiten von Programmen, die auch zum Ausspähen von Computersystemen verwendet werden könnten,
- Einbau von Hintertüren, die den unautorisierten Zugang auf Systeme erlauben, z. B. Hardware-Trojaner,
- Leugnen, Verschweigen oder Offenhalten von Sicherheitslücken,
- Verbreiten von Lügen oder Unwahrheiten,
- unerlaubtes Erstellen von Bewegungsprofilen.

Was beschleunigt, was bremst den Trend?

Cyberkriminalität ist eines der am stärksten zunehmenden Kriminalitätsphänomene mit hohem Schadenspotential: Im Jahr 2021 gab es in Deutschland mit 146.363 Delikten einen neuen Höchstwert an Cyberstraftaten – ein Anstieg von mehr als zwölf Prozent gegenüber 2020. Der wirtschaftliche Schaden betrug 223,5 Milliarden Euro[1]. Die infolge des coronabedingten Digitalisierungsschubs entstandenen neuen Tatgelegenheiten haben sich im Jahr 2022 durch die Aufhebung der Schutzmaßnahmen in der Pandemie teilweise wieder reduziert. Allerdings sind die Auslandstaten (Aufenthaltsort der Kriminellen im Ausland oder unbekannt) im Vergleich zum Vorjahr stark gestiegen, was die Aufklärung und Strafverfolgung erschwert[2].

Es gibt viele Faktoren, die der Kriminalität im Netz Vorschub leisten. Die Täterinnen und Täter passen sich flexibel an technische und gesellschaftliche Entwicklungen an und handeln zunehmend professionell und global. Zudem können Kriminelle nahezu von jedem Ort der Welt agieren und ihre Spuren gut verschleiern.

Auch steigt der Vernetzungsgrad in der Gesellschaft dynamisch und bietet Kriminellen immer neue Angriffspunkte und Möglichkeiten. Insbesondere die zunehmende Verbreitung des Internet of Things (IoT) und von Industrie 4.0 bietet neue Einfallstore für Cyberkriminelle[3]. Weitere Treiber sind die vermehrte Nutzung von GPS-Technologien, zentralen Datenbanken, drahtlosen und mobilen Geräten, Netzwerken oder Open-Source-Software.

Mittels Künstlicher Intelligenz (KI) können Hacker ihre Angriffe effektiver und effizienter durchführen und Schwachstellen in Programmcodes aufspüren. Beispielsweise kann der KI-gestützte Chatbot ChatGPT Phishing-Angriffe qualitativ deutlich verbessern[4]. Auch die Sammlung, Speicherung und Verarbeitung riesiger Informationsmengen im Zuge von Big Data bieten Kriminellen attraktive Angriffsziele und machen solche Systeme anfällig[5]. KI und Big Data können aber auch umgekehrt zur Stärkung der Cybersecurity eingesetzt werden. KI kann beispielsweise bei der Erkennung von KI-generiertem Bild und Text helfen. Mit Big Data lassen sich auffällige Netzwerkaktivitäten in Echtzeit identifizieren[6].

Einen negativen Einfluss auf die IT-Sicherheit hat der im Jahr 2007 verabschiedete „Hackerparagraph“ StGB 202c, der auch Personen kriminalisiert, die nach Sicherheitslücken suchen oder Tools programmieren oder verwenden, die dazu geeignet wären[7].

Der leichtfertige Umgang mit Daten verschärft die Sicherheitslage. Die Verschlüsselung und Signatur von E-Mails werden beispielsweise zu selten eingesetzt. Mails mit HTML-Code lassen sich leicht fälschen und mit versteckten Inhalten versehen.

Die Wahrscheinlichkeit von Hackerangriffen steigt, wenn persönliche Daten zu schnell preisgegeben werden oder wenn Apps genutzt werden, deren technische Vertraulichkeit nicht sichergestellt ist. Oft fördern Kriminelle ein solches Verhalten, indem sie Belohnungen in Aussicht stellen. Im Gegensatz dazu kann es sich positiv auswirken, wenn Kinder und Jugendliche schon früh den Umgang mit digitalen Technologien erlernen und technische Fähigkeiten erwerben.

Durch das Outsourcen von Fachleuten, die mit der Unternehmens-IT vertraut sind, verlieren Betriebe eigene Kompetenz. Auch werden Schutzmöglichkeiten, beispielsweise das „Minimale-Rechte-Prinzip“, oft nicht wahrgenommen.

Wer ist betroffen?

Laut BKA gibt es in Deutschland kein Unternehmen mehr, das nicht von Cybercrime betroffen ist. Generell stellt jedes Unternehmen unabhängig von Branche oder Größe ein potenzielles Ziel für Cyberkriminelle dar. Im Fokus stehen allerdings besonders Banken, Sparkassen, (private) Versicherungen, Unternehmen der Finanztechnologie (FinTechs), das produzierende Gewerbe, Medien, Krankenhäuser und Kliniken, Rechenzentren und die öffentliche Verwaltung[8].

Das Spektrum von Hackerangriffen reicht vom angreifbaren Herzschrittmacher, dessen Sicherheitslücken lange offenbleiben[9, 10], über Angriffe auf Kransteuerungen und Industrieanlagen bis hin zu Manipulationen einfacher IT-Komponenten. Es gibt Sicherheitslücken wie Ripple20, bei denen lediglich die Erreichbarkeit im Netzwerk für einen erfolgreichen Angriff genügt[11], oder auch Router, die bei abgeschalteter Fernwartung aus der Ferne kompromittiert werden können[12].

Beispiele

Beispiel 1

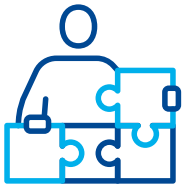
Die bislang größte Cyber-Attacke auf Internetkonzerne

Beispiel 2

Home-Office und mobiles Arbeiten erhöhen das Risiko für Cyberangriffe

Beispiel 3

KI als doppelter Game Changer in der Cyberkriminalität



Welche Veränderungen ergeben sich für die Sicherheit und Gesundheit der Beschäftigten?

Für die Beschäftigten in Unternehmen können Cyberangriffe eine akute Bedrohung für die Sicherheit der Beschäftigten darstellen und dramatische dramatische Folgen haben, etwa wenn Externe die Kontrolle über sicherheitsrelevante Systeme (z. B. Kühlsysteme zum Umgang mit chemischen Stoffen)[13] oder Anlagen und Maschinen (z. B. kollaborierende Roboter) übernehmen[14].

Es drohen schwere oder sogar tödliche Verletzungen für die Mitarbeitenden. Cyberattacken können – mit ihren unvorhersehbaren Folgen – aber auch eine psychische Belastung für die Beschäftigten sein, die relevante Netzwerke betreuen. Dazu gehören nicht nur akute Stresssituationen bei Angriffen, sondern auch schwerwiegende, langfristige psychische Probleme. Einige Betroffene leiden sogar unter schweren Traumasymptomen und benötigen psychologische Unterstützung[15]. Sofern vertrauliche oder sensible Informationen über Unternehmen oder Beschäftigte betroffen sind, können Angriffe sogar die gesamte Belegschaft beeinträchtigen. Den Betrieben drohen Reputationsschäden bis hin zum vollständigen Verlust der Wettbewerbsfähigkeit.

Dem Schutz Kritischer Infrastrukturen (Energie- und Wasserversorgung, Transport und Verkehr, Informationstechnik, Telekommunikation) vor Cyberattacken kommt besondere Bedeutung zu. Der Druck auf die Unternehmen und Beschäftigten ist hoch, denn das potenzielle Schadensausmaß und die Folgen für die betroffenen Betriebe und Einrichtungen und in extremen Fällen auch für die Gesellschaft und die öffentliche Sicherheit können immens sein.

Die zunehmende Arbeit im Homeoffice, ein unzureichender Schutz der Heimnetzwerke, der Einsatz privater IKT-Geräte – auch in Unternehmen – und die verbreitete Nutzung der sozialen Medien zu privaten oder dienstlichen Zwecken können den Schutz vor Cyberattacken erschweren. So kann die Sorge vor Angriffen dazu führen, dass Unternehmen mobile Arbeit einschränken mit möglichen nachteiligen Folgen für Betrieb und Beschäftigte (Verlust von Flexibilität, Motivation, Commitment)[13].

Sich gegen Cyberbedrohungen und -angriffe zu wappnen („Cyberresilienz“) ist für Unternehmen essenziell, geht meist mit einem enormen finanziellen und personellen Aufwand einher und wird durch den verbreiteten Mangel an IT-Personal deutlich erschwert.

Was sind Erkenntnisse und Perspektiven für den Arbeitsschutz?

- Cyberkriminalität stellt für alle Unternehmen ein massives und weiter an Bedeutung zunehmendes Problem dar. Die frühzeitige und regelmäßige Sensibilisierung für das Thema und Schulungen zum bewussten Umgang mit potenziellen Security-Risiken müssen ein Thema im Arbeitsschutz werden.

- Grundsätzlich sollte zur Abwehr von Cyberangriffen jeder einzelne Datenzugriff verifiziert werden – unabhängig von seinem Ausgangspunkt. Für Unternehmen, Behörden und wissenschaftliche Einrichtungen ist die Umsetzung dieses Zero-Trust-Paradigmas notwendig. Ein umfassender Schutz im Inneren des eigenen Systems ist essenziell, da es Cyberangreifern fast immer gelingt, ins Zentrum von Systemen vorzudringen[16].

- Industrial Security: Zu den wichtigen Maßnahmen gegen Cyberkriminalität gehören technische Sicherheitsmaßnahmen (Absicherung von Netzübergängen, Verschlüsselung der E-Mail-Kommunikation, Zwei-Faktor-Authentifizierungen etc.), aber auch die Sensibilisierung der gesamten Belegschaft für die allgegenwärtige Gefahr von Cyberangriffen.

- Ein Kernproblem im Bereich der IT-Security ist die bislang schlechte Kommunikation. Bei kritischen Sicherheitslücken müssen Hersteller und Betreiber erreichbar sein und schnell die benötigten Informationen erhalten. Über eine security.txt -Datei können Webseiten diese Information bereitstellen (technische Spezifikation RFC 9116)[17]. Ergänzende Softwarestücklisten (SBOM) hinterlegen zentral, welche Software in einem Projekt Verwendung findet, damit diese bei Bekanntwerden von Sicherheitslücken schnell auffindbar ist[18].

- Besonders angesichts des gravierenden Mangels an IT-Fachleuten sollten Unternehmen in die regelmäßige Aus- und Weiterbildung der Beschäftigten investieren. Allen Beteiligten sollte bewusst sein, dass sich das Fehlen von Fachkräften und Sicherheitsforschenden verschärft, wenn die Suche nach Sicherheitslücken weiterhin kriminalisiert wird,

- Bei einem Cyberangriff ist ein Krisenmanagement mit Notfallplänen zu gewährleisten, das konkret die Gefahren für die Beschäftigten mithilfe technischer Maßnahmen minimiert, besonders bei Havarien, Attacken auf Kritische Infrastrukturen, Industrieanlagen etc. Idealerweise wird auch eine digitale Rettungskette mit einem „Digitalen Ersthelfer“ etabliert[19]. Ein Notfallkontakt für das Security-Management sorgt dafür, dass bei einem kritischen Sicherheitsproblem die entsprechende Information möglichst schnell an die zuständigen Stellen gelangt[20].

- Das Bundeskriminalamt (BKA) hat im Bereich der Cybercrimebekämpfung eine koordinierende Funktion. Zudem gibt es verschiedene Initiativen mit Akteuren aus Bundesländern, Wirtschaft und Gesellschaft, die sich für Cybersicherheit engagieren[6]. Mit diesen Institutionen bietet sich auch für die Unfallversicherung eine Vernetzung zur Optimierung und Weiterentwicklung der Prävention an. Grundlegende quantitative Informationen zur Lage der Cybersicherheit sowie vorbeugende Maßnahmen und Hilfestellung für den Fall eines Cyberangriffs stellt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) bereit.

- Der geplante Cyber Resilience Act (CRA) der EU will die digitale Sicherheit durch gemeinsame Standards für vernetzte Geräte und Dienste verankern. ‚Secure-by-Design‘ soll eine Sicherheitsarchitektur im digitalen Kern von Geräten sicherstellen, die von Beginn an alle relevanten Bedrohungsszenarien und Schwachstellen berücksichtigt[21]. Die DGUV sieht hinsichtlich des Verordnungsentwurfs noch Optimierungspotenzial und bringt sich in die weitere Ausgestaltung des CRA ein[22].

- Das Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA) klärt auf und forscht zum Thema Industrial Security. Zur Prüfung und Zertifizierung wurden die Prüfgrundsätze GS-IFA-M24 entwickelt, nach denen im Prüflabor für Industrial Security geprüft wird[23].

Herausgegeben von:

Deutsche Gesetzliche Unfallversicherung e.V. (DGUV)
Glinkastraße 40 · 10117 Berlin
Telefon: 030 13001-0 (Zentrale)
E-Mail: info@dguv.de
Internet: www.dguv.de

Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Risikoobservatorium der DGUV

Verfasst von: Dr. Ruth Klüser

Ausgabe:
Januar 2024

Satz & Layout:
Atelier Hauer + Dörfler, Berlin

Bezug: www.dguv.de/publikationen
Webcode: p022502

Die **Literaturliste** ist in der Online-Fassung der Trendbeschreibung verfügbar.

www.dguv.de/ifa
risikoobservatorium