Herausforderungen durch Cyberbedrohungen

Worauf sich Unternehmen in 2023 bezüglich IT-Sicherheit einstellen sollten

Die Lage der IT-Sicherheit in Deutschland spitzt sich zu. Das ist ein Fazit des Berichts zur Lage der IT-Sicherheit in Deutschland im Jahr 2022 des Bundesamts für Sicherheit in der Informationstechnik (BSI). Die Bedrohung im Cyberraum ist damit so hoch wie nie. Was wird uns 2023 erwarten und wie wappnen wir uns dagegen?

©Sikov - stock.adobe.com

Das BSI als die Cybersicherheitsbehörde des Bundes legt jährlich einen Überblick über die Bedrohungen im Cyberraum vor und bewertet diese auch zielgruppenspezifisch bezüglich Gesellschaft, Wirtschaft und Staat/Verwaltung. Für 2022 bezieht der Bericht auch die IT-Sicherheitslage im Kontext des russischen Angriffskrieges auf die Ukraine mit ein.

Cybererpressung bleibt große Bedrohung

Hauptbedrohung besonders für Unternehmen bleibt Ransomware, also Schadprogramme, die den Zugriff auf Daten und Systeme vor allem über Datenverschlüsselungen einschränken oder verhindern. Eine Freigabe der Ressourcen erfolgt nur gegen Zahlung eines Lösegelds (engl. „ransom"). Die Angreifenden nutzen Fehler wie falsche Bedienung, Fehlkonfigurationen, veraltete Software-Stände oder mangelhafte Datensicherungen aus. Die Zahlung des Lösegelds wird meist in elektronischen Währungen (üblicherweise Bitcoin oder Monero) gefordert.


© BSI

> *Wir müssen Nutzer stärker motivieren und anleiten, ihr Wissen zur IT-Sicherheit auch in die Tat umzusetzen.*
>
> Gerhard Schabhüser, Vizepräsident, BSI

Das häufigste Angriffsziel bei Ransomware ist der Mensch. Ein Haupteinfallspunkt ist bei Client-Systemen in der Regel eine E-Mail mit schadhaftem Anhang. In Unternehmensnetzen öffnen auch verwundbare oder schlecht gesicherte und extern erreichbare Server Angreifenden die Tür. Bei maliziösen Anhängen handelt es sich häufig um Office-Dateien mit VBA-Makros. Gerhard Schabhüser, Vizepräsident des BSI betont dazu: „Wir müssen Nutzerinnen und Nutzer stärker motivieren und anleiten, ihr Wissen zu IT-Sicherheit auch in die Tat umzusetzen."

Insbesondere das sog. Big Game Hunting, also die Erpressung umsatzstarker Unternehmen mit verschlüsselten und exfiltrierten Daten, hat weiter zugenommen. Sowohl die von IT-Sicherheitsdienstleistern berichteten Lösegeld- und Schweigegeld-Zahlungen als auch die Anzahl der Opfer, deren Daten etwa wegen ausbleibender Zahlungen auf Leak-Seiten veröffentlicht wurden, sind weiter gestiegen. Dass nicht nur Unternehmen Ziel von Ransomware-Angriffen sind, zeigt eindrücklich der folgenschwere Angriff auf eine Landkreisverwaltung in Sachsen-Anhalt: Erstmals wurde wegen eines Cyberangriffs der Katastrophenfall ausgerufen. Bürgernahe Dienstleistungen waren monatelang nicht oder nur eingeschränkt verfügbar.

Advanced Persistent Threat (APT)

Wenn ein gut ausgebildeter, typischerweise staatlich gesteuerter Angreifender zum Zweck der Spionage oder Sabotage über einen längeren Zeitraum hinweg sehr gezielt ein Netz oder System angreift, sich unter Umständen darin bewegt und/oder ausbreitet und so Informationen sammelt oder Manipulationen vornimmt, spricht man von einem Advanced Persistent Threat (APT).

Grundsätzlich stellen solche Angriffe für jedes Unternehmen, das vertrauliche, geschäftskritische Informationen auf IT-Systemen verarbeitet oder dessen Erfolg von der Verfügbarkeit seiner IT-Systeme abhängt, eine Bedrohung dar. In der Wirtschaft stehen Betriebs- und Geschäftsgeheimnisse, wie bspw. technologische Forschungs- und Entwicklungsergebnisse, Herstellungsverfahren oder unternehmenspolitische und operativ-betriebswirtschaftliche Entscheidungen wie Fusionen oder Verkäufe im Fokus der Angreifer. Angegriffen werden aber nicht nur bekannte Großunternehmen, sondern auch Beratungsunternehmen, Anwaltskanzleien und klein- und mittelständische Unternehmen (KMU), die bspw. in ihrem Marktsegment eine herausragende Position einnehmen (Hidden Champions) oder die Rolle eines wichtigen Zulieferers in der Supply Chain der zuvor genannten Großunternehmen innehaben. Dieser Einfallsvektor dient den Angreifenden dann u.U. als Sprungbrett bzw. Multiplikator, wodurch sich ihnen weitere Angriffsmöglichkeiten bieten.

Vor diesem Hintergrund stehen viele Institutionen vor der Herausforderung, sich vor gezielten Angriffen bzw. APTs zu schützen. Für die Prävention, Detektion und Reaktion hat das BSI Maßnahmendokumente erstellt, die das Ziel verfolgen, „Erste Hilfe" bei der Vorfallbearbeitung zu leisten.

Wiperware und hybride Mensch-Maschine-Angriffe

Der Angriff Russlands auf die Ukraine führt deutlich vor Augen, dass der moderne, digitale Krieg auch vor der eigenen Haustür stattfindet. Laut Barracuda Networks fällt insbesondere der verstärkte Einsatz von Wiperware auf, also destruktiver Schadsoftware, die gut getarnt in das Netzwerk einer Organisation gelangt und dort Daten löscht und überschreibt und sogar die Wiederherstellung verhindert. „Die Häufigkeit hat drastisch zugenommen, wie etwa WhisperGate, CaddyWiper oder HermeticWiper zeigen, die seit Ausbruch des Krieges Schlagzeilen machen" erläuter Fleming Shi, CTO bei Barracuda Networks. Im Gegensatz zu den monetären Motiven und dem Entschlüsselungspotenzial von Ransomware wird Wiperware in der Regel von nationalstaatlichen Angreifern mit dem Ziel eingesetzt, die Systeme eines Gegners so zu beschädigen und zu zerstören, dass eine Wiederherstellung unmöglich ist. Zudem wird die von Russland ausgehende Wiperware künftig wahrscheinlich auf andere Länder übergreifen, da die geopolitischen Spannungen keineswegs abnehmen. Dies gilt aber auch für Hacktivismus nichtstaatlicher Angreifer, die nach weiteren Maßnahmen zur Ausbeutung ihrer Opfer suchen. Um die Geschäftskontinuität trotz eines Angriffs zu gewährleisten, müssen sich Unternehmen auf die Wiederherstellung des gesamten Systems konzentrieren, damit nicht nur die Daten, sondern die gesamte IT-Infrastruktur wieder funktionsfähig ist. Eine schnelle Wiederherstellung der virtuellen Version eines angegriffenen physischen Systems kann bspw. die Widerstandsfähigkeit eines Unternehmens gegen Wiperware oder andere destruktive Malware-Angriffe erheblich verbessern.


© Barracuda Networks

> *Wiperware wird verstärkt länderübergreifend eingesetzt und Ransomware-Banden werden kleiner und geschickter.*
>
> Fleming Shi, CTO, Barracuda Networks

2022 standen die großen Ransomware-Banden – LockBit, Conti und Lapus$ – hinter Aufmerksamkeit heischenden Angriffen, die sie regelmäßig in die Schlagzeilen brachten. 2023 mit dem boomenden Geschäftsmodell Ransomware-as-a-Service und dem jüngsten Build-Leak von LockBit 3.0 wird eine neue Generation kleinerer und intelligenterer Banden ihnen die Schau stehlen. Und Unternehmen werden sich öfter Ransomware-Angriffen mit neuen Taktiken gegenübersehen. Wer darauf nicht vorbereitet ist, riskiert Geschäft und Ruf zu beschädigen.

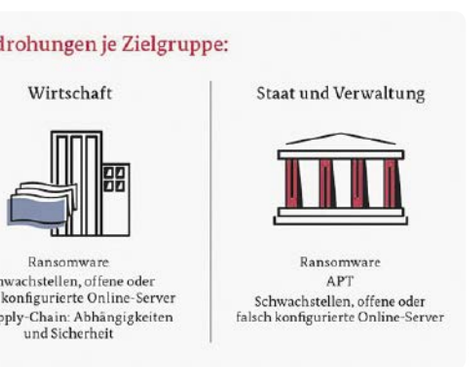
„Der Wettlauf zwischen Hackern und IT-Sicherheitsteams geht 2023 weiter" betont auch Jörg von der Heydt, Director DACH bei Bitdefender. Neue Tools und schnellere Hardware bei wachsendem oft staatlich unterstütztem Budget bringen die Angreifer in eine immer stärkere Position.

Eine kontinuierlich steigende Anzahl von Schwachstellen und die fehlenden Ressourcen oder unzureichende Tools, diese zeitnah zu patchen, unterstützen diese Tendenz. Eine besondere Gefahr ist die zeitnahe Verfügbarkeit von Quanten-Computing, welche Verschlüsselung und Passwortsicherheit disruptiv verändern wird. Bereits jetzt ist ein Umdenken nötig.

Ebenso wichtig sind hybride Mensch-Maschine-Angriffe: Automatisierte Tools identifizieren Schwachstellen in der anzugreifenden Infrastruktur – Experten werten diese dann hinsichtlich des Angriffspotenzials aus. Eigentlich sollte auch die Cyberabwehr so vorgehen. Ihr fehlen jedoch häufig Budget, Zeit, Skills und das kompetente Personal.

Wollen Unternehmen – gleich welcher Größe und Branche – nicht Opfer eines solchen intelligenten Angriffs werden, müssen sie ebenfalls auf hybride Abwehr setzen. „Fight Fire with Fire" gilt also auch hier: Firmen müssen entweder selbst Teams (aus-)bilden – oder sie durch externe Managed Detection and Response (MDR) ergänzen. Wichtig ist dabei, die möglichen Schäden zu verstehen. Oft fehlt dieses Bewusstsein noch und IT-Sicherheit wird lediglich als Kostenfaktor mit unsichtbarem Nutzen betrachtet.

Fortsetzung auf **Seite 18** ▶



© BSI

Das BSI, die Cyber-Sicherheitsbehörde des Bundes, hat seinen jährlichen Überblick über die Bedrohungen im Cyber-Raum vorgelegt und bewertet diese auch zielgruppenspezifisch bezüglich Gesellschaft, Wirtschaft und Staat/Verwaltung. Für 2022 bezieht der Bericht auch die IT-Sicherheitslage im Kontext des russischen Angriffskrieges auf die Ukraine mit ein.

Herausforderungen durch Cyberbedrohungen

◄ Fortsetzung von **Seite 17**

E-Mail-Security und Ransomware-as-a-Service

„So lange Russland Krieg führt, ist die Bedrohungslage besonders ernst zu nehmen. Hier sind vor allem KRITIS-Betreiber gefordert, beispielsweise im Energie- und Finanzsektor. In der öffentlichen Verwaltung ist künftig vermehrt mit DDoS-Angriffen zu rechnen – wie etwa kürzlich bei der Attacke gegen den Website-Zugang des EU-Parlaments“ betont Lothar Hänsler von Radar Cyber Security.


© Radar Cyber Security

> *Die Bedrohungslage bleibt 2023 angespannt, insbesondere KRITIS-Betreiber sind gefordert.*
> **Lothar Hänsler, COO, Radar Cyber Security**

Eine der größten Bedrohungen für Unternehmen und Behörden ist nach wie vor die sich ständig verändernde Bedrohungslage um Ransomware und E-Mails, die gefährliche Schadsoftware enthalten bzw. sogar die Kombination aus beiden Formen. Neuere Arten der Erpressungssoftware setzen gar nicht mehr unbedingt auf die Verschlüsselung von Daten, sondern auf die Exfiltration. Die Angreifer üben dann Druck aus, indem sie mit der Veröffentlichung der Daten drohen. Sie wenden immer ausgefeiltere Methoden an, um zu erreichen, dass E-Mail-Anhänge geöffnet werden oder bestimmte Websites angesteuert werden. Im schlimmsten Fall erreichen sie es, dass Anmeldedaten und Login-Informationen abgefangen werden, die zur weiteren Kompromittierung genutzt werden.

Eines der zentralen Themen für Unternehmen und Behörden bleibt daher E-Mail-Security. Um die wesentlichen offenen Flanken abzudecken, braucht man ein dreiteiliges Maßnahmenpaket: Technik (Reputationsprüfung von Webseiten, Sandboxing, Malware-Schutz, kontinuierliche Überwachung, Analyse von Ereignissen), Personal (Sensibilisierungsmaßnahmen, Schulungen) und Prozesse (regelmäßige zeitnahe Behebung von Schwachstellen, Notfallpläne und -übungen). Hänslers Empfehlung: „Als Konsequenz daraus ergibt sich, dass wir Systeme konsequent cyberwiderstandsfähiger machen müssen. Zero-Trust-Netzwerke müssen ebenso ins Auge gefasst werden wie die Absicherung von Remote-Zugängen. Der Einsatz von Endpoint Detection and Response (EDR) ist dringend anzuraten – und auch die OT-Sicherheit darf nicht vergessen werden. Die ganzheitliche und konsolidierte Sicherheitsbetrachtung wird im Kontext von Risikomanagement zunehmend wichtiger.“


© Cradlepoint

> *Mobiles Edge-Computing über 5G-Netze geht 2023 in den Produktivbetrieb und erfordert moderne Sicherheitskonzepte wie ZTNA.*
> **Jan Willeke, Area Director Central Europe, Cradlepoint**

Robert Rudolph, Product Marketing Consultant bei ForeNova, sieht zukünftig noch mehr Bedrohungen zur Genüge vorhandenen Kapitals, um hohe Lösegeldforderungen zu bedienen, zum anderen wegen einer zu traditionellen IT-Security aus Firewall und Anitvirus-Software. Die aktuellen Krisenlagen finden ihren Niederschlag in gezielten Angriffen auf Verbündete in Konflikten und deren kritische Infrastruktur. Zugleich professionalisieren sich die Cyberkriminellen weiter. Ransomware-as-a-Service im Darknet führt zu mehr Begehrlichkeiten bei allen, die die Konkurrenz sabotieren wollen oder Cyberattacken politisch ausnutzen möchten.“

Die Angreifer gehen immer gezielter vor. Sie durchleuchten die Opfer im Vorfeld umfangreich und finden über Sicherheitslücken und Social Engineering nur allzu oft einen Weg in die Unternehmensnetzwerke. Zunehmend viele „Clients“ – wie etwa IoT-Geräte im Gesundheitswesen – sind dann Angriffsfläche für Cyberattacken. IT-Verantwortliche müssen daher klassische signaturbasierte Abwehransätze mit Sicherheitstechnologien ergänzen, die anomale Aktivitäten im Netzwerk und auf Endpunkten effektiv aufspüren. Neben der Verhaltensanalyse ist der nächste Trend der proaktive Schutz: Funktionen wie Ransomware Honeypots können Aktionen der Angreifer gezielt triggern und aktiv bekämpfen, bevor der Cyberkriminelle seinen Gesamtplan durchführt. Wer sich dagegen wehren will, sollte auf die Hilfe externer Cybersecurity-Experten zurückgreifen.


© Hornetsecurity

> *Unternehmen müssen der Schulung und Fortbildung eine höhere Priorität einräumen, um Remote-Arbeit sicher zu machen.*
> **Daniel Hofmann, CEO, Hornetsecurity**

für mittelständische Unternehmen: „Das Jahr 2023 wird die Welt der Cybergefahren weiter umwälzen. Insbesondere der Mittelstand, wie etwa das produzierende Gewerbe, steht dabei im Blickpunkt. Zum einem wegen seines wertvollen sensiblen Know-hows und potenziell steht hier ein intelligenter, einfach anzuwendender und zuverlässiger Ansatz zur Verfügung. Unternehmen können damit das Risiko sog. Seitwärtsbewegungen von Schadsoftware im Netzwerk verringern, weil die Benutzer direkt mit Anwendungen statt mit dem Netzwerk verbunden sind. ZTNA entwickelt sich immer mehr zu einem Standard im Networking-Bereich, den es auch bei Wireless-WANs einzuhalten gilt.“

Einfallstor „Mensch“

Je einfältiger der Tor, desto größer das Einfallstor für Cyberkriminelle: Als Grundlage aller Cybersecurity-Maßnahmen ist zunächst der gesunde Menschenverstand gefragt.

Die durch Corona beschleunigte Flexibilisierung der Arbeitswelt mit dem verstärkten Einsatz von Homeoffice bzw. hybrider Arbeit und Remote-Arbeitsplätzen hebt auch die Cyberrisiken auf eine neue Ebene: der private Bereich verbindet sich IT-mäßig mit dem dienstlichen, und neben der IT-OT-Konvergenz, also dem Zusammenrücken von Produktionstechnologien und der Büro-IT, könnte man auch von einer B-C-Konvergenz, also dem Zusammenwachsen von Business- und Consumer-IT sprechen.


© ForeNova

> *Heterogene Angriffe diktieren eine verhaltensbasierte und proaktive Abwehr.*
> **Robert Rudolph, Product Marketing Consultant, ForeNova**


© privat

> *Gesunder Menschenverstand ist gefragt: Je einfältiger der Tor, desto größer das Einfallstor für Cyberkriminelle.*
> **Volker Oestreich, Inhaber, Dr. Oestreich Consulting**

Eine aktuelle Umfrage von Hornetsecurity zeigt die Herausforderungen für das Sicherheitsmanagement und die Risiken für die Cybersicherheit der Remote-Mitarbeiter und identifiziert zwei Hauptprobleme: Auf der einen Seite haben Mitarbeiter Zugang zu kritischen Daten, auf der anderen Seite werden nicht genügend Schulungen zum Umgang mit der Cybersicherheit oder zur Verringerung des Risikos von Cyberangriffen oder einer Sicherheitsverletzung angeboten. Cyberkriminelle werden immer erfinderischer und nutzen nachlässige Remote-Anwender zu ihrem Vorteil. Beobachtet wird eine Zunahme vor allem bei Angriffen auf Smartphones, da Hacker erkannt haben, dass Menschen ihre Arbeit auch auf privaten Endgeräten erledigen und diese sowohl private als auch berufliche Daten enthalten. „Die Popularität von hybrider Arbeit und die damit verbundenen Risiken bedeuten, dass Unternehmen der Schulung und Fortbildung eine höhere Priorität einräumen müssen, um Remote-Arbeit sicher zu machen“, sagt Daniel Hofmann, CEO von Hornetsecurity.

2022 wurden durchschnittlich 400.000 neue schädliche Dateien entdeckt – pro Tag! Auch für das kommende Jahr erwarten die Sicherheitsexperten von Kaspersky, dass sich Cyberkriminelle die aktuellen Trends für ihre Angriffe weiter zu Nutze machen. Damit Verbraucher sicher ins neue Jahr starten können und im Laufe dessen auch geschützt bleiben, gibt Kaspersky Verbrauchern den Tipp, sich vor Betrugsmaschen durch Cyberbedrohungen jeglicher Couleur zu schützen. Deshalb sollte man großzügigen „Werbegeschenken“ und „Rabatten“, z.B. für knapp gewordenen Konsolen, äußerst kritisch gegenüberstehen.

In Anbetracht der dicht gedrängten Liste von Filmpremieren im Jahr 2023 erwartet Kaspersky mehr Trojaner, die sich als bekannte Streamingdienste tarnen, sowie diverse Betrugsversuche, die auf Streamingdienstnutzer abzielen. Weiterhin werden Betrüger die zunehmende Beliebtheit der Spiele-Abonnementdienste von Sony und Microsoft für sich ausnutzen. Fans sollten die Webseiten der Anbieter nur über die Original-URL besuchen und bei Mails, die vermeintlich von Streamingdiensten stammen und bspw. nach Login-Daten fragen, aufmerksam sein – seriöse Anbieter fragen nach solchen Daten nicht per Mail.


© TÜV Süd

> *Mit einer Zertifizierung stärken Unternehmen ihren Schutz vor Cyberangriffen und beugen dem Verlust sensibler Informationen vor.*
> **Alexander Häußler, Lead Auditor, TÜV Süd**

Fazit – was tun?

Cyberbedrohungen sind allgegenwärtig und stellen eines der größten Risiken für Unternehmen dar. Der international etablierte Standard ISO/IEC 27001 für Informationssicherheit wurde überarbeitet und enthält neue Maßnahmen für mehr Cybersicherheit und Datenschutz. „Ein Informationssicherheitsmanagementsystem (ISMS) kann Unternehmen jeder Größe helfen, sich gegen Cyberangriffe und andere böswillige Datenmanipulationen effektiv zu schützen. Mit einer ISO/IEC 27001-Zertifizierung stärken Unternehmen ihren Schutz vor Cyberangriffen und beugen dem Verlust sensibler Informationen vor“, sagt Alexander Häußler, Global Product Performance Manager IT and Lead Auditor beim TÜV Süd.

Der Standard ISO/IEC 27001 ist die international führende Norm für ISMS und damit auch für die Cybersicherheit. Nach einer Überarbeitung im Oktober 2022 löst die neue ISO/IEC 27001:2022 die bisher geltende ISO/IEC 27001:2013 ab. Dadurch erhält die Sicherheitsnorm eine lange erwartete Anpassung bei Maßnahmen zu IT-Sicherheit, Datenschutz sowie konkrete Maßnahmen zur Cloudsicherheit. Die wichtigsten Änderungen betreffen die im Anhang A in vier Abschnitten definierten Maßnahmen (“Controls”): Organisational Controls (37 Maßnahmen), People Controls (acht Maßnahmen), Physical Controls (14 Maßnahmen) und Technological Controls (34 Maßnahmen). Die neu eingeführten Maßnahmen betreffen u.a. Datenmaskierung (um Daten für Hacker unbrauchbar zu machen), die Überwachung von Aktivitäten (um unübliche IT-Aktivitäten zu entdecken) sowie Informationssicherheit für die Nutzung von Cloud-Diensten. Ein Whitepaper vom TÜV Süd gibt dazu einen Überblick.

Volker Oestreich, CHEManager


© Bitdefender

> *Hybride Mensch-Maschine-Angriffe zielen auf Unternehmen aller Größen.*
> **Jörg von der Heydt, Regional Director DACH, Bitdefender**

„Verbraucher folgen Popkultur- und Social-Media-Trends, um dazu zu gehören“, sagt Anna Larkina, Sicherheitsexpertin bei Kaspersky. „Wir beobachten genau, wie Cyberkriminelle diese Interessen überwachen, um davon zu profitieren. Sie entwickeln betrügerische Systeme, die auf die aktuellen Trends abgestimmt sind.“ Zu diesen Trends zählen auch Mental-Health-Apps oder Online-Bildungsplattformen. Die Kaspersky-Experten erwarten mehr Trojaner, die sich als weitverbreitete Online-Bildungsplattformen ausgeben, genauso wie Phishing-Seiten für Videokonferenzdienste und den Diebstahl von LMS-Anmeldedaten. Nutzer sollten daher entsprechende Tools nur über die Webseiten der offiziellen Anbieter herunterladen sowie für jeden Dienst ein eigenes starkes Passwort wählen.


© Kapersky

> *Verbraucher folgen Popkultur- und Social-Media-Trends, um dazu zu gehören – Cyberkriminelle profitieren davon.*
> **Anna Larkina, Sicherheitsexpertin, Kaspersky**