Unsichtbare Bedrohung

Die Bedrohungslage von deutschen Unternehmen verschärft sich. Insbesondere die Cyberattacken legen kräftig zu. Das zeigt der aktuelle „Wirtschaftsschutzbericht 2024“ von Bitkom und BSI. Wie sich Unternehmen vor solchen Angriffen schützen können, zeigt der Beitrag.

ZayNyi/stock.adobe.com (KI-generiert)

Kleine und mittlere Unternehmen (KMU) werden zunehmend Ziel von Cyberattacken.

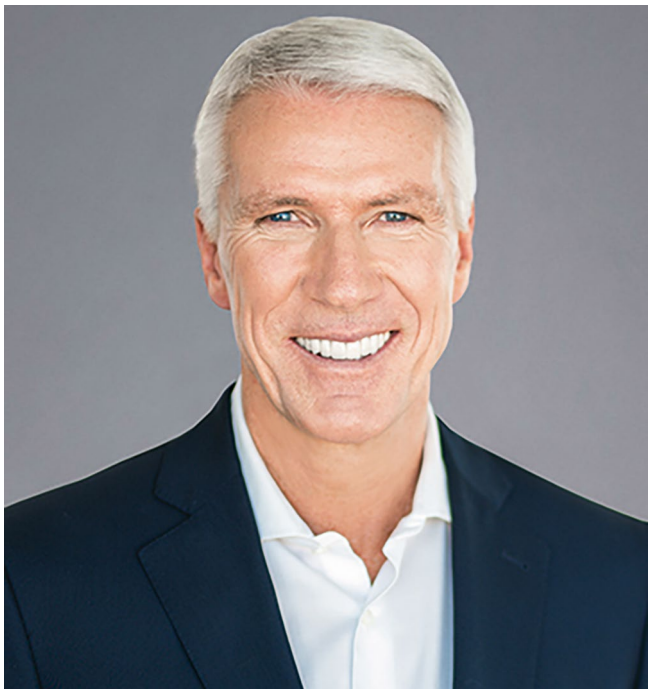
Es ist wie in der realen Welt: Einbrecher steigen nicht zuerst in die alarmgesicherte und videoüberwachte Villa mit hohen Sicherheitszäunen ein, wenn im Nebenhaus ein gekipptes Fenster den Einstieg erleichtert und das Gartentor nur angelehnt ist.

KMU im Visier der Angreifer

Auch in der virtuellen Welt suchen sich Kriminelle den einfachsten Weg, um in ein Unternehmensnetzwerk einzudringen, schrieb das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem Bericht zur „Lage der IT-Sicherheit in Deutschland“ im November 2023. Danach suchen Cyberkriminelle verstärkt solche Opfer aus, die ihnen leicht angreifbar erscheinen. Daher geraten nicht vor allem große Konzerne, wo viel zu holen wäre, sondern vermehrt kleine und mittlere Unternehmen (KMU) ins Visier der Angreifer. Und deutsche Firmen rücken offenbar immer stärker in den Fokus von Angreifern aus dem In- und Ausland, wie der aktuelle „Wirtschaftsschutzbericht 2024“ zeigt, den der Digitalverband Bitkom und das Bundesamt für Verfassungsschutz Ende August veröffentlicht haben. Demnach waren in den letzten zwölf Monaten 81 Prozent aller Betriebe von Diebstahl von Daten und IT-Geräten sowie von digitaler und analoger Industriespionage oder Sabotage betroffen. Weitere zehn Prozent vermuten dies. 2023 lagen die Anteile noch bei 72 und acht Prozent. Für die Studie waren laut Bitkom mehr als 1000 Firmen quer durch alle Branchen repräsentativ befragt worden. Dabei konnten 70 Prozent der Betriebe, die Opfer wurden, Angriffe der organisierten Kriminalität zuordnen. 2023 waren es erst 61 Prozent. Ausländische Geheimdienste wurden mit 20 Prozent deutlich häufiger als Täter genannt (2023: sieben Prozent).

Eine besondere Gefahr für die Wirtschaft bilden Bitkom zufolge allerdings Cyberangriffe. So sehen sich inzwischen zwei Drittel (65 Prozent) der Unternehmen durch Cyberattacken in ihrer Existenz bedroht, vor einem Jahr waren es noch 52 Prozent, 2021 sogar erst neun Prozent. 178,6 Milliarden Euro Schaden entstand der deutschen Wirtschaft in den vergangenen zwölf Monaten allein durch Cybercrime (Datendiebstahl, Sabotage und Industriespionage). „Die Bedrohungslage für die deutsche Wirtschaft verschärft sich also“, kommentiert Ralf Wintergerst, Präsident des Digitalverbandes Bitkom, die Zahlen des Wirtschaftsschutzberichts. Umso dringlicher ist: „Die Unternehmen müssen ihre Schutzmaßnahmen weiter hochfahren“, mahnt er. „Das gilt für digitale ebenso wie klassische Angriffe, etwa das Abhören von Besprechungen oder den Diebstahl von physischen Dokumenten.“

Die häufigste Bedrohung für Firmen ist „Ransomware“, eine Form der digitalen Erpressung: Daten gegen Geld. So berichten laut dem aktuellen Wirtschaftsschutzbericht Betriebe am häufigsten von Schäden durch Ransomware (31 Prozent, plus 8 Prozentpunkte), dahinter folgen Phishing-Attacken (26 Prozent, minus 5 Prozentpunkte), Angriffe auf Passwörter (24 Prozent, minus 5 Prozentpunkte) und Infizierung mit Schadsoftware (21 Prozent, minus 7 Prozent). Ebenfalls häufig Schäden verursachen sogenannte Distributed-Denial-of-Service-Angriffe, durch die zum Beispiel Webserver lahmgelegt werden (18 Prozent, plus 6 Prozentpunkte). Die Cyberkriminellen nutzen Schlupflöcher wie falsche Bedienung, Fehlkonfigurationen, veraltete Softwareversionen oder mangelhafte Datensicherungen aus, um Unternehmenssysteme tiefgreifend zu infiltrieren und Daten zu verschlüsseln. Für die Entschlüsselung verlangen die Angreifer ein Lösegeld. Häufig drohen sie zusätzlich noch damit, gestohlene Daten zu veröffentlichen. Hierbei steht für die Erpresser laut BSI nicht eine Maximierung des potenziellen Lösegelds im Vordergrund, sondern das rationale Kosten-Nutzen-Kalkül. Das Perfide ist, dass die Angreifer verschiedene Wege nutzen, um in Firmennetze zu gelangen. Zudem gibt es jedes Jahr neue „Vorlieben“ der Kriminellen, die zu ihrem Erfolg führen: Waren laut BSI-Bericht bis in den Berichtszeitraum 2023 hinein maliziöse Office-Dokumente das häufigste Angriffsmittel für die initiale Infektion, ersetzten Angreifer diese im Laufe des Jahres 2022 durch schadhafte Container-Dateien mit Formaten wie ISO oder IMG, während sie Anfang 2023 mehrheitlich zu maliziösen OneNote-Dateien für Spam- und Phishing-Mails wechselten.



Bitcom

Ralf Wintergerst, Präsident des Digitalverbandes Bitcom.

Sechs Phasen eines Angriffs

In sechs Phasen gliedert sich eine Attacke dem BSI zufolge. Auch wenn es einen vollständigen Schutz vor Ransomware-Angriffen nicht gibt, weil Angreifer auch neue Wege nutzen können, für die es noch keine Detektions- und Abwehrmethoden gibt, sind kleine Unternehmen nicht machtlos. Denn in jeder dieser sechs Phasen sind Gegenmaßnahmen möglich, um das Eindringen in Netzwerke oder das Verschlüsseln von Daten entweder zu verhindern oder möglichen Schaden wenigstens, so gut es geht, zu begrenzen.

1. Erstinfektion: Ein Ransomware-Angriff beginnt häufig mit einer maliziösen E-Mail, der Kompromittierung eines Fernzugriff-Zugangs (Remote-Zugang) wie zum Beispiel Remote Desktop Protocol (RDP) oder der Ausnutzung von Schwachstellen. Hier empfiehlt das BSI, empfangene E-Mails grundsätzlich als „Nur-Text" oder „reiner Text" codiert anzuzeigen. Mitarbeiter sollten im Umgang mit Mails sensibilisiert und geschult werden – gerade in Bereichen, wo viele externe Mails eintreffen. Bei Busunternehmen kann das im Marketing oder in der Kundenbetreuung der Fall sein. Als Gegenmaßnahme zum Remote-Zugang rät das BSI zur Multifaktor-Authentifizierung, auch sollte der Zugriff von außen über Virtual Private Networks (VPN) in Kombination mit einer Multifaktor- Authentifizierung abgesichert werden.

2. und 3. Rechteerweiterung und Ausbreitung: Nach dem Einbruch verfügt der Angreifer nur über diejenigen Zugriffsrechte, die der kompromittierte Account besitzt. Deshalb laden Angreifende in der Regel weitere Schadsoftware nach, um die erlangten Zugriffsrechte zu erweitern und zum Beispiel an Administratorrechte zu gelangen. Um sich davor zu schützen, sollten KMU privilegierte Konten wie Administrator-Accounts absichern, zum Beispiel über Multifaktor-Authentifizierung. Zudem rät das BSI, für die Administration von Clients keine Domänen-Administrationskonten zu verwenden. Vor Ausbreitung schützt eine saubere Netzwerksegmentierung.

4. Datenabfluss: Die Cyberkriminellen können Daten entwenden, um später mit deren Veröffentlichung zu drohen, falls ein Opfer nicht zu einer Lösegeld- oder Schweigegeldzahlung bereit ist. Mit einer Anomalie-Detektion im Netzwerk kann das laut BSI verhindert oder begrenzt werden. Damit sei es zeitnah möglich, einen potenziell unerwünschten Datenabfluss zu erkennen. Hierfür muss der regulär anfallende Netzwerkverkehr sehr gut bekannt sein. Auf Basis eines festgelegten Normalzustands können Schwellenwerte gewählt werden, bei deren Über- oder Unterschreitung das System anschlägt.

5. Verschlüsselung: Daten werden auf möglichst vielen Systemen verschlüsselt, damit die erpressten Firmen selbst nicht mehr darauf zugreifen können. Der beste Schutz sind Backups und Datensicherung in einem Offline-Speicher, denn dann sind Daten auch im Falle eines Angriffs weiter verfügbar.

6. Reaktion: Firmen stehen vor der Herausforderung, ihre Systeme und Daten wiederherzustellen. Je nach Ausmaß muss dafür ein Übergangsbetrieb organisiert und der Vorfall an Kunden und Partner kommuniziert werden. Helfen kann hierbei ein IT-Sicherheitsdienstleister. Für das Worst-Case-Szenario, dass es einem Angreifer gelingt, alle Systeme im Netzwerk zu verschlüsseln, müssen KMU eine Notfallplanung für Notbetrieb und Wiederaufbau entwickelt haben. Das BSI rät sogar dazu, die Prozesse zur Reaktion und Wiederherstellung geschäftskritischer Systeme in regelmäßigen Abständen zu üben. Hilfreich ist es zudem, trotz aller Digitalisierungsbestrebungen Telefonnummern und Daten von wichtigen Kontaktpersonen in Papierform vorliegen zu haben.

Was Betriebe nicht tun sollten

Was kleinere und mittlere Betriebe nicht tun sollten: auf die Forderung der Kriminellen eingehen und das Lösegeld zahlen.

CHECKLISTE: MASSNAHMENKATALOG FÜR IT-NOTFÄLLE

Vorbereitung auf einen IT-Notfall:

- Beauftragte im Unternehmen für Informationssicherheit und Notfallmanagement bestimmen, nach Möglichkeit nicht in Personalunion. Beide arbeiten bei IT-Notfällen eng zusammen
- Sicherstellen, dass die individuellen und fallbezogenen Erstmaßnahmen im IT-Notfall vorliegen, unter anderem Meldewege im Unternehmen
- Zeitkritische Geschäftsprozesse und Assets im Rahmen eines strukturierten Prozesses identifizieren und Schutzmaßnahmen für diese priorisiert umsetzen
- Dienstleister suchen und kontaktieren, die bei IT-Notfällen geeignet unterstützen könnten. Mit IT-Dienstleistern klären, für welche IT-Vorfälle Unterstützung gewährt werden kann
- Liste mit allen Ansprechpartnern anfertigen und Vorabsprachen mit diesen hinsichtlich Erreichbarkeit, Verfügbarkeit und gegebenenfalls Service-Level-Agreement treffen
- Regeln zur Kommunikation nach innen und außen festlegen. Eine erfolgreiche Presse- und Öffentlichkeitsarbeit während eines IT-Notfalls kann einen Imageschaden erheblich begrenzen
- Falls möglich: aktive Überwachungsmaßnahmen für die IT implementieren, auch durch IT-Dienstleister machbar
- IT-Notfallszenarien jeglicher Art wie IT-Ausfälle oder Cyber-Angriffe üben und gesamtes Personal sensibilisieren
- Vertiefende Schulungen für Personen durchführen, die mit der Bewältigung von IT-Notfällen betraut sind
- Grundlegende Schutzmaßnahmen durchführen wie regelmäßige Patches und Sicherheitsupdates, Programme zum Schutz vor Schadsoftware sowie Firewalls, Änderung von Standard-Passwörtern in sichere, Zwei-Faktor-Authentisierung, regelmäßige Sicherheitskopien (Backups) der Daten und deren Wiederherstellung regelmäßig üben
- IT-Infrastruktur (unter anderem Netzplan) dokumentieren
- Restriktive Benutzerrechte an IT-Systemen, besonders privilegierte Benutzerkonten schützen, zum Beispiel durch Zwei-Faktor-Authentisierung
- Restriktiv bei der Vernetzung der IT-Systeme vorgehen
- Meldewege vorbereiten, um externen Meldepflichten während des IT-Notfalls fristgerecht nachzukommen

Bereitschaft:

- Sicherheitsstatus der IT-Systeme regelmäßig überprüfen
- Sicherstellen, dass alle Mitarbeiter den richtigen Ansprechpartner für IT-Notfälle kennen und handlungssicher sind
- Erreichbarkeit zu den relevanten Arbeitszeiten gewährleisten
- Bedenken, dass nicht jede Fehlfunktion von Hardware oder Software ein Cyber-Angriff ist. Gleichwohl kann der Ausfall eines IT-Systems auf einen Cyberangriff zurückzuführen sein

your123/stock.adobe.com

Prävention ist der beste Schutz gegen Cyberangriffe.

Bewältigung eines IT-Notfalls:

- Ruhe bewahren und sofort alle zur Bewältigung benötigten Ansprechpartner kontaktieren. Gegebenenfalls betroffene Nutzer über Beobachtungen und Aktivitäten befragen
- IT-Dienstleister kontaktieren, der bei der Bewältigung behilflich sein kann
- System-Protokolle, Log-Dateien, Notizen, Fotos von Bildschirminhalten, Datenträger und andere digitale Informationen sammeln und sichern, am besten, bevor auf den Systemen eine Analyse gestartet wird. Diese Daten sind im Fall einer forensischen Auswertung essenziell (Strafanzeige)
- Alle mit dem IT-Notfall im Zusammenhang stehenden Sachverhalte dokumentieren
- Gegebenenfalls mit der Zentralen Ansprechstelle für Cybercrime (ZAC) beim Landeskriminalamt Kontakt aufnehmen, um eine Anzeige zu erstatten
- Freiwillige Meldung an die Meldestelle der Allianz für Cyber-Sicherheit (ACS) prüfen
- Meldepflichten beachten: Datenschutz, KRITIS (kritische Infrastrukturen, zu denen auch Unternehmen aus Transport und Verkehr gehören)

Arbeitsgruppe deutscher Cyber-Sicherheitsorganisationen, bestehend aus: Bundeskriminalamt, Charter of Trust, Cyber Security Sharing and Analytics (CSSA), Deutscher Industrie- und Handelskammertag, eco – Verband der Internetwirtschaft, G4C German Competence Centre against Cyber Crime, Initiative Wirtschaftsschutz, Nationale Initiative für Informations- und Internet-Sicherheit, VOICE – Bundesverband der IT-Anwender, Allianz für Cyber-Sicherheit des BSI.

Davon rät das BSI ab. Viele Opfer lassen sich darauf ein in der Hoffnung, schnell wieder arbeitsfähig zu sein. Laut einer Umfrage von Bitkom haben hierzulande elf Prozent der Betriebe, die Opfer von Ransomware wurden, Lösegeld bezahlt. Es gibt indes laut BSI keine Garantie, dass die Cybererpresser die verschlüsselten Daten, die ja zudem prinzipiell als kompromittiert zu betrachten sind, tatsächlich wieder freigeben oder gestohlene Daten löschen. Auch kann das vom Angreifer gebotene Entschlüsselungstool fehlerhaft sein. Und nicht zuletzt, und das ist ein wichtiger Grund, macht sich eine Firma, die auf die Forderungen der Kriminellen eingeht, für einen zweiten Erpressungsversuch attraktiv. **mp/eh**