Die Gefahr lauert im Innern

Es ist höchste Zeit, die Sicherheit der eigenen **IT-Infrastruktur** in den Blick zu nehmen. Mögliche Schäden sind existenzbedrohend.

Cyberangriffe sind zu einer enormen Bedrohung für die deutsche Wirtschaft geworden. In seinem jüngsten Lagebericht beschrieb das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Situation als sehr ernst. Jedes zehnte Unternehmen sieht sich demnach in seiner Existenz bedroht.

Laut des Verbandes der deutschen Informations- und Telekommunikationsbranche (Bitkom) verursachten Cyberangriffe im Jahr 2021 in 86 Prozent der Unternehmen einen Schaden. Mit besonderer Wucht haben Ransomware-Angriffe die Wirtschaft erschüttern. In allen Branchen und Größen. Die Schäden durch Drohungen, verbunden mit dem Ausfall von Systemen oder der Störung von Betriebsabläufen, sind laut Bitkom seit 2019 um 358 Prozent gestiegen.

Es werden nicht nur Daten gestohlen. Die Angreifer erpressen die Unternehmen und fordern Schutzgeld. Kriminelle drohen, bestimmte Ressourcen gezielt zu überlasten – beispielsweise mit massenhaften Anfragen. Zuletzt waren 27 Prozent der Unternehmen im Land von solchen DDoS-Attacken betroffen.

Sicherheitslücke Mensch

Henry Georges, Mitarbeiter der Hamburger Zentralen Ansprechstelle Cybercrime (ZAC) beobachtet die fortlaufenden Angriffe auf Firmen und berät Unternehmen in IT-Sicherheitsfragen.

FOTOS: ADOBE STOCK

7 Gebote der Datensicherheit

Technische und organisatorische Maßnahmen der Kontrolle, die Datensicherheit in Unternehmen zu erhöhen

1. Zutrittskontrolle

Alle zu verarbeitenden Daten dürfen räumlich nicht frei zugänglich gemacht werden. Es muss eine ausreichende Sicherung von Gebäuden, Räumen und Endgeräten gegeben sein.

2. Zugangskontrolle

Unbefugte dürfen keine Datenverarbeitung in Betrieb nehmen oder verwenden können. Dies kann durch die Vergabe von Passwörtern gewährleistet werden.

3. Zugriffskontrolle

Wer kann und darf auf die Daten zugreifen? Es werden Regelungen festgelegt, dass nur berechtigte Personen Einblick in Daten erhalten oder nutzen können.

4. Weitergabekontrolle

Um den Datenschutz und die Datensicherheit zu gewährleisten, sollte Datenweitergabe vorhersehbar und kontrollierbar gemacht werden.

5. Auftragskontrolle

Ist nur dann relevant, wenn Daten externer Dienstleister verarbeitet werden.

6. Verfügbarkeitskontrolle

Personenbezogene Daten werden vor zufälliger Zerstörung und Verlust geschützt – beispielsweise durch Stromausfälle.

7. Trennungsgebot

Daten müssen anhand ihres Zweckes getrennt werden. So wird eine leichtere Zuordenbarkeit der Daten gewährleistet. Zum anderen erfüllt dies das datenschutzrechtliche Grundprinzip der ausschließlich zweckgebundenen Nutzung von Daten.

Quelle: Uni Mainz

Der Experte nennt ein unterschätztes Problem: „Mitarbeiter sind die größte Sicherheitslücke."

Sie sind es oft aus Unwissenheit. Wer unvorsichtig E-Mails oder deren Anhänge öffnet, kann dazu beitragen, dass sich eine Schadsoftware im Firmennetzwerkinstalliert. Was dann folgen kann, ist das Verschwinden oder Verschlüsseln von Daten. Diese werden von den Tätern den Unternehmen zum Rückkauf angeboten.

Hierfür übersenden die Täter den Unternehmen oftmals einen kleinen Teil der Daten oder publizieren diese im Darknet, um zum einen den Druck zu erhöhen und zum anderen nachzuweisen, dass sie im Besitz der Daten sind. Sollte das Unternehmen die Daten nicht zurückkaufen wollen, wird damit gedroht, die gesamten Daten im Darknet zu veröffentlichen oder zu verkaufen.

Oftmals schützen Mitarbeiter Passwörter nicht oder verschicken sensible Daten an den Chef, obwohl die Anfrage (CEO-Fraud) nicht von ihm kam. Zur Begehung dieses Deliktes erstellen die Täter eine E-Mail-Adresse mit dem Namen des Geschäftsführers eines Unternehmens. Diese E-Mail-Adresse wird genutzt, um eine Person aus der Buchhaltung des Unternehmens anzuschreiben und eine finanzielle Transaktion zu veranlassen.

Henry Georges. Experte für IT-Sicherheit der Hamburger Zentralen Ansprechstelle Cybercrime der Polizei.

Als seltener auftretendes Problem beschreibt Henry Georges jene Mitarbeiter, die Betriebs- und Geschäftsgeheimnisse verraten, weil sie kündigen, entlassen wurden oder unzufrieden sind.

Die einen nutzen betriebsinterne Daten bei einem neuen Arbeitgeber. Georges empfiehlt vorbeugend: Jeder Mitarbeiter sollte nur für die Daten Zugriff erhalten, die er für seine persönliche Tätigkeit benötigt. In anderen Fällen sind Mitarbeiter der IT oder von IT-Dienstleistern eine Gefahr. Sie schaffen sich Möglichkeiten des weiteren Zugriffs auf das Unternehmensnetzwerk. So können sie auch nach Verlassen einer Firma auf deren Daten zuzugreifen, sie verändern, weitergeben oder löschen.

Oftmals werden in Unternehmen im Bereich der Administration jahrelang die gleichen internen Standardpasswörter verwendet, welche auch nach dem Ausscheiden von Mitarbeitern nicht geändert werden. „Dies kommt häufiger vor, insbesondere wenn arbeitsrechtliche Auseinandersetzungen vorhanden sind", so Georges. | JES

Förderung: *Wer seine Datensicherheit verbessern will, erhält Fördermittel.* *(weitere Infos auf Seite 6)*

8 Schritte zur Umsetzung von Datensicherheit in Unternehmen

1. Sensibilisierung und Schulung

Jeder im Unternehmen muss für das Thema sensibilisiert und geschult werden. Denn so gut wie jeder Mitarbeiter eines Unternehmens hat an irgendeinem Punkt im Arbeitsablauf mit personenbezogenen Daten zu tun. Neben dem Schaffen eines generellen Bewusstseins für das Thema Datensicherheit, ist auch eine eingehende Schulung nötig.

2. Verantwortlichkeiten festlegen

Rechtlich ist die Geschäftsführung für den Datenschutz zuständig. Für die praktische Umsetzung sollte ein fester Ansprechpartner festgelegt sein oder ein Datenschutzbeauftragter bestellt werden.

3. Transparente Infrastruktur

Es muss klar sein, wo Daten sich befinden.

4. Daten verschlüsseln

Daten sollten im besten Falle stets verschlüsselt werden, um im Ernstfall einen Schaden gering zu halten.

5. Programme aktuell halten

Verschaffen Sie sich einen Überblick über die in ihrem Unternehmen eingesetzten Programme und sorgen Sie dafür, dass Sicherheitsupdates so rasch wie möglich eingespielt werden – oder nutzen Sie die häufig angebotene automatische Aktualisierungsfunktion.

6. Passwort-Sicherheit erhöhen

Nicht 123456 ist sicher. Durch die Wahl von sicheren Passwörtern und eine vernünftige Verwaltung kann die Cyber-Sicherheit im Unternehmen erheblich erhöht werden.

7. Daten regelmäßig sichern

Legen Sie Sicherungskopien Ihrer Daten an und testen Sie Backups regelmäßig. Damit sind Sie auf der sicheren Seite, wenn Computer von Viren befallen oder gestohlen werden. Sie können Schäden durch Erpressungs-Trojaner (Ransomware) vermeiden.

8. Den Ernstfall proben

Wer darf entscheiden, ob alle Computer heruntergefahren oder der Webshop vom Netz genommen wird? Wer ist im Notfall außerhalb der Bürozeiten erreichbar, auch ohne funktionierendes Netzwerk?

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)