Video: Mit Roboterhund „Spot“ im Einsatz >
< Video: Taschendiebe auf Beutezug

Cybercrime – Angriffe auf Unternehmen

Cyberkriminalität ist eine massive Gefahr für die Wirtschaft

Unternehmen müssen sich mehr denn je gegen Cyberangriffe schützen

© VideoFlow, stock.adobe.com

Diebstahl, Spionage, Sabotage: Cyberangriffe auf Unternehmen in Deutschland nehmen zu und die Täter agieren hoch professionell. Die Schäden belaufen sich laut einer Studie des Branchenverbands Bitkom aus dem Jahr 2021 jährlich auf mehr als 220 Milliarden Euro. Unternehmen sollten die Bedrohung nicht unterschätzen.

Cyberangriffe auf deutsche Unternehmen

Neun von zehn Unternehmen waren 2020/2021 laut der Bitkom-Studie von Cyberangriffen betroffen. Für die repräsentative Umfrage wurden mehr als 1.000 Unternehmen quer aus allen Branchen befragt. Am häufigsten sind Erpressungsvorfälle, verbunden mit dem Ausfall von IT- und Produktionssystemen sowie der Störung von betrieblichen Abläufen, etwa durch Ransomware-Angriffe. Jedes zehnte Unternehmen (9 Prozent) sieht sogar seine geschäftliche Existenz durch Cyberattacken bedroht. „Die Gefahr, Opfer eines Cyberangriffs zu werden, ist für die Unternehmen leider massiv gestiegen. Die verursachten Schäden haben sich im Vergleich zu den Vorjahren 2018/2019 mehr als vervierfacht“, sagt Sebastian Artz, Referent für Informationssicherheit und Sicherheitspolitik beim Branchenverband Bitkom. Zwar sei die Ausschaltung der Schadsoftware Emotet durch das Bundeskriminalamt zum Jahresbeginn 2021 ein wichtiges Signal an die Branche gewesen, dass die Strafverfolgung auch im Cyberspace funktioniert. „Jedoch ergeben sich im Zuge der digitalen Transformation für Kriminelle immer neue Einfallstore, über die sich die Unternehmen dringend Gedanken machen müssen“, so der Experte. Viele Unternehmen

hätten als Reaktion auf die verschärfte Bedrohungslage bereits verstärkt in ihre IT-Sicherheit investiert. Aber auch von der Politik erwarten sie entschlossenes Handeln: Jeweils 99 Prozent der Unternehmen fordern ein stärkeres Vorgehen gegen ausländische Cyberangriffe, eine stärkere EU-weite Zusammenarbeit bei Cybersicherheit und einen besseren Austausch zwischen Staat und Wirtschaft zu IT-Sicherheit.

Wer ist gefährdet?

Besonders groß ist die Gefahr durch Cyberangriffe vor allem für kleine und mittelständische Unternehmen, meint Sebastian Artz: „Leider erkennen viele von ihnen gar nicht den Wert, der in ihrem Unternehmen schlummert und denken: Bei mir gibt es für Kriminelle doch sowieso nichts zu holen. Aber damit liegen sie völlig falsch“, warnt der Experte. Zahlreiche Firmen verfügen über Patente und wichtiges geistiges Eigentum. Das weckt Begehrlichkeiten. Außerdem hat es durch die Corona-Pandemie in nahezu allen Unternehmensbereichen einen kräftigen Schub bei der Digitalisierung der Arbeits- und Geschäftsprozesse gegeben. „Das Arbeiten im Home Office und die Migration großer Datenmengen in die Cloud eröffnen viele neue Sicherheitsfragen, die es dringend mitzudenken gilt“, mahnt Artz. In der Bitkom-Studie gaben 59 Prozent der Unternehmen mit Home Office an, es habe seit Pandemiebeginn IT-Sicherheitsvorfälle gegeben, die auf die Heimarbeit zurückzuführen seien. In 24 Prozent dieser Unternehmen sei das sogar häufig geschehen.

Anzeichen für einen Hack

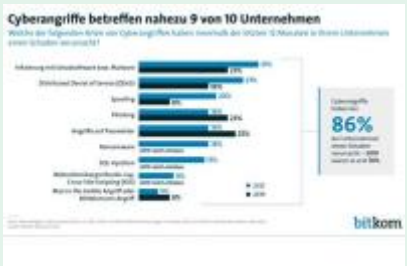
Häufig merken Unternehmen gar nicht, dass sie Opfer einer Cyberattacke geworden sind. Dies können Anzeichen eines Angriffes sein: • Ein unbekannter Nutzer hat sich ins System eingeloggt • Die Rechner werden langsamer und reagieren zeitverzögert • Dateien verschwinden oder lassen sich plötzlich nicht mehr öffnen • In kurzer Zeit erreichen viele Datenpakete das System • Rechner stürzen unvermittelt ab oder starten sich von selbst neu • Eine Lösegeld-Bildschirm-Meldung erscheint • E-Mails mit ungewöhnlichen Anhängen oder mit Aufforderungen, ungewohnte Dinge zu tun, erscheinen im Maileingang

Wie können sich Unternehmen schützen?

Als ganzheitliches Konzept für Informationssicherheit hat sich das IT-Grundschutzkompendium des Bundesamtes für Sicherheit in der Informationstechnik (BSI) etabliert. Es ist anwendbar für alle Institutionen, die in Zeiten der Digitalisierung ihre IT-Systeme und Datennetze und damit ihre Geschäfts- oder Verwaltungsprozesse nach dem aktuellen Stand der Technik absichern wollen. Informationen zu Schutzmaßnahmen speziell für kleine und mittelständische Unternehmen bietet die „Allianz für Cybersicherheit“ unter www.allianz-fuer-cybersicherheit.de. „Getreu dem Motto „Netzwerke schützen Netzwerke“ haben sich dort bereits mehr als 5.000 Unternehmen aus ganz Deutschland zusammengetan – Cybersicherheit gelingt nur gemeinsam“, betont Artz. Zu den kostenfreien Unterstützungsangeboten zählen Checklisten für IT-Sicherheitsvorfälle, Weiterbildungsangebote und aktuelle Informationen über Bedrohungen. Nützliche Informationen bietet auch das Bundeskriminalamt in seiner Broschüre „Handlungsempfehlungen für die Wirtschaft“ und stellt darüber hinaus eine Liste mit weiteren Anlaufstellen zum IT-Grundschutz und zur Sicherheit in Unternehmen zur Verfügung.

Im Ernstfall zählt jede Sekunde

„Die Zeitspanne von der Entdeckung einer Sicherheitslücke bis zum ersten Angriff wird immer kürzer. Daher sollte man ein gut aufgestelltes Informationssicherheitsmanagement haben, um im Ernstfall möglichst schnell und auf alle Eventualitäten reagieren zu können“, erklärt Sebastian Artz. „Oft haben Unternehmen kaum Notfallprozesse aufgesetzt und lassen so im Ernstfall wertvolle Zeit verstreichen.“ Dabei können die Schäden eines Vorfalls beträchtlich werden: Datenverluste, Produktionsausfälle, Klagen wegen des



Die Bitkom-Studie quantifiziert die Methoden der Cyberangriffe auf Unternehmen

© Bitkom e. V.

Diebstahls von personenbezogenen Daten, hohe Lösegeldforderungen: Der finanzielle Schaden kann gerade für kleinere Unternehmen existenzbedrohend sein. „Unternehmer sollten das Thema Cybersicherheit nicht als lästigen Kostenpunkt betrachten, sondern als Qualitätsmerkmal und Existenzgrundlage ihres Betriebs. Eine gute IT-Sicherheitsstrategie kann ein Wettbewerbsvorteil sein, wenn man in die Zukunft blickt“, betont Artz.

Wo findet man schnelle Hilfe?

Nach einem Vorfall liegen in betroffenen Unternehmen häufig die Nerven blank. Das ist auch völlig verständlich, denn die Auswirkungen sind in vielen Fällen verheerend und es vergehen meist Tage, bis wieder alle Systeme ans Laufen gebracht wurden. Auf der Website des BSI finden Unternehmen eine Liste mit qualifizierten IT-Dienstleistern, um sich im Ernstfall schnell Hilfe zu holen. „Unternehmen sollten präventiv tätig werden und sich in Ruhe und mit Augenmaß nach einem passenden und qualitativ guten IT-Dienstleister umschauen. Im Ernstfall ist keine Zeit für Angebotsvergleiche“, berichtet Artz. Um die Beschäftigten auf IT-Vorfälle in Zukunft besser vorzubereiten, bietet das BSI auch die IT-Notfallkarte „Verhalten bei IT-Notfällen“ an. Die Notfallkarte soll an zentralen Orten platziert werden und – ähnlich wie das Hinweisschild „Verhalten im Brandfall“ – dafür sorgen, dass die Beschäftigten bei Notfällen im IT-Bereich sofort richtig handeln.

Prävention auf allen Ebenen

Weil IT-Infrastrukturen auch existentiell für das Funktionieren von Staat, Gesellschaft und Wirtschaft sind, gibt es die unterschiedlichsten Präventionsstellen auf EU-, Bundes- und Länderebene. Auf EU-Ebene ist das Europäische Zentrum zur Bekämpfung der Cyberkriminalität für die grenzübergreifende Strafverfolgung von Computerkriminalität in Den Haag zuständig. In Deutschland sind auf Bundesebene alle wichtigen Stellen für das IT-Krisenmanagement unter dem Dach des BSI vereint. Darunter das CERT-Bund, das IT-Lage- und Analysezentrum, das IT-Krisenreaktionszentrum und das Nationale Cyber-Abwehrzentrum (NCAZ) des Bundeskriminalamtes. Auf Länderebene bieten die Zentralen Ansprechstellen Cybercrime (ZAC) der Landeskriminalämter den Unternehmen fachliche Unterstützung bei Cybervorfällen an. (AL/WL, 27.08.2021)

Sebastian Artz, Referent Informationssicherheit & Sicherheitspolitik, Bitkom e. V.

© Bitkom e. V.

Folgende Artikel könnten Sie auch interessieren:

- Markierung von Wertgegenständen durch künstliche DNA
- Schwarzarbeit sorgt für Milliardenschaden
- Cyberversicherungen
- CEO-Fraud auf dem Vormarsch
- Wanzen im Wohnzimmer
- Gefälschte Stellenanzeigen
- Betrug beim Online-Gaming

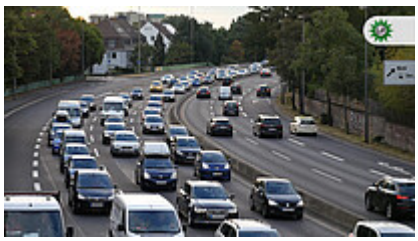
Alle Artikel dieser Kategorie

Weitere Präventionsvideos

Der Alkohol-Parcours für Schülerinnen und Schüler

Video: Interaktive Suchtprävention

Die erste größere Party, das erste Mal Alkohol trinken: Um...[mehr erfahren]



Mit Christian Kellner, Hauptgeschäftsführer des Deutschen Verkehrssicherheitsrat

Video: Mehr Sicherheit durch Fahrerassistenzsysteme

Immer mehr Autos verfügen über moderne Fahrerassistenzsysteme. Wie...[mehr erfahren]

Mit Carl Philipp Rudolfi, Erste-Hilfe-Ausbilder beim Malteser Hilfsdienst

Video: Erste Hilfe – So handeln Sie im Notfall richtig!

In diesem Video informiert Carl Philipp Rudolfi vom Malteser...[mehr erfahren]

Mit Peter Werkmüller, Polizeiliche Beratungsstelle Düsseldorf

Video: Tipps zum Einbruchschutz

In diesem Video gibt Hauptkommissar Peter Werkmüller von der...[mehr erfahren]

Präventionstheater für Seniorinnen und Senioren

Video: Ausgetrickst – nicht mit uns!

Ob der klassische Enkeltrick oder der falsche Handwerker: Seniorinnen...[mehr erfahren]

© Verlag Deutsche Polizeiliteratur

Cookie Einstellungen

□Statistiken
□Essentiell

Wir nutzen Cookies auf unserer Website, die in unserer Datenschutzerklärung beschrieben sind. Wir verwenden anonyme Statistiken, um unsere Website zu verbessern. Bitte unterstützen Sie unsere wichtige Präventionsarbeit und akzeptieren Sie alle Cookies. Vielen Dank!

AblehnenAlle akzeptieren