Firmen CyberSchutz

ZURICH

Wenn Ihre Firewall nicht hält, was sie verspricht

Firmen CyberSchutz gegen digitale Risiken

Alle drei Minuten erfolgt laut Verfassungsschutz ein Cyber-Angriff auf ein Unternehmen in Deutschland. Dadurch entstand laut einer Bitkom Studie für die gesamte deutsche Wirtschaft in 2019 ein Schaden von ca. 100 Mrd. Euro. Jedes zweite mittelständische Unternehmen in Deutschland war bereits Opfer eines Angriffs auf die eigene IT – Tendenz steigend.

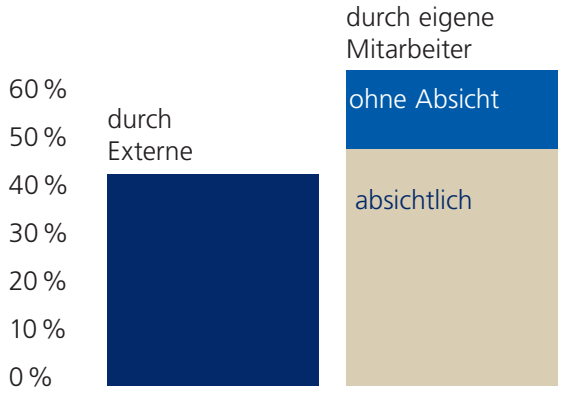
Top 5 der häufigsten Cyber-Attacken

- **Botnetze**
  Verbreitung von Schad-programmen durch einen System-Verbund von Rechnern
- **Man-In-The-Middle**
  Abfangen oder Unterbrechen einer Kommunikation zwischen zwei Systemen
- **Diebstahl**
  von Daten und Identitäten
- **Social Engineering**
  Preisgeben vertraulicher Informationen durch Manipulation von Menschen
- **Denial-of-Services-Attacken**
  Dienst, der normalerweise funktioniert, ist nicht mehr abrufbar

Zu den materiellen Einbußen, die den Unternehmen durch Eigenschäden (z. B. Betriebsunterbrechung, Forensik- oder Wiederherstellungskosten) oder Drittschäden (z. B. infolge von Daten-schutzverletzungen) entstehen, kommt der Imageverlust, der sich finanziell nur schwer erfassen lässt.

Cyberkriminalität hat viele Formen. Es gibt spektakuläre Fälle, in denen Hacker komplette Anlagen stilllegen oder große Geldbeträge stehlen. Meistens läuft eine Cyberattacke jedoch im Stillen ab – besonders dann, wenn es sich um Industriespionage oder den Diebstahl personen-bezogener Daten handelt. Experten schätzen, dass es im Schnitt 200 Tage dauert, bis ein mittelständisches Unter-nehmen bemerkt, dass sein Computer-system gehackt wurde. Deshalb ist es besonders wichtig, Sicherheitslücken zu schließen, um einem Cyberangriff vorzubeugen. Mindestens genauso wichtig ist es, Prozesse zu schaffen, die helfen, Cyberkriminalität möglichst früh zu entdecken und den Schaden zu begrenzen. Mit der Datenschutz-grundverordnung (DSGVO) zwingt der Gesetzgeber Unternehmen, sich mit diesem Aspekt der Internetkriminalität stärker auseinanderzusetzen.

Weltweite Cyberattacken nach Verursacher



Kleine Ursache – große Wirkung

Daten sind das Herz auch Ihres Unternehmens. Und sie werden immer wichtiger. Ein Verlust oder Missbrauch Ihrer Unternehmensdaten kann Ihre Existenz gefährden. Schützen Sie Ihr Unternehmen gegen die Folgen von Cyberkriminalität.

Schadenbeispiel Büro

Der Server einer gemeinnützigen Stiftung wird gehackt. Auf dem Server befinden sich ca. 1.500 Datensätze mit den Adressdaten der Spender. Die Daten werden kopiert und zum Teil zerstört, der Newsletter der Stiftung wird manipuliert.

Rechtsanwaltskosten	30.000 EUR
Kosten für Benachrichtigung an Spender	15.000 EUR
Forensische Untersuchungen	50.000 EUR
Wiederherstellungskosten	25.000 EUR
Schadenhöhe	**120.000 EUR**

Schadenbeispiel Rechtsanwalt

Durch die E-Mail eines Mandanten wird ein Virus in das EDV-System einer Anwaltskanzlei eingeschleust. Ein Mitarbeiter öffnet den Anhang einer E-Mail. Der darin befindliche Virus verschlüsselt alle Daten auf den Computern und iPads des Büros. Für die Wiederherstellung und Nichtveröffentlichung der Daten wird Lösegeld gefordert. Die Wiederherstellung der Systeme dauert mehrere Tage, in denen im Büro nicht gearbeitet werden kann.

Kosten für Benachrichtigung der Kunden	20.000 EUR
Wiederherstellungskosten	30.000 EUR
Betriebsunterbrechungskosten	10.000 EUR
Lösegeldzahlung	50.000 EUR
Schadenhöhe	**110.000 EUR**

Die Lösung: Firmen CyberSchutz

Firmen CyberSchutz schützt Sie umfassend vor den finanziellen Folgen von Datenverlusten und Cyberattacken.

Für eine lückenlose Absicherung Ihres Unternehmens empfehlen wir Ihnen ergänzend:

- D&O Entscheiderhaftpflicht
- Vertrauensschadenversicherung
- Firmen ElektronikSchutz

Glossar

Advanced Persistent Threat (Apt)
„Advanced Persistent Threats" (APT) sind zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netz verschafft und diesen in der Folge auf weitere Systeme ausweitet. Hierzu sind hohe Ressourceneinsätze und erhebliche technische Fähigkeiten auf Seiten der Angreifer nötig.

Botnetze
Als „Botnetz" wird ein Verbund von Rechnern (Systemen) bezeichnet, die von einem fernsteuerbaren Schadprogramm (Bot) befallen sind. Die betroffenen Systeme werden vom Botnetz-Betreiber mittels eines Command-and-Control-Servers (C&C-Server) kontrolliert und gesteuert.

Backdoor
Bildlich gesprochen: Eine Hintertür, um sich Zugang zu einem geschützten Bereich zu verschaffen. Man geht also nicht durch die gesicherte und verschlossene Haustür, sondern geht einmal um das Haus herum und kommt herein beziehungsweise bricht ein.

Cache Poisoning
Unter „Cache Poisoning" versteht man das Einschleusen von manipulierten Daten in einen Zwischenspeicher „Cache", der dann von anderen Anwendungen oder Diensten genutzt wird. Ein Angreifer kann so z. B. allgemein die Routen von Datenpaketen ändern oder gezielt Anfragen für Webseiten einer Bank auf eine gefälschte Seite umleiten.

DoS-Attacke
Eine künstlich herbeigeführte Überlastung eines Webservers oder Datennetzes, gesteuert von Cyberkriminellen. Im Gegensatz zu einer einfachen Denial-of-Service-Attacke („DoS") haben Distributed-Denial-of-Service-Attacken („DDoS") eine immense Schlagkraft. Mehrere Computer greifen dabei gleichzeitig und im Verbund („Botnetze") eine Webseite oder eine ganze Netzinfrastruktur an. Dies kann sehr schnell zum Ausfall der Server führen.

Fuzzing
„Fuzzing" ist eine automatisierte Testmethode für Software, bei der ein Programm eine Vielzahl automatisch generierter Eingabedaten verarbeiten muss, ohne dabei eine Fehlfunktion zu zeigen. Findet ein Hacker durch Fuzzing ein Eingabemuster, das eine Fehlfunktion erzeugt, muss überprüft werden, ob sich der gefundene Fehler als Sicherheitslücke ausnutzen lässt.

HTTP
Das „Hypertext Transfer Protocol" HTTP ist im Gegensatz zu HTTPS nicht verschlüsselt. Daten, die mit diesem Protokoll übertragen werden, können leicht von Dritten gelesen oder manipuliert werden. Wenn Sie schützenswerte Informationen über das Internet austauschen, ist eine verschlüsselte Verbindung (z. B. HTTPS) sehr empfehlenswert.

IT-Forensik
Die „IT-Forensik" befasst sich mit der Untersuchung, Analyse und Aufklärung von Sicherheitsvorfällen im Zusammenhang mit IT-Systemen.

Keylogger
Als „Keylogger" wird Hard- oder Software zum Mitschneiden von Tastatureingaben bezeichnet. Sie zeichnen alle Tastatureingaben auf, um sie möglichst unbemerkt an einen Angreifer zu übermitteln. Dieser kann dann aus diesen Informationen für ihn wichtige Daten, wie z. B. Anmeldeinformationen oder Kreditkartennummern filtern.

Malware
Damit bezeichnet man Computerprogramme, die bewusst unerwünschte und gegebenenfalls schädliche Funktionen ausführen. Malware ist damit ein Oberbegriff, der u. a. das Computervirus umfasst. Der Begriff des Virus ist älter und häufig nicht klar abgegrenzt. So ist die Rede von Virenschutz, womit viel allgemeiner der Schutz vor Schadsoftware jeglicher Art gemeint ist. Ein typischer Virus verbreitet sich, während die heute gängigen Schadprogramme die Struktur von Trojanischen Pferden zeigen, deren primärer Zweck nicht die Verbreitung, sondern die Fernsteuerbarkeit ist.

Nicknapping
Personen treten im Internet mit ihrem realen Namen oder unter der Verwendung eines Pseudonyms oder Nicknames auf. Als „Nicknapping" bezeichnet man einen Cyberangriff, bei dem der Angreifer unter einem bekannten Namen oder Pseudonym auftritt. Dadurch versucht der Angreifer gegenüber Dritten den Eindruck zu erwecken, er sei der eigentliche/ursprüngliche Inhaber des Namens oder des Pseudonyms. Gelingt dies, kann der Angreifer in begrenztem Maße als der eigentliche/ursprüngliche Inhaber agieren.

Phishing
Beim „Phishing" wird z. B. mittels gefälschter E-Mails und/oder Webseiten versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen. Wird diese Manipulation vom Opfer nicht erkannt und die Authentizität einer Nachricht oder Webseite nicht hinterfragt, gibt das Opfer seine Zugangsdaten u. U. selbst unwissentlich in unberechtigte Hände.

Ransomware
Als „Ransomware" werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch: „ransom") wieder freigeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.

Spyware
Als „Spyware" werden Programme bezeichnet, die heimlich, also ohne darauf hinzuweisen, Informationen über einen Benutzer bzw. die Nutzung eines Rechners sammeln und an den Urheber der Spyware weiterleiten. Spyware gilt häufig nur als lästig, es sollte aber nicht übersehen werden, dass durch Spyware auch sicherheitsrelevante Informationen wie Passwörter ausgeforscht werden können.

Trojanisches Pferd
Ein „trojanisches Pferd", oft auch (fälschlicherweise) kurz „Trojaner" genannt, ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Ein trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogramms für seine Installation durch den Benutzer.

Viren
Klassische Form von Schadsoftware, die sich selbst verbreitet und unterschiedliches Schadpotenzial in sich tragen kann (keine Schadfunktion bis hin zum Löschen der Daten auf einer Festplatte). „Viren" treten in Kombination mit einem Wirt auf, z. B. einem infizierten Dokument oder Programm.

Zero-day-exploit
Die Ausnutzung einer Schwachstelle, die nur dem Entdecker bekannt ist, charakterisiert man mit dem Begriff „Zero-Day-Exploit". Die Öffentlichkeit und der Hersteller des betroffenen Produkts merken in der Regel erst dann die Schwachstelle, wenn Angriffe entdeckt werden, die auf dieser Schwachstelle basieren. Der Hersteller hat keine Zeit, die Nutzer vor den ersten Angriffen zu schützen.

Firmen CyberSchutz – unsere Antwort auf Ihre IT-Risiken

Krisenmanagement und Soforthilfe

Ihr Ansprechpartner koordiniert und beauftragt alle Maßnahmen, die zur Bewältigung eines Cyberangriffs erforderlich sind.

Cyber-Eigenschaden

Ihr Unternehmen ist für den Fall einer Cyberattacke auf das Computersystem, wie z. B. DoS-Angriffe, Einführung von Malware, Veränderung oder Zerstörung von computergespeicherten Daten und Programmen, Beschädigung oder Zerstörung von Hardware, Systemunterbrechung und einer damit verbundenen Betriebsunterbrechung, versichert.

Cyber-Haftpflicht

Versichert Ihr Unternehmen gegen Haftpflichtansprüche Dritter sowie Vermögensschäden durch illegale Vervielfältigung, Verbreitung, Veröffentlichung oder Bekanntmachung von vertraulichen oder personenbezogenen Informationen.

Cyber-Erpressung

Ihr Unternehmen ist bei einer Cyber-Erpressung in Form einer Drohung, das Computersystem durch einen DoS-Angriff zu blockieren, mit einer Malware zu infizieren, sich durch unbefugten Gebrauch des Computersystems Zugang zu personenbezogenen Daten oder anderen geschäftlich relevanten Vertraulichkeiten zu verschaffen und zu entwenden, versichert.

Cyber-Betrug (optional)

Versichert ist Ihr Unternehmen gegen den Verlust von Geld oder Wertpapieren durch einen Cyber-Betrug (z. B. durch Eingriffe in die Buchhaltung).

Zurich Gruppe Deutschland
Deutzer Allee 1
50679 Köln
www.zurich.de

212811080 2101

ZURICH®