Sich bei einer Straftat richtig verhalten

Reagieren Sie sofort bei Verdacht

Bei einem Verdacht auf eine Cyberattacke sammeln Sie alle Informationen zum Vorfall und lassen diese aufzeichnen. Halten Sie sich dabei an die im Unternehmen festgelegten Meldewege. Lassen Sie eine identische Kopie des betroffenen Systems erstellen, um den Schaden abzuschätzen, die Schwachstellen zu identifizieren oder den Angreifer zurückzuverfolgen. Prüfen Sie gleich, ob Sie dafür die Polizei einschalten. Denn die Kopie des betroffenen Systems sollte möglichst von anerkannten Forensikern der Polizei erstellt werden. Dadurch können zugleich Spuren und Hinweise gesichert werden. Nutzen Sie für die Kontaktaufnahme nicht das betroffene System. Ist bereits ein Schaden eingetreten, dokumentieren Sie alle damit zusammenhängenden Ereignisse (z. B. Anrufe, E-Mails, Systemstörungen, Logdaten).

Melden Sie den Angriff früh der Polizei

Empfehlenswert ist es sich an eine Zentrale Ansprechstelle Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft (ZAC) zu wenden. Diese sind in den Landeskriminalämtern oder beim Bundeskriminalamt eingerichtet. Eine Übersicht der Ansprechstellen gibt es unter www.polizei-beratung.de/zac oder unter www.polizei.de Grundsätzlich nimmt jede Polizeidienststelle eine Anzeige entgegen.

Arbeiten Sie mit der Polizei zusammen

Bei einem strafbaren Angriff auf Ihre IT-Infrastruktur wird die Polizei alle notwendigen Ermittlungsmaßnahmen mit Ihrem Unternehmen abstimmen. Dabei ist sie immer bemüht, die Unternehmensabläufe so wenig wie möglich zu beeinträchtigen. Bei ihren Ermittlungen geht die Polizei sensibel vor und behandelt Ihre Angaben im gesetzlichen Rahmen vertraulich. Nur durch eine vertrauensvolle Kooperation lassen sich Gegenmaßnahmen immer weiter verbessern, Angreifer konsequent verfolgen und Unternehmen dauerhaft vor neuen Angriffen schützen.

Beratung und Hilfe einholen

Dieses Faltblatt der Polizei vermittelt nur grundlegende Empfehlungen, ohne Anspruch auf Vollständigkeit. Vertiefende Informationen, rechtliche Rahmenbedingungen sowie konkrete Schutzmöglichkeiten sind auf den folgenden Internetseiten zu finden.

- Bundesamt für Sicherheit in der Informationstechnik: www.bsi.bund.de
- Materialien zum IT-Schutz: www.allianz-fuer-cybersicherheit.de
- Cybercrime – Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime: www.bka.de
- Wirtschaftsschutz – Gebündelte Informationen der Initiative Wirtschaftsschutz: www.wirtschaftsschutz.info
- Ratgeber für Unternehmen: www.sicher-im-netz.de/
- Informationen rund um das Thema Gefahren im Internet finden Sie auch unter: www.polizei-beratung.de/gefahren-im-internet

Informationen zum Thema Schutz vor Cyberangriffen sowie IT-Sicherheit und vorbeugende Maßnahmen erhalten Sie kostenlos bei den (Kriminal-)Polizeilichen Beratungsstellen sowie im Internet unter:
www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet.html

OSCAR CHARLIE

Mit freundlicher Empfehlung

(00V)150.2016.08

HERAUSGEBER:
PROGRAMM POLIZEILICHE KRIMINALPRÄVENTION DER LÄNDER UND DES BUNDES
Zentrale Geschäftsstelle
Taubenheimstraße 85, 70372 Stuttgart

Wir wollen, dass Sie sicher leben. Ihre Polizei

www.polizei-beratung.de

Sicherheit im digitalen Alltag

Schutz vor Cyberangriffen

IT-Sicherheit für kleine und mittlere Unternehmen

Wir wollen, dass Sie sicher leben. Ihre Polizei

Kompetent. Kostenlos. Neutral.

Die Gefahr erkennen

Für Cyberkriminelle sind Angriffe auf die Wirtschaft ein lukratives Geschäft. Doch nicht nur Weltkonzerne werden Opfer von Datenklau, Computersabotage oder Computerbetrug, sondern auch immer mehr kleine und mittlere Unternehmen (KMU). In einer repräsentativen Studie gibt fast die Hälfte der befragten Unternehmen an, Opfer eines Cyberangriffs geworden zu sein. Jedoch haben nur 20 Prozent der Betroffenen den Angriff auch an staatliche Stellen gemeldet (BITKOM 2015).

Die Cyberkriminellen haben es nicht nur auf neue Entwicklungen oder Unternehmensinterna abgesehen. Oft wollen sie dem Unternehmen finanziell schaden oder das Unternehmensimage negativ beeinflussen.

Cyberangriffe werden ermöglicht durch:

1. Technische Mängel
2. Menschliches Fehlverhalten
3. Organisatorische Mängel

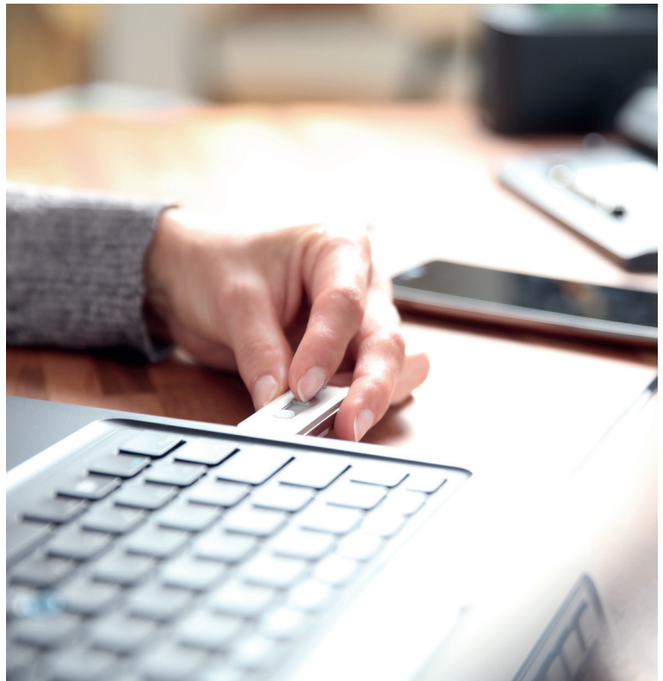
Mitarbeiter spielen bei der IT-Sicherheit eine große Rolle. Sie können durch richtiges Verhalten Cyberangriffe verhindern. Aber Mitarbeiter, Geschäftspartner sowie andere Dienstleister können auch ein großes Risiko für Cyberangriffe darstellen, z. B. wenn sie Kundendaten kopieren oder sich mit Unternehmenswissen selbstständig machen. Auch ein gestohlenes Laptop oder der verlorene USB-Stick mit Firmeninfos ermöglichen Cyberangriffe. Leichtsinniger Umgang der Mitarbeiter mit Firmendaten beispielsweise in sozialen Netzwerken bietet ebenfalls eine gute Grundlage für professionelle Angreifer.

Schutz vor Angriffen

Insgesamt betrachtet sind Cyberangriffe häufig eine Kombination aus technischem Mangel und menschlichem Fehlverhalten. Aus diesem Grund sollten in einem Unternehmen technischer Schutz mit der Sensibilisierung der handelnden Personen Hand in Hand gehen.

DELIKTE IM BEREICH CYBERCRIME

- Ausspähen von Daten (§ 202a StGB)
- Abfangen von Daten (§ 202b StGB)
- Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB)
- Datenhehlerei (§ 202d StGB)
- Computerbetrug (§ 263a StGB)
- Datenveränderung (§ 303a StGB)
- Computersabotage (§ 303b StGB)



Schutzmaßnahmen ergreifen

Um grundlegende Sicherheitslösungen zum Schutz vor Cyber-Attacken zu entwickeln, sollte die Unternehmensleitung folgende Punkte in ihre Überlegungen einbeziehen:

- Entwickeln und fördern Sie ein Sicherheitsverständnis in allen Bereichen Ihres Unternehmens.
- Analysieren und definieren Sie schützenswerte Bereiche im Unternehmen.
- Achten Sie auf rechtliche Rahmenbedingungen (z. B. § 9 des Bundesdatenschutzgesetzes bei der Verarbeitung personenbezogener Daten).
- Entwickeln Sie eine Sicherheitsstrategie für sensible Unternehmensbereiche und halten Sie diese in einem Plan fest.
- Überprüfen Sie regelmäßig, ob Ihr Sicherheitsplan funktioniert und eingehalten wird.
- Führen Sie regelmäßige Datensicherungen durch. Bewahren Sie gesicherte Daten abgeschottet auf, so dass sie nicht aus dem Netz erreichbar sind.
- Halten Sie Notfallpläne zur Systemwiederherstellung ausgedruckt parat.

Konzept für den Schutz Ihrer IT erstellen

Je nach Unternehmen, Systemumgebung, Mitarbeiteranzahl oder Produktionsablauf sind individuelle Sicherheitspläne für den Fall eines Cyberangriffs gefragt. Folgende Aspekte sollten u. a. beachtet werden:

- Benennen Sie einen Sicherheitsbeauftragten.
- Organisieren Sie IT-Schulungen für Mitarbeiter.
- Stellen Sie Zugangsregeln für sensible Bereiche (technisch/baulich/organisatorisch) auf.
- Klassifizieren Sie Ihre Daten und regeln Sie den Zugriff darauf (Machen Sie bestimmte Daten nur bestimmten Personengruppen zugänglich).
- Überlegen Sie, ob PC mit sensiblen Daten an Netzwerke mit Internetzugang angeschlossen werden müssen.
- Erstellen Sie einen Plan für den Angriffsfall.
- Legen Sie Kommunikationswege und -mittel für einen Schadensfall fest und machen Sie diese allen verständlich.
- Ziehen Sie externen Fachverstand bei der Erstellung und Überprüfung Ihres Sicherheitskonzepts hinzu. Fragen Sie beispielsweise die IHK nach geeigneten Ansprechpartnern.
- Seien Sie als Unternehmensführung Vorbild und bringen Sie den Sicherheitsgedanken immer wieder ins Bewusstsein aller Mitarbeiter.

Das Bundesamt für Sicherheit in der Informationstechnik hat grundlegende Empfehlungen zur IT-Sicherheit formuliert unter: www.bsi.bund.de