Nicht auf die leichte Schulter nehmen:

Cyberkriminalität bedroht jeden Betrieb

Stellen Sie sich vor, Ihre Brieftasche ist verschwunden und mit ihr auch Ausweise und EC- und Kreditkarten. Verloren oder gestohlen? Um zu verhindern, dass das Konto geplündert wird, gibt es nur eins zu tun: die Karten (Zentrale Nummer: 116 116) sperren lassen und bei der Polizei eine Verlustanzeige machen.
Aber was machen Sie, wenn Sie feststellen, dass Sie Opfer eines Datendiebstahls geworden sind? Im Prinzip dasselbe wie bei der abhanden gekommenen Brieftasche: Kontaktieren Sie die Notfall-Nummer des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in der Zeit von 8 bis 18 Uhr unter: 0800-2741000 und informieren Sie die Polizei.
Trennen Sie Ihre Systeme vom Netz, schalten die betroffenen Geräte aus und stoppen Sie die Backup-Funktion.

Woran erkennen Sie, dass Sie gehackt wurden?

Wenn Sie keine Schutzmaßnahmen getroffen haben, dann kann es sein, dass Sie erst über Hinweise von Kunden und Geschäftspartnern darauf aufmerksam gemacht werden, dass etwas nicht stimmt.

Auf Internetseiten wie www.haveibeenpwned.com können Sie überprüfen, ob Daten abgeflossen sind.

Haben Sie Schutzmaßnahmen eingerichtet, sollten die IT-Systeme reagieren und den Angriff versuchen, in Schach zu halten.

Im schlimmsten Fall werden Ihre Systeme von außen gesperrt, Daten abgegriffen und von Ihnen wird ein Lösegeld zum Freischalten der Systeme verlangt. Gehen Sie auf diese Erpressung ein, laufen Sie Gefahr, dass die Systeme trotzdem nicht freigeschaltet werden.

Strukturiert vorgehen

Nachdem Sie Ihre Systeme heruntergefahren haben, müssen Sie systematisch überprüfen, welche Bereiche betroffen sind und an die entsprechenden Stellen Meldung machen: Einerseits an die jeweiligen Landesdatenschutzbeauftragten und andererseits an alle betroffenen Geschäftspartner, deren Daten gestohlen worden sein könnten.

Prävention

Spätestens nach dem Cyberangriff sollten Sie recherchieren, auf welchem Weg die Angreifer in das Unternehmenssystem gelangt sind und diese Wege verschließen.

Notfallplan und Routenplaner von Stephan Blank:
Unter https://cybersicherheit-handwerk.de/Notfallhilfe finden Sie bspw. sehr viele Informationen für Handwerksbetriebe, welche Sie gut auf Handelsbetriebe übertragen können.

Ein oft übersehenes Risiko sind die Smartphones und die Social Media, die von den Mitarbeitern genutzt werden. Hier sollte auf eine strikte Trennung von privater und beruflicher Nutzung geachtet werden und im beruflichen Kontext auf entsprechende Apps zurückgegriffen werden (z.B. WhatsApp Business oder Threema Work).
Ohnehin sind die Mitarbeiter häufig die größte Schwachstelle, da Sicherheitsvorgaben als lästig angesehen und entsprechend nachlässig umgesetzt werden. Dagegen hilft nur, regelmäßig zu schulen und den Mitarbeitern vor Augen zu führen, welche Auswirkungen ein erfolgreicher Cyberangriff haben kann.

Muster der IHK München

Ein gut entwickelter und regelmäßig getesteter IT-Notfallplan ist unerlässlich, um im Falle eines Ausfalls der IT-Infrastruktur schnell und effizient reagieren zu können. Es geht dabei nicht nur um die Wiederherstellung von Systemen und Daten, sondern auch darum, das Vertrauen von Kunden, Partnern und Mitarbeitern zu bewahren und den fortlaufenden Geschäftsbetrieb zu sichern.

Unter folgender Internetadresse finden Sie sehr ausführliche Informationen zum Verhalten bei einem Angriff und können sich verschiedene Notfallpläne herunterladen:
https://www.ihk-muenchen.de/de/Service/Digitalisierung/Informationssicherheit/Muster-IT-Notfallplan/
Die Pläne können Sie auch in der Geschäftsstelle (E-Mail: claudia.koch@zhh.de) erhalten.

Basismaßnahmen

Durch die Digitalisierung steigen die Risiken für die tägliche Arbeit, aber keine Digitalisierung ist mit Sicherheit keine Lösung, wenn man erfolgreich sein will.

Achten Sie auf
- eine sichere **Firewall** im Betrieb, bei der regelmäßig das Passwort aktualisiert wird,
- insgesamt ein automatisches und Zeitfaktor gestütztes **Passwort-Management**,
- eine regelmäßige **Aktualisierung** der Software des Routers,
- regelmäßige Backups und
- die regelmäßige **Schulung** der Mitarbeiter.

Umfragen zeigen, dass eine Mehrheit der Unternehmer schon vor einigen

Jahren erkannt hat, dass Maßnahmen notwendig sind, aber 61% sehen auch die Schwierigkeiten bei der richtigen Umsetzung. Es sei sehr schwierig, die passenden IT-Dienstleister zu finden.

KFW - Studie: Mittelständische Unternehmen als Opfer

29 % der mittelständischen Unternehmen sind im Zeitraum von 2018–2020 Opfer von Cyberkriminalität geworden. Betroffen davon sind vor allem große Mittelständler (49 % der Unternehmen mit 100 oder mehr Beschäftigten) und Unternehmen mit ausgeprägten Digitalisierungsaktivitäten. Dies gilt etwa hinsichtlich der Höhe der Ausgaben für die Digitalisierung (43% der Unternehmen mit Digitalisierungsausgaben von 10.000 Euro oder mehr), der Bandbreite der verschiedenen Digitalisierungsprojekte (45% der Unternehmen mit 4 oder mehr verschiedenen Projektarten) und für Unternehmen mit einer Digitalisierungsstrategie (37%). Wesentlicher Grund für die häufigere Betroffenheit von Vorreitern ist die größere Angriffsfläche dieser Unternehmen in Verbindung mit unzureichenden Schutzvorkehrungen. Die Anstrengungen zur Verbesserung der IT-Sicherheit müssen daher dringend erhöht werden. Dies gilt nicht nur für die Vorreiter, sondern auch für die kleinen und nur in einem geringen Umfang digital aktiven Unternehmen. Denn diese Unternehmen sind mit Anteilen von rund einem Viertel ebenfalls häufig Opfer von Cyberkriminalität.
Schutzvorkehrungen werden gerade in mittelständischen Unternehmen häufig nicht getroffen, da in vielen Unternehmen das fachliche Knowhow fehlt. Die Bedrohungslage wird oftmals nicht erkannt und notwendige Investitionen in die IT-Sicherheit unterbleiben.
Die Hauptbedrohung gehe von der Erpressung von Löse- oder Schweigegeld aus. Auch die gezielte Überlastung von Internetseiten sei eine weit verbreitete Angriffsmethode, so Befragungsergebnisse unter mehr als 11.000 Unternehmen. Die Experten rechnen bei zunehmender Digitalisierung mit zusätzlichen kriminellen Machenschaften.

Totalverlust vermeiden

Wesentlich ist ein gutes Backup-System, welches automatisiert mehrere Sicherungskopien aller relevanten Daten anlegt. Diese Kopien sollten auf unterschiedlichen Datenträgern an verschiedenen Orten aufbewahrt werden und wenn möglich auch nicht miteinander verbunden sein.
Im Falle einer Verschlüsselung der Daten können Sie dann mit dem aktuellen Backup weiterarbeiten.
Es sollte auch über den Abschluss einer Cyberversicherung nachgedacht werden, die im Ernstfall einen finanziellen Ausgleich bietet.

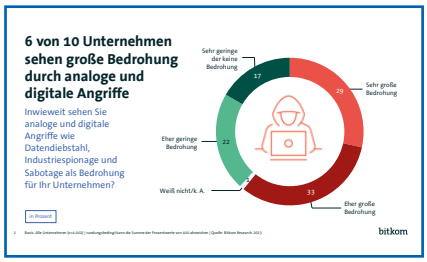
Bitkom-Studie zur KI im Bereich Cybersicherheit

KI kann nahezu perfekt klingende Phishing-Mails formulieren oder sogar Codes für Schadsoftware programmieren, KI kann aber auch Spam-Mails aus dem Postfach herausfiltern, verdächtige Kommunikation auf Servern erkennen und die Verantwortlichen frühzeitig bei Angriffen warnen. Ist generative Künstliche Intelligenz wie ChatGPT & Co. also ein Werkzeug für Cyberkriminelle oder unterstützt es eher die Cyberabwehr? Die Mehrheit der Unternehmen sieht derzeit vornehmlich Gefahren durch KI für die Cybersicherheit. 57% meinen, die Verbreitung generativer KI wird die IT-Sicherheit gefährden, weil sie von Cyberangreifern genutzt werden kann. Auf der anderen Seite sind 35% überzeugt, dass die Verbreitung von generativer KI die IT-Sicherheit verbessern wird, weil sie bei der Abwehr von Cyberangriffen genutzt werden kann. Das sind Ergebnisse einer Befragung von 1.002 Unternehmen ab 10 Beschäftigten im Auftrag des Digitalverbands Bitkom. *„KI ist eine Basistechnologie, die sowohl großen Nutzen stiften als auch Schaden anrichten kann. Regulierung und Verbote werden insbesondere international und teilweise mit staatlicher Unterstützung agierende Cyberkriminelle nicht vom KI-Einsatz abhalten. Umso wichtiger ist es, die Möglichkeit von KI bei der Cyberabwehr bereits heute zu nutzen und die Entwicklungen mit Tempo voranzutreiben“*, sagt Susanne Dehmel, Mitglied der Bitkom-Geschäftsleitung.

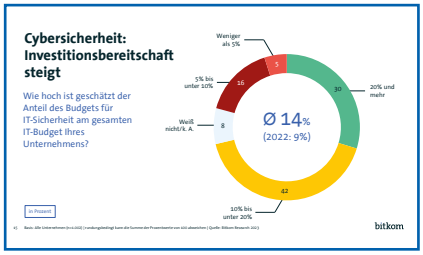
Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI)

„Cyberattacken sind die derzeit wohl größte Bedrohung für Wirtschaft, Gesellschaft und Staat. Indem sie das Bundeslagebild Cybercrime heute erstmals gemeinsam vorstellen, zeigen Bundesinnenministerium, Bundeskriminalamt und BSI, dass die Bedeutung erkannt wurde. Pro Jahr entstehen der deutschen Wirtschaft 206 Milliarden Euro Schaden durch Diebstahl von IT-Ausrüstung und Daten sowie digitale und analoge Industriespionage und -sabotage, rund drei Viertel (72 Prozent) aller Unternehmen in Deutschland sind davon betroffen. Inzwischen entfallen davon 148 Milliarden Euro, also 72 Prozent, auf reine Cyberangriffe, 2021 lag der Anteil noch bei 59 Prozent. Und fast jedes zweite Unternehmen (48 Prozent) befürchtet, dass eine erfolgreiche Cyberattacke die eigene Existenz bedrohen könnte. Wir begrüßen die Ermittlungserfolge der Behörden, auf die Bundesinnenministerin Faeser zu Recht verweist. Allerdings ist den Unternehmen wenig geholfen, wenn man weiß, wer einen Cyberangriff ausgeübt hat, der Zugriff auf die Kriminellen aber fehlt, weil ausländische Behörden die Zusammenarbeit verweigern. Wir müssen unsere digitale Abwehrfähigkeit und Resilienz massiv erhöhen. (...),“ so der Bitkom-Präsident Dr. Ralf Wintergerst Mitte Mai zu Vorstellung des Lagebildes Cyberkriminalität.

Wirtschaftsschutz Cybercrime 2023



Der Digitalverband Bitkom untersucht mit dieser Studie seit 2015 jährlich, wie es um die deutsche Wirtschaft beim Thema Wirtschaftsschutz bestellt ist. Mit der Studie hat Bitkom ein Instrument entwickelt, das umfassende Erkenntnisse über Cyberangriffe auf die deutsche Wirtschaft gibt. Welche Unternehmen sind von Spionage, Sabotage und Datendiebstahl betroffen? Wer sind die mutmaßlichen Täter? Und in welcher Höhe liegt der finanzielle Schaden für die deutsche Wirtschaft?



Weitere Graphiken aus der Studie können Sie in der Geschäftsstelle abrufen:
E-Mail: claudia.koch@zhh.de.