Cyberkriminalität steigt mit zunehmender Digitalisierung:

Kein Corona, aber genauso ansteckend

Der digitale Wandel betrifft alle Bereiche: Von der Kommunikation, dem Büro, der Warenwirtschaft, über das Lager und den Transport bis hin zur Produktion und wird demzufolge für Cyberkriminelle immer interessanter. Schon vor drei Jahren ist mehr als jedes zweite Unternehmen Opfer von Internetkriminalität geworden. Cybersicherheit ist ein fortlaufender Prozess. Die zunehmende Digitalisierung und immer stärkere Vernetzung der Unternehmensprozesse erfordert ein stetes Überprüfen und Anpassen der Schutzmaßnahmen.

Statistisches

Der Digitalverband Bitkom erstellt regelmäßig Studien zur Cybersicherheit. Schon in einer Veröffentlichung von 2018 gaben 68% der Industrieunternehmen an, Opfer von Datendiebstahl, Spionage oder Sabotage geworden zu sein. Fast 90% erwarten durch die zunehmende Digitalisierung eine Verschärfung der Bedrohungslage.
Die Wirtschaftsprüfungs- und Beratungsgesellschaft KPMG hat im vergangenen Jahr festgestellt, dass die Schäden durch Cyberkriminalität häufig im fünf- bis sechsstelligen Bereich angegeben wurden. Strafanzeigen wurden allerdings nur in 40% der Fälle gestellt. Gründe hierfür liegen u.a. in der geringen Hoffnung auf Aufklärung, Angst vor weiterem Schaden für das Unternehmen (schlechte Presse), aber auch in der erfolgreichen Abwehr von Angriffen.

Begünstigende Faktoren

Da sowohl technische als auch menschliche Faktoren eine Rolle spielen, muss auf beiden Ebenen präventiv gearbeitet werden. Zunehmende Komplexität der Technik und Unachtsamkeit der Mitarbeiter sind Hauptgründe für erfolgreiche Cyberangriffe.

Schutzmaßnahmen

Wie in der realen Welt können Sie auch im Cyberspace das Risiko nicht auf Null setzen, aber Sie können es minimieren und die Sicherheit erhöhen. Wichtig ist zuallererst die Information. Die Internetseiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die Seiten der Polizei und des Bundeskriminalamtes (BKA) zeigen eine Reihe von Maßnahmen auf. Prüfen Sie, was für Ihr Unternehmen passt, und setzen Sie die Maßnahmen um.

- Aktualisieren Sie Ihr Betriebssystem und die genutzten Programme regelmäßig.
- Nutzen Sie auch die Sicherheitsupdates.
- Ein immer aktueller Virenschutz sowie eine Firewall sind unverzichtbar.
- Richten Sie ein Benutzerkonto mit eingeschränkten Rechten ein, das für das Internet genutzt wird.
- Verwenden Sie komplexe Passwörter (ein regelmäßiger Wechsel wird inzwischen als unnötig erachtet, da viele nur marginale Änderungen an ihren Passwörtern vornehmen), die Sie im Falle eines Hacks umgehend ändern müssen.
- Verschlüsseln Sie Ihre E-Mails und verwenden Sie digitale Signaturen in der internen und externen Kommunikation.
- Achten Sie auf Auffälligkeiten, trennen Sie infizierte Systeme vom Rest.
- Erstellen Sie regelmäßig Backups, bewahren Sie sie längere Zeit auf, bevor sie überschrieben werden.
- Testen Sie im Normalbetrieb, ob sich die Backups problemlos installieren lassen.

Ein wesentlicher Faktor sind - genauso wie im realen Leben - die (ehemaligen) Mitarbeiter. In den weitaus meisten Fällen ist es keine kriminelle Energie, sondern Fahrlässigkeit und Unwissenheit. Es gibt spezielle IT-Schulungen, die die Kompetenzen erhöhen. Grundsätzlich sollten Sie ihren Mitarbeitern folgende Tipps geben - und auch selbst beachten:

- Seien Sie vorsichtig, mit der Weitergabe von vertraulichen und persönlichen Informationen.
- Nutzen Sie Ihren gesunden Menschenverstand und fragen Sie nach, wenn ihnen etwas komisch vorkommt. Besser einmal zuviel, als einmal zuwenig fragen.
- Prüfen Sie E-Mailadressen im Hinblick auf den Absender und die Domain.
- Öffnen Sie verdächtige Mails nicht, ebenso keine Anlagen von Unbekannten.
- Auch beim Anklicken von Links sollten Sie vorsichtig sein. Manche gefälschten Mails sehen den originalen sehr ähnlich, so dass ein genaues Hinsehen erforderlich ist. Oftmals verrät die Absenderadresse die Fälschung.

Kriminelle reagieren häufig auf allgemeine Situationen; z.B. wird derzeit auf Corona Bezug genommen, um an Zugangsdaten zu kommen. Noch immer werden mit Ransomware, also Makroviren, die Computer oder auch ganze Systeme verschlüsselt und nur nach Zahlung einer Geldsumme (häufig in Bitcoins) wieder entschlüsselt - oder auch nicht. Diese Erpressungssoftware ist im Vorfeld schwierig zu identifizieren, da sie von normalen Virenscannern oft nicht erkannt wird. Es gibt Programme, die PC-Systeme in Echtzeit überwachen und auf untypisches Verhalten reagieren.
Besser ist es, in Firmensmartphones zu investieren als das Nutzen privater Geräte zu erlauben. Die Firmensmartphones können mit Sicherheitssoftware und Verschlüsselungen versehen werden und so auch privat genutzt werden.
Auch Telefonanlagen können gehackt werden und dann wird auf Ihre Kosten telefoniert.

Reaktionen

Sollte ein Angriff erfolgreich gewesen sein, dann sollten Sie einen Reaktionsplan vorliegen haben, der schnell umgesetzt werden muss. Dieser Notfallplan muss - falls vorhanden - zusammen mit den Compliance- bzw. Datenschutzbeauftragten und ggf. dem Betriebsrat und der Rechtsabteilung erarbeitet werden. Lassen Sie sich ggf. von externen Fachleuten beraten. Jeder Mitarbeiter sollte ihn kennen und ggf. anwenden können. Detaillierte Handlungsanweisungen finden Sie in der am Ende des Textes genannten Broschüre des BKA.
Cybercrime kann jeden jederzeit treffen, deshalb müssen Sie für den Ernstfall konkrete Handlungsregelungen parat haben.

Homeoffice

In den letzten Monaten wurde von vielen Unternehmen aufgrund der Coronakrise verstärkt das Homeoffice genutzt. Auch Onlinekonferenzen fanden häufiger statt. Dies nutzen Cyberkriminelle aus, um ihr Unwesen zu treiben. Entweder durch gezielte Hackerangriffe auf Server oder durch den Versand von Mails mit Malware. Hier wird häufig auf die Corona-Krise abgestellt.
Homeoffice ist ein Risiko für Unternehmen, wenn die IT-Sicherheit nicht gewährleistet ist. An Datensicherheit wurde bei einer schnellen Einführung des Homeoffice oft nicht gedacht. Spätestens jetzt sollten aber Maßnahmen ergriffen werden. Oberste Maxime ist es, die Mit-

arbeiter zu sensibilisieren. Im Homeoffce sollte auf Dienstrechnern gearbeitet werden, auf jedem muss ein aktuelles Virenschutzprogramm (zur Not ein kostenfreies) installiert sein. Auch müssen die Programme regelmäßig aktualisiert werden, da dadurch Sicherheitslücken geschlossen werden.
Dienstrechner sollten nicht privat genutzt werden, im Homeoffice auch nicht anderen zugänglich sein. Achten Sie auf eine verschlüsselte passwortgeschützte Verbindung des Routers (WPA2).

Konferenztools nutzen

Auch Sie werden in den vergangenen Monaten auf Videotools wie Skype, Zoom oder Teams zurückgegriffen haben, um den Betrieb am Laufen zu halten. Wichtig ist hierbei die Beachtung datenschutzrechtlicher Vorgaben. Solche Tools dürfen nicht zur Überwachung eingesetzt werden, auch nicht, um zu prüfen, ob ein Teilnehmer sich zwar angemeldet hat, aber die Anwendung im Hintergrund laufen lässt. Aufzeichnungen sollten vermieden werden, besser ist es, im Nachgang Präsentationen oder Zusammenfassungen zu verschicken. Um die Vertraulichkeit zu wahren, sollten Zugangsregelungen (Warteraum, Schließen des Zugangs, wenn alle eingelassen wurden) genutzt werden. Dokumentationen solcher Meetings sollten aus dem Konferenz-Tool gelöscht werden und im Unternehmen nur solange wie nötig aufbewahrt werden.
Neben technischen und organisatorischen Sicherheitsmaßnahmen könnten auch transparente Moderationsfunktionen oder vorab festgelegte Verhaltensregeln die Sicherheit erhöhen.
Vor allem in kleineren und mittleren Unternehmen, die sich bislang kaum oder gar nicht mit dieser Technik befasst haben, besteht nach wie vor ein großer Informations- und Beratungsbedarf, dem z.B. das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) mit entsprechenden Hinweisen helfen will. Dazu hat die Behörde eine neue Online-Broschüre mit dem Titel *"Datenschutz: Plötzliche Videokonferenzen – und nun?"* herausgegeben, die viele Fragen rund um das Thema beantwortet. Gleich am Anfang der Ausführungen werden einige grundsätzliche Fragen gestellt. So etwa, ob eine Videokonferenz überhaupt das angemessene Kommunikationsmittel in der jeweiligen Situation ist, oder ob nicht auch andere bewährte Formen, wie der schriftliche Nachrichtenaustausch oder eine Telefonkonferenz, genauso gut geeignet sein könnten, wodurch sich einige der Risiken vermeiden ließen.

Sie können die Broschüre als PDF in der Geschäftsstelle abrufen. E-Mail: claudia.koch@zhh.de.

Cloudsicherungen

Eine Auslagerung von Daten in die Cloud sollte nur nach Prüfung der Datensicherheit stattfinden, am besten stehen die Server in der EU, dann gilt die DSGVO. Vorteile einer Cloudlösung sind flexibles Datenvolumen, Wartung durch Provider, aktuelle Technik, aktuelle Infrastruktur. Sie können auch ein privates Cloudsystem einrichten.

Cyberversicherungen

In Anbetracht der hohen Bedrohung durch Cyberkriminalität machen inzwischen viele Versicherungen Angebote, die die Risiken minimieren sollen. Diese sind - wie alle Policen - genau zu prüfen, ob sie die benötigten Risiken abdecken. Häufig sind sie nach dem Baukastenprinzip angelegt. Auch unser Rahmenabkommenspartner Hemmer und Felder bietet eine Cyberversicherung zu vergünstigten Konditionen für ZHH-Mitglieder an.

Kontaktieren Sie die Agentur unter: Hemmer & Felder GmbH, Berrenrather Straße 203, 50937 Köln - Sülz, Tel. 0221 94 08 15-0, E-Mail: info@hefe-gmbh.de.

Cyberangriffe sind unsichtbar! Das macht sie so gefährlich.

Allgemeine Empfehlungen

Das Bundeskriminalamt hat *„Handlungsempfehlungen für die Wirtschaft"* herausgebracht, die das Thema Cyberkriminalität ausführlich darstellen. Hier finden Sie auch eine ausführliche Liste von Ansprechpartnern.

Sie können die Broschüre als PDF in der Geschäftsstelle erhalten. E-Mail: claudia.koch@zhh.de.