Was ist Cybersecurity?

cebra GmbH - new technologies
Sankt Martin Str. 9, 84539 Ampfing
Telefon: +49 8636 69 76 67
E-Mail: info@cebra.it
Webseite: https://www.cebra.it

Allgemeines

Autor:	Christian Sigl
Version:	4.0
Versionsdatum:	2022-12-19

Vorwort

"Es gibt nur zwei Arten von Unternehmen: Solche, die gehackt wurden, und solche, die noch gehackt werden." Robert Mueller, ehem. FBI-Chef, 2012, zit. im "Rechtshandbuch Cyber-Sicherheit", Gabel/Heinrich/Kiefer (Hrsg.), 2019.

Ich würde derzeit sogar noch einen Schritt weitergehen und das Zitat erweitern um **"solche, die gehackt wurden, es aber noch nicht wissen."**

Leider können wir derzeit täglich mehrere Cyber-Angriffe auf kleine und mittelständische Unternehmen verzeichnen - Tendenz steigend. Dabei ist nicht immer klar, welches Ziel die Angreifer verfolgen. In manchen Fällen geht es nur darum im Unternehmen Schaden anzurichten. Oftmals werden die Firmen aber auch mit einer Lösegeldforderung konfrontiert, um an die heiligen Unternehmensdaten wieder heranzukommen.

Ein **ganzheitliches** Sicherheitskonzept ist deshalb unumgänglich - auch für den Mittelstand!

Stellen Sie sich Ihr Netzwerk als Ihr eigenes Zuhause vor. Hier werden Sie sich vermutlich auch schützen indem Sie alle Türen und Fenster schließen. Sie können noch so ein hochmodernes Sicherheitsschloss an Ihrer Haustür besitzen - wenn Sie das Fenster offen lassen kommt der Eindringling in Ihr Haus.

Genauso ist es auch mit Ihrem Unternehmensnetzwerk. Es nützt relativ wenig nur eine Tür gut zu sichern - der Angreifer wird früher oder später das offene Fenster finden.

Was ist also Cybersecurity?

Unter Cybersicherheit versteht man Maßnahmen, um Computer, Server, Mobilgeräte, elektronische Systeme, Netzwerke und Daten gegen böswillige Angriffe zu verteidigen. Sie wird auch als IT-Sicherheit oder elektronische Datensicherheit bezeichnet. Der Begriff wird in einer Vielzahl von Kontexten, von Geschäftsanwendungen bis zum mobilen Computing, verwendet und lässt sich in einer Reihe von allgemeinen Kategorien zusammenfassen.

- **Netzwerksicherheit** ist ein Verfahren zur Sicherung eines Computernetzwerkes vor Eindringlingen, sei es in Form von gezielten Angreifern oder einer auf eine günstige Gelegenheit hoffenden Malware.
- **Programmsicherheit** bezieht sich darauf, Software und Geräte von Bedrohungen zu bewahren. Ein gefährdetes Programm könnte Zugriff auf die Daten gewähren, die es eigentlich schützen soll. Erfolgreiche Sicherheit beginnt in der Designphase, noch lange bevor ein Programm oder Gerät bereitgestellt wird.
- **Informationssicherheit** schützt die Integrität und Privatsphäre von Daten, sowohl in Speichern als auch beim Versenden.
- **Betriebssicherheit** bezieht sich auf Prozesse und Entscheidungen zum Umgang und Schutz von Datenbeständen. Unter diese Bezeichnung fallen die Berechtigungen, über die ein Benutzer beim Zugriff auf ein Netzwerk verfügt, sowie die Verfahren, über die festgelegt ist, wie und wo Daten gespeichert oder freigegeben werden dürfen.
- **Disaster Recovery und Business Continuity** definieren, wie eine Organisation auf eine Verletzung der Cybersicherheit oder jedes andere Ereignis, das zum Verlust betrieblicher Abläufe oder Daten führen, reagieren. Wie eine Organisation ihren Betrieb und ihre Daten auf denselben Stand wie vor dem Ereignis wiederherstellt, ist in den Disaster Recovery-Richtlinien festgelegt. Auf den Business Continuity-Plan greifen Organisationen zurück, um die eigene Geschäftstätigkeit auch ohne bestimmte Ressourcen fortsetzen zu können.
- Bei der **Endbenutzer-Aufklärung** geht es um den am wenigsten vorhersagbaren Faktor der Cybersicherheit: den Menschen. Jeder kann versehentlich ein Virus in ein ansonsten sicheres System einschleusen, indem er bewährte Sicherheitsprinzipien verletzt. Benutzer darüber aufzuklären, dass verdächtige E-Mail-Anhänge gelöscht oder unbekannte USB-Sticks nicht eingesteckt werden dürfen, sowie eine Reihe von weiteren wichtigen Lektionen sind für die Sicherheit jeder Organisation unverzichtbar.

Katz-und-Maus-Spiel

Die kontinuierliche Entwicklung

Eine der größten Herausforderungen im Bereich Cybersecurity ist die stetige Weiterentwicklung der Technologien. Neue Technologien bieten auch neue potenzielle Möglichkeiten und Angriffspunkte für Cyberkriminelle. Im Umkehrschluss heißt dies, dass auch die Security Software Anbieter und Sicherheitsexperten ständig neue Lösungen zur Schließung von Schwachstellen entwickeln müssen.

Klar - eine sehr große Herausforderung für kleine und mittelständische Unternehmen - zumal der Ganze Spaß nicht nur nervenaufreibend sondern auch sehr kostenspielig werden kann, da die Sicherheit immer mit dem Komfort und der Bequemlichkeit einhergeht und die Systeme ständige Aufmerksamkeit und regelmäßige Updates benötigen, um potentielle Sicherheitslücken schnellstmöglich zu schließen.

Ausbildung der Mitarbeiter

Die Angriffszenarien haben sich in den letzten Jahren stark verändert. Dabei war es vor nicht allzulanger Zeit üblich, Systeme etwa mit einer Brute-Force-Attacke anzugreifen. Aufgrund zusätzlicher Sicherheitsmechanismen, wie zum Beispiel einer Multi-Factor-Authentifizierung (MFA), ist dies für Angreifer oft nicht mehr das richtige Werkzeug, weshalb mehr und mehr auf den Faktor Mensch, mithilfe Social Engineering, gesetzt wird.

Fazit

Seien Sie nicht naiv! Schützen Sie Ihr Unternehmensentzwerk mithilfe geeigneter Maßnahmen, sensibilisieren Sie Ihre Mitarbeiter und handeln Sie proaktiv. Wir sind in einem digitalen Zeitalter angekommen, bei dem sich nicht die Frage stellt ob Ihr Unternehmen angegriffen wird. Es wird passieren! Vielmehr sollten Sie sich die Frage stellen, ob Sie gegen aktuelle Angriffe bestmöglich geschützt sind, um das Ausmaß der Angriffe auf ein Minimum reduzieren zu können.

Sprechen Sie uns an - wir beraten Sie gerne.

Revision #8
Created 2022-08-02 11:53:09 UTC by Christian Sigl
Updated 2022-12-19 12:36:27 UTC by Christian Sigl