3 einfache Schritte, mit denen Sie Ihr Unternehmen vor Cyberangriffen schützen

Sich vor einem Cyberangriff zu schützen ist immer sehr viel einfacher, als hinterher die Scherben aufzusammeln.

Viele Kleinunternehmer glauben, dass ihre Unternehmen aufgrund der Größe kein Ziel von Hacks, Ransomware und anderen Arten von Cyberangriffen werden. Andere sind sich der Notwendigkeit von Cybersicherheit bewusst, sind aber der Meinung, nicht über genügend Ressourcen zu verfügen, um Cybersicherheit zur Priorität zu machen. Dies sind nur einige der Gründe, **weshalb ganze 90 % aller Kleinunternehmen keine Sicherheitsvorkehrungen treffen, die die Daten des Unternehmens und der Kunden schützen könnten.**[1]

Cyberkriminellen sind diese Schwachstellen nicht verborgen geblieben. Einer aktuellen Studie zufolge war bereits ein Fünftel aller Kleinunternehmen von Cyberangriffen betroffen.[2]

Monate können vergehen, bis ein Cyberangriff erkannt wird. Doch bis dahin ist bereits ein beträchtlicher Schaden entstanden – durchschnittlich entstehen Kosten zwischen 84.000 USD und 148.000 USD, vom Vertrauensverlust bei den Kunden ganz zu schweigen.[3] Oft lässt sich der Schaden nicht mehr rückgängig machen. Einer Studie von Better Business Bureau aus dem Jahr 2017 zufolge „bleiben nur 35 % der Unternehmen mehr als drei Monate lang profitabel, wenn sie dauerhaft den Zugang zu wichtigen Daten verlieren."[4]

SCHRITT 1

Einschränken des Zugriffs

Hacker werden beim Erraten oder Stehlen von Kennwörtern immer raffinierter. Aus diesem Grund raten Experten zusätzlich zum Kennwort zu einer weiteren Sicherheitsebene, die oft als „zweistufige Authentifizierung" oder „mehrstufige Authentifizierung" bezeichnet wird. Dieses zweite Hindernis hält Hacker effektiv fern. Im Folgenden sind einige Beispiele für mehrstufige Authentifizierung (Multi-Factor Authentication, MFA) aufgeführt, die häufig entweder bei Computerhardware oder beliebten Websites und Anwendungen zum Einsatz kommen:

Eine vierstellige PIN oder eine geheime Antwort auf eine Frage (Beispiel: „Wie lautete der Name Ihres ersten Haustiers?").

Ein eindeutiger Code, der per SMS versendet wird (beliebteste Form von MFA).

Biometrische Sensoren wie Netzhautscanner, Gesichtserkennung oder Fingerabdruckscanner ermöglichen einen schnellen und personalisierten Zugang. So können Benutzer sich beispielsweise bei Latitude-Laptops und ausgewählten Vostro-PCs mit Windows Hello mit nur einer Berührung oder einem Blick sicher anmelden.

SCHRITT 2

Erkennen und Vermeiden von Bedrohungen

„Malware" steht kurz für „malicious software" (schädliche Software). Unter diesem Sammelbegriff sind verschiedenartige Schädlinge zusammengefasst – Spyware, Viren, Trojaner, Rootkits und Ransomware sind nur einige davon. Die verursachten Störungen können von Computerabstürzen, Identitätsdiebstahl bis hin zu einem durch Ransomware bedingten netzwerkweiten Ausfall reichen. Dabei haben Sie so lange keinen Zugriff auf Ihre Daten, bis Sie dem Angreifer ein Lösegeld zahlen.

Eine der häufigsten Arten zur Verbreitung von Malware im System eines Mitarbeiters erfolgt über eine Phishing-E-Mail. Diese E-Mails scheinen zwar harmlos. Wenn Ihr Mitarbeiter jedoch auf den Link in der E-Mail klickt, wird er möglicherweise dazu aufgefordert, vertrauliche Informationen weiterzugeben, oder Malware beschädigt das System. Ihre Mitarbeiter müssen E-Mails und URLs genau auf alles prüfen, was ihnen verdächtig vorkommt (z. B. Falschschreibung in einer URL), bevor sie darauf klicken.

McAfee™

Außerdem bieten Softwareunternehmen wie McAfee einen nahtlosen Schutz an, der im Hintergrund automatisch nach Bedrohungen sucht und sie eliminiert, bevor das System beeinträchtigt wird. Ein umfassendes Softwarepaket kann Benutzer außerdem vor unsicheren Websites und gefährlichen Downloads schützen.

SCHRITT 3

Mehr Sicherheit durch einen Sicherungsplan

Kleinunternehmer rechnen jetzt mit allem – Fehler passieren, Systeme stürzen ab und Überraschungen tauchen auf. Anhand der ersten beiden Tipps beseitigen Sie viele Bedrohungen, Angriffe sind jedoch trotzdem nicht auszuschließen. Wenn Sie ein Sicherungssystem verwenden, ist die Wiederherstellung Ihrer Daten um einiges leichter. Sie haben im Grunde zwei Möglichkeiten Ihre Daten zu sichern: mithilfe von Hardware wie einem Speicherlaufwerk oder anhand eines cloudbasierten Speichers auf lokalen Servern.

Externe Festplatten sind einfach in der Verwendung – Sie müssen nur eingesteckt werden. Anschließend werden die Daten an die Festplatte übertragen und die Festplatte wird sicher gelagert. Der Nachteil ist, dass ein Ablagesystem und Platz vorhanden sein müssen. Die Festplatten können also verloren gehen oder beschädigt werden.

mozy® BY DELL

Alternativ bietet der Clouddatenschutz von Unternehmen wie MozyPro eine komfortable Lösung, mit der Sie Ihre Daten nicht mehr manuell auf Festplatten herunterladen und diese anschließend lagern müssen.

Sobald Sie Ihre Dateien hochladen, erkennt MozyPro automatisch Änderungen und synchronisiert sie auf all Ihren Geräten – in der Cloud ist immer die aktuelle Version gespeichert. Ihre Daten werden außerdem mit einer äußerst ausgeklügelten Verschlüsselungstechnik gesichert, die zusätzlichen Schutz vor Angriffen durch Ransomware bietet. Ein Angriff durch Ransomware ist nur dann effektiv, wenn Sie auf Ihre Daten nicht auf einem anderen Weg zugreifen können. Durch eine Datensicherung in der Cloud wird der Ransomware-Angriff also wirkungslos.

Haben Sie Fragen? Die Technologieberater für kleine Unternehmen von Dell unterstützen Sie mit zuverlässigen Sicherheitslösungen, die Ihr Unternehmen schützen.

SPRECHEN SIE NOCH HEUTE MIT IHREM DELL BERATER:

0800-138 33 55*

KLICKEN | **ANRUFEN** | **CHATTEN**

[1] https://www.theguardian.com/business/2015/jan/21/cybersecurity-small-business-thwarting-hackers-obama-cameron | [2] https://www.bbb.org/stateofcybersecurity/
[3] https://www.theguardian.com/business/2015/jan/21/cybersecurity-small-business-thwarting-hackers-obama-cameron | [4] https://www.bbb.org/stateofcybersecurity/

*Mo-Fr. 8:30-17:30 Uhr (bundesweit zum Nulltarif aus dem dt. Fest- und Mobilfunknetz).