Zehn Cybersecurity-Irrtümer, die sehr teuer werden können.

Cyberkriminalität ist zu einem so allgegenwärtigen Thema geworden, dass wir die zahlreichen Meldungen über Ransomware-Angriffe, Datenschutzverletzungen und andere Betrügereien kaum mehr wahrnehmen. Das ist allerdings ein grosser Fehler. Cyberkriminalität ist zu einem lukrativen Geschäftsfeld geworden, das Milliardenumsätze generiert. Betroffen sind wir alle, und deshalb ist es wichtig, dass wir das Risiko richtig einschätzten. Fehler könnten sehr teuer werden.

Irrtum Nummer 1_
Ransomware ist der komplette Angriff – wenn wir das überleben, sind wir sicher.
Ransomware ist in den allermeisten Fällen nur der Punkt, an dem die Angreifer das Opfer darauf aufmerksam machen, dass sie da sind und was sie getan haben. Die Angreifer waren wahrscheinlich schon Tage, wenn nicht Wochen, im Netzwerk, bevor sie die Ransomware aktiviert haben. In dieser Zeit haben Sie das Netzwerk erkundet, Backups deaktiviert oder gelöscht, Computer mit wichtigen Informationen oder Anwendungen gefunden, Informationen entfernt und zusätzliche Nutzdaten oder Backdoors installiert. Das Verbleiben in den Netzwerken der Opfer ermöglicht es den Angreifern, einen zweiten Angriff zu starten - wann immer sie wollen.

Irrtum Nummer 2_
Die Zahlung eines Lösegelds wird unsere Daten wiederherstellen.
Die Zahlung des Lösegelds ist – auch wenn es die einfachste Option zu sein scheint – keine Lösung, um wieder auf die Beine zu kommen. Laut der „State of Ransomware"-Umfrage 2021 liegt die Erfolgsquote für Unternehmen, die das Lösegeld bezahlt haben, nur etwa bei 65 Prozent ihrer Daten. Lediglich acht Prozent erhielten sämtliche Daten zurück, und 29 Prozent konnten weniger als die Hälfte wiederherstellen. Ausserdem ist die Wiederherstellung der Daten nur ein Teil des Wiederherstellungsprozesses – in den meisten Fällen legt die Ransomware die Computer komplett lahm, wodurch Software und Systeme von Grund auf neu aufgebaut werden müssen, bevor die Daten wiederhergestellt werden können. Diese Wiederherstellungskosten sind im Durchschnitt zehnmal so hoch wie die Lösegeldforderung.

Irrtum Nummer 3_
Wir haben eine Firewall. Damit ist unsere IT gut gesichert.
Aufgabe der Firewall ist es, den Datenverkehr zwischen den internen und den externen Netzen laufend zu überprüfen und zu filtern. Gleichzeit soll sie die IT-Schlüsselpersonen im Unternehmen oder den externen IT-Dienstleister bei Fehlfunktionen oder Cyberangriffen alarmieren. Allerdings genügt eine Firewall alleine nicht, um Ihre Organisation wirkungsvoll zu sichern. Zum Beispiel werden Daten, welche die Nutzer über USB-Laufwerke auf die Computer laden, nicht von der Firewall erfasst. Sie sind somit ein potenzielles Einfallstor für Schadsoftware. Auch der unkorrekte Umgang mit Login-Daten (zum Beispiel bei einer Phishing-Attacke) kann von einer Firewall nicht verhindert werden.

Irrtum Nummer 4_
Sicherheit ist Sache der IT-Abteilung.
Viel zu oft wird das Thema Sicherheit an den IT-Verantwortlichen delegiert. Oder das Unternehmen verlässt sich darauf, dass der IT-Partner das schon irgendwie richtig macht – ohne, dass die Zuständigkeiten klar geregelt werden. Nicht selten entstehen folgenreiche Angriffe an den Schnittstellen, weil diese nicht klar definiert oder missverstanden werden. Im Falle eines Cyberangriffs haftet die Firma. Der Verwaltungsrat und allenfalls auch die Geschäftsleitung könnten bei Schäden aufgrund eines Cyberangriffs wegen ungenügender Schutzmassnahmen verantwortlich gemacht werden. Diese Verantwortung lässt sich nicht an IT-Verantwortliche und schon gar nicht an Externe delegieren. IT-Sicherheit sollte daher von der Geschäftsleitung als strategisches Thema von höchster Wichtigkeit behandelt werden.

Irrtum Nummer 5_
Sicherheit gebe ich nicht raus. Das Thema ist mir zu wichtig.
Insbesondere für KMU ist es kaum möglich, sich laufend mit allen Aspekten und neuesten Erkenntnissen der Cyber Security zu beschäftigen. Somit können bei einer veränderten Bedrohungslage die unmittelbar notwendigen Massnahmen nicht er-

griffen werden. Auch das Monitoring der eigenen IT-Infrastruktur und eine rasche Reaktion bei Zwischenfällen ist nur in wenigen KMU mit der eigenen Schutz-Organisation möglich. Selbst wenn das Unternehmen über ein eigenes IT-Team verfügt, lohnt sich die Zusammenarbeit mit einem externen IT-Sicherheitspartner – so kann sich die eigene IT-Abteilung auf geschäftsrelevante IT-Projekte konzentrieren.

Irrtum Nummer 6_
Wir sind für Hacker nicht interessant und haben sowieso keine Geheimnisse.
Viele Opfer von Cyberangriffen halten sich für zu klein, zu uninteressant oder wenig lukrativ, um bedroht zu sein. Kriminelle nehmen darauf wenig Rücksicht. Jede Person oder jedes Kleinstunternehmen mit digitaler Präsenz und Einsatz von Computern ist ein potenzielles Opfer. Die meisten Hackerangriffe geschehen wenig spektakulär, sondern werden von Opportunisten auf der Suche nach leichter Beute ausgeübt. Zu den beliebtesten Zielen zählen Unternehmen mit nicht gepatchten Sicherheitslücken oder Fehlkonfigurationen. Wer denkt, er sei als Ziel zu unbedeutend, sollte noch heute sein Netzwerk nach verdächtigen Aktivitäten durchforsten.

Irrtum Nummer 7_
Wir haben einen Notfallplan.
Ein Notfallplan ist tatsächlich sehr zentral. Damit wird sichergestellt, dass Sie oder Ihre IT im Falle eines Cyberangriffes die passenden Sicherheitsmassnahmen ergreifen und schnell reagieren können. Ein solcher Plan kann eine Anleitung dazu enthalten, wie Sie einen Server schnell vom Netz trennen, sollten Sie angegriffen werden. Bei einem Cyberangriff ist schnelles Reagieren einer der wichtigsten Faktoren, um die Konsequenzen so gering wie möglich zu halten. Trotzdem ist der Notfallplan alleine noch kein Schutz. Eher eine Absicherung, um grösseren Schaden zu verhindern. Schutz muss proaktiv sein. Ein Notfallplan ist immer reaktiv.

Irrtum Nummer 8_
Wir haben eine Versicherung.
Eine Versicherung alleine schützt leider nicht. Und sie bezahlt typischerweise höchstens den monetären Schaden. Proaktive Cyber Security Massnahmen sind wie Bremsen an einem Fahrzeug. Nur weil das Fahrzeug versichert ist, verzichtet niemand auf die Bremsen.

Irrtum Nummer 9_
Unsere Mitarbeiter werden regelmässig geschult, das reicht.
Nach der Studie „State of Ransomware 2021“ glauben 22 Prozent der Unternehmen, dass sie in den nächsten zwölf Monaten Opfer von Ransomware werden können. Social-Engineering-Taktiken wie Phishing-E-Mails sind immer schwieriger zu erkennen. Die Nachrichten sind oft so spezifisch, überzeugend und sorgfältig geschrieben, dass es für Mitarbeiter nahezu unmöglich ist diese zu erkennen. Selbstverständlich können durch regelmässige Mitarbeiterkampagnen viele Angriffe abgewehrt werden. Trotzdem sollte Mitarbeiterschulung in eine umfassende Cyber-Security-Strategie integriert werden.

Irrtum Nummer 10_
Jede Mitarbeiterin und jeder Mitarbeiter ist selber verantwortlich
Firmen übertragen den Mitarbeitenden die Verantwortung für den sicheren Umgang mit E-Mail und Internet. Dabei ist die Sensibilisierung der Mitarbeitenden für Sicherheitsrisiken eine Bringschuld der Firma, genauso wie Sicherheitsschuhe oder der Helm für die Baustelle. Der Mitarbeiter ist in der Pflicht, diese bereitgestellten Werkzeuge richtig und jederzeit anzuwenden.

UMB Cybersecurity

UMB kreiert dank modularen Cybersecurity Services permanenten Schutz in einer zunehmend digitalen und komplexen Welt. Nur ausgewogene organisatorische und technische Massnahmen schützen Ihr Unternehmen wirkungsvoll und ganzheitlich. Dafür müssen neue Sicherheits-Dimensionen eingeführt werden, welche die klassische Prävention (Netzwerk- und Perimeterschutz) ergänzen. Dazu gehört einerseits die Fähigkeit, einen Angreifer frühzeitig zu entdecken. Andererseits müssen rasch die richtigen Gegenmassnahmen eingeleitet werden können.

IBM Platinum Business Partner

Klingt spannend? Kontaktieren Sie uns!

Gerne beantworten wir Ihre Fragen zu Cybersecurity und mehr.

Kontakt
Markus Kaegi
Team Leader Strategic Sales Consultant
markus.kaegi@umb.ch
+41 58 510 17 26
www.umb.ch