DIE MYTHEN DER CYBERSECURITY: ERKLÄRT UND AUSGERÄUMT

Veröffentlicht am 04.10.2023 um 18:17 von Redaktion AltkreisBlitz

Sicherheit im Internet ist wichtig, keine Frage. Es können
versteckte Gefahren lauern, die auch bei genauerem Hinsehen nicht auffallen müssen.

Wichtig ist aber auch, es mit der Sicherheit nicht sehr zu übertreiben. So gibt es durchaus auch Vorsichtsmaßnahmen, die unter Umständen gar nicht ergriffen werden möchten.Doch die Unsicherheit bleibt. Vielleicht haben Sie sich auch schon die Frage gestellt: Ist ein VPN eigentlich legal oder muss ein Passwort wirklich stark sein, um auch für ausreichend Sicherheit zu sorgen?Hier erfahren Sie alles zum Thema Cybersicherheit und mit welchen Mythen sie endlich aufräumen können.

Mythos 1: Ein starkes Passwort muss sein

Es stimmt durchaus, dass es hilfreich sein kann, wenn das Passwort stark ist und somit nicht nur aus Buchstaben, sondern auch Zahlen besteht. So haben andere es schwer, dieses herauszufinden.Hierbei muss aber bedacht werden, dass ein **starkes Passwort allein nicht ausreicht**. Es braucht zusätzlich eine Zwei-Faktor-Authentifizierung und gutes Monitoring. Sind diese beiden zusätzliche Dinge nicht gegeben, kann unter Umständen auch das stärkste Passwort keinen ausreichenden Schutz bieten.Besonders wichtig ist dies für Unternehmen, die sensible Daten schützen wollen und müssen. Hilfreich kann an dieser Stelle auch sein, nicht allen Mitarbeitern den Zugriff auf alle Daten zu erlauben. Wenn schon hier eine Differenzierung erfolgt, kann das beim Schutz sehr helfen.

Mythos 2: Kleine Unternehmen sind für Hacker unwichtig

Es scheint auf der Hand zu liegen. Hacker haben absolut kein Interesse an kleinen Unternehmen. Es sind die großen Konzerne, die sie interessieren. Aber ganz so ist es nicht. Forschungen und Beobachtungen haben immer wieder ergeben, dass bis **zu 58 % der betroffenen Unternehmen zu den kleinen Konzernen** gehören.Grund dafür ist das sogenannte ?Spray-and-Pray? verfahren. Es werden ganz zufällig Unternehmen ausgewählt, sodass es jeden treffen kann. Hierbei sollte auch gesagt werden, das kleine Betriebe durchaus leichtere Beute sind. Die Sicherheitsmaßnahmen sind oft nicht so groß und sensible Daten, die zur weiteren Verwendung genutzt werden können, gibt es natürlich auch dort.Somit ist es wichtig, dass auch kleine Unternehmen die Gefahr nicht unterschätzen und bestimmte Maßnahmen beachten, um wirklich sicher zu sein.

Mythos 3: Bestimmte Branchen sind besonders gefährdet

Ein Fahrradhandel ist nicht so interessant wie eine Bank? Das mag auf den ersten Blick so sein. Die Realität sieht aber anders aus, denn **sensible Daten gibt es überall.**
Dabei kann es sich um folgende Informationen handeln:AdressenKreditkartennummernZahlungsdatenWeitere persönliche DatenSie sehen schon, es gibt recht viele Daten, die wichtig sein können und im Darknet eine große Rolle spielen.Es kann somit festgehalten werden: Niemand ist sicher und Schutz geht jedes Unternehmen etwas an.

Mythos 4: Antivirensoftware bietet umfassenden Schutz

Es stimmt: Wer ein Virenprogramm besitzt, ist geschützt und kann sich zumindest ein Stück zurücklehnen. Aber diese **Software reicht natürlich bei Weitem nicht aus**, um wirklich sicher sein zu können.Hier braucht es eine Sicherheitsstrategie, die tiefgreifender ist und noch viele weitere Bereiche abdeckt.Wichtig ist hier:Mitarbeiterschulungen zu IdentifizierungInsider BedrohungenNotfall-ManagementWenn Sie all dies zusätzlich beherzigen, sind Sie auf einem guten Weg, wirklich geschützt zu sein.

Mythos 5: Bedrohungen sind außen

Sehr oft ist es der Fall, dass ?Angriffe? von außen kommen. Aber das ist wahrlich nicht immer der Fall. Zahlen belegen sogar, dass **75 % der Bedrohungen von innen kommen** und somit sogar eine sehr große Gefahr darstellen. Jetzt sind Sie sicherlich überrascht, aber diese Zahl lässt sich immer wieder bestätigen.Niemand kann wirklich sicher sein. Hierbei kann es sich z.B. um verärgerte Unternehmen oder auch Mitarbeiter handeln, die sich für etwas rächen wollen.Das klingt jetzt vielleicht seltsam, aber Sie sollten darauf wirklich vorbereitet sein.

Mythos 6: Schutz gehört in die IT-Abteilung

Es ist richtig, dass in der IT-Abteilung die Weichen gestellt werden und viele Programme genau dort hingehören. Aber dort allein kann der Schutz nicht gewährleistet werden.Eine sehr **große Verantwortung tragen auch die Mitarbeiter**. Sie müssen für Gefahren sensibilisiert werden. Eine große Gefahr geht hierbei von Links und E-Mails aus, die unbedacht geöffnet werden.Passiert das, kann auch die IT-Abteilung nicht mehr helfen und Daten, die einmal gestohlen wurden, bleiben es auch für immer. Hier braucht es viel Grundwissen.

Mythos 7: Wi-Fi-Netzwerk ist durch ein Passwort sicher

Wer gerne mobil arbeitet, wird dieses Passwort kennen und nutzen. Es bietet etwas Sicherheit, ohne Frage. Aber sobald Mitarbeiter das gleiche Passwort verwenden, ist es für diese kein Problem, auf Ihre sensiblen Daten zuzugreifen. Der **richtige Schutz ist somit in erster Linie nicht gegeben.**Auch sollte nicht jeder Zugang genutzt werden. Entscheiden Sie sich nur für Orte, die Sie kennen. Unter Umständen kann es sich durchaus um Hotspots handeln, die von Hackern installiert wurden.

Cybersecuritiy ist wichtig

Diese Mythen machen klar: **Es ist wichtig, jedes Unternehmen zu schützen**, dabei spielt auch die Branche keine Rolle. Jeder kann getroffen werden und es gibt niemals genug Schutz. Schulen Sie Mitarbeiter, bleiben Sie wachsam und finden Sie einen Weg, der für Sie und ihre Firma einfach aber auch lukrativ ist.Hören Sie sich um, gehen Sie mit der Zeit und finden Sie heraus, was bei Ihnen umgesetzt werden kann.