Sicherheitsstrategie: Grundregeln für Ihre Unternehmens-IT

Wie Sie Ihre Netzwerke und Daten schützen

In Unternehmen werden hochsensible Daten gespeichert. Deren Verlust kann existenzbedrohend sein. Dem sind sich die Entscheidungsträger wohl bewusst, die Etats für IT-Security wachsen stetig. Die Sicherheit selbst tut das leider oft nicht im gleichen Maße. Einfach mehr Geld zu investieren nützt aber nur bedingt, wenn keine vernünftige Strategie dahinter steckt. Nur damit kann man langfristig und deutlich an Sicherheit gewinnen.

Ganzheitliche Strategie

Große Gefahr geht von geteilter Verantwortung aus. Wenn ein Kollege für Virenscanner und Firewall zuständig ist und der andere sich um Cloud Computing kümmert, sind Probleme vorprogrammiert. Es muss eine zentrale Stelle geben, von der aus alle Initiativen gesteuert werden. Eine Erfolgsformel für eine Unternehmensstrategie gibt es dabei nicht, zu individuell sind die Anforderungen, gewisse Fixpunkte gibt es aber schon.

Bewusstsein schaffen

Die teuersten Sicherheitssysteme verpuffen nutzlos, wenn die Mitarbeiter nicht sensibilisiert werden. Für Datendiebe ist es oft der einfachste Weg, durch Aushorchen von Personen Zugang zu sensiblen Informationen zu erhalten. Schulungen und das Aufstellen von verbindlichen Verhaltensregeln sind unbedingt notwendig und auch gesetzlich vorgeschrieben.

Schnittstellen sichern

Es wäre alles so einfach, wenn man ein komplett in sich geschlossenes Computernetzwerk hätte. Davon sind wir heute aber so weit entfernt wie noch nie. Jeder besitzt mehrere USB-Sticks, oft werden sie auch als Geschenk angenommen oder untereinander getauscht. Diese kleinen Helfer können böse Überraschungen bereithalten. Über sie können alle denkbaren Arten von Schadprogrammen in das IT-Netzwerk eingeschleust werden. Ob man die Sticks nun komplett aussperrt oder nur gesicherte Speicher des Unternehmens zulässt, hier muss man die individuell passende Lösung finden, die auch wirklich im Unternehmen umsetzbar ist. Noch größer ist mittlerweile das Risiko des WLANs. Das kabellose Internet bietet viel Komfort, aber das WLAN-Netz ist auch einer der anfälligsten Einfallpunkte für Angriffe auf Unternehmen. Den Zugriff auf besonders sensible Daten via WLAN sollte man darum besser abschalten, auch ein separates Netz für externe Personen ist sinnvoll und natürlich sollte das Firmen-WLAN so sicher wir nur möglich durch entsprechende Router-Einstellungen aufgesetzt werden.

Mobiles Risiko

BYOD - Bring Your Own Device. Der Albtraum jedes Sicherheitsexperten, gleichzeitig nicht mehr weg zu denken. Die Mitarbeiter nutzen vor allem ihre Handys oft privat und beruflich, munter werden unkontrolliert Apps installiert und das Gerät kommt weit herum, ist ständig in unsicheren Netzwerken unterwegs. Es gibt aber Mittel und Wege, wie man hier eine Trennlinie zwischen privater und beruflicher Welt ziehen kann. Dafür gibt es spezielle Software aber auch Hardware, Blackberry bietet z.B. Smartphones mit genau so einer integrierten Trennlinie an. Mit Smartphone und Tablet hat auch die Cloud die Unternehmen erreicht. Auch dies kann zu beträchtlichen Risiken führen, wenn man bedenkt, dass Daten des Unternehmens über öffentliche Netzwerke hoch- und runtergeladen werden. Die Verschlüsselung aller Daten in der Cloud ist essentiell, schon bei der Wahl des Cloud-Anbieters sollte darauf geachtet werden, dass er hier größtmöglichen Schutz bietet.

Immer up-to-date

Auf einem modernen Computer ist weit mehr als Betriebssystem und Office-Paket installiert. Eine Vielzahl an Programmen tummelt sich auf der Festplatte. Hier muss dafür gesorgt werden, dass ständig alle Sicherheitsupdates installiert sind. Werden Schlupflöcher für Angriffe bekannt, erscheinen meistens innerhalb weniger Stunden bis Tage Updates, die die Gefahr bannen. Wer hier nicht ständig auf dem aktuellsten Stand ist, macht

sich fahrlässig zur Zielscheibe. Im Besonderen sei noch das bei Hackern sehr beliebte Homebanking erwähnt. Achten Sie auch hier darauf, dass im Unternehmen das neueste Zugangsverfahren eingesetzt wird, das die Bank zum Einloggen bereitstellt.

Sichere Passwörter

Es ist ein oft besprochenes Thema. Die beste Verschlüsselung und die perfekt abgesicherte Schnittstellen, das alles nützt nichts, wenn das Passwort "123456" ist. Je komplexer - desto besser. Groß- und Kleinschreibung, Sonderzeichen, so viele Stellen wie möglich, nichts, was man in einem Wörterbuch finden kann... Es gibt viel zu beachten und Mitarbeiter schätzen die unmerkbaren Zugriffsdaten nicht besonders. Es gibt aber auch hier Möglichkeiten z.B. durch Passwort-Manager oder Tokens, damit dieses Kernstück jeder Sicherheitsstrategie wirklich in der Praxis umgesetzt wird.

Stand: 18.12.2018