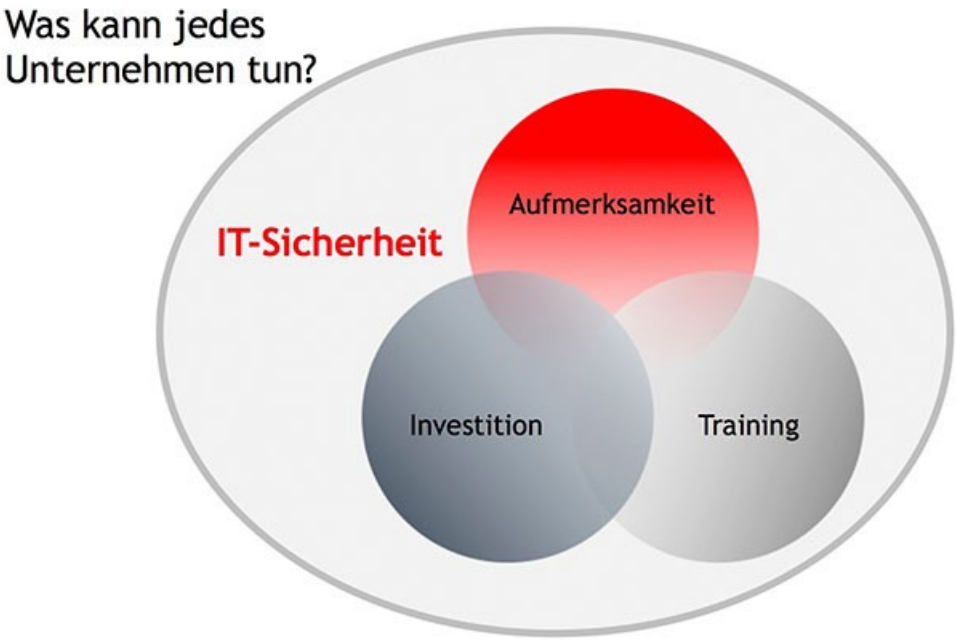
it-safe.at

it-safe: Achten Sie gerade jetzt auf Cybersicherheit!

IT-Sicherheitsstrategie: Was ist alles zu beachten?

So kommen Sie zu einer ganzheitlichen Lösung

Stand: 31.05.2017



360 Grad Sicherheit für die Unternehmens-IT sind mit technischen Maßnahmen allein unmöglich zu erreichen. Ein ganzheitlicher Strategieansatz stellt die individuellen Anforderungen im Unternehmen in den Mittelpunkt und berücksichtigt auch den Faktor Mensch.

In jedem Unternehmen werden wichtige, zum Teil sogar hochsensible Daten gespeichert. Der Verlust dieser Daten kann existenzbedrohend sein. Doch auch wenn solche Daten „nur" kompromittiert werden – also gestohlen und womöglich veröffentlicht – hat das für das Unternehmen zumeist unangenehme Folgen. Neben hohen Kosten für Ursachensuche, Information der Betroffenen, Rechtsberatung etc. drohen Geschäftsentgang, Kunden- und Reputationsverlust.

Immer mehr Geld in IT-Security-Technologien zu investieren nützt aber nur bedingt. Entscheidend ist, dass eine umfassende Sicherheitsstrategie dahintersteckt. Nur damit kann das Unternehmen langfristig deutlich an Sicherheit gewinnen.

Grenzen der Unternehmens-IT verschwimmen

Vor einigen Jahren genügten noch eine gute Firewall und ein aktueller Virenscanner und die Unternehmens-IT war weitgehend gegen Angriffe „von außen" geschützt. Doch seit dem Einzug von USB-Sticks und mobilen Geräten wie Smartphones und Laptops (Stichwort „BYOD") haben sich die Grenzen der Unternehmens-IT weit nach außen verschoben. Die Nutzung von Clouddiensten erweitert die Grenzen und zugleich die Verantwortung für die

Sicherheit der Unternehmensdaten noch einmal mehr. Auf wichtige unternehmensinterne Daten und Informationen wird von überall dort zugegriffen, wo die Mitarbeiter gerade arbeiten.

Durch technologische Absicherung und Überwachung wird 100-prozentige Sicherheit wohl niemals mehr zu erreichen sein – das geben auch ausgewiesene IT-Sicherheitsexperten zu bedenken. Hier kommt die umfassende Sicherheitsstrategie ins Spiel, welche genau auf die Bedürfnisse und Besonderheiten des Unternehmens zugeschnitten ist.

Ganzheitliche Strategie für die IT-Sicherheit

Eine wissenschaftlich häufig vertretene Ansicht ist, dass Sicherheit als Matrix zu sehen ist, bestehend aus den Aspekten

Aufmerksamkeit x Training x eingesetzte Mittel

Was ist damit gemeint? Alle drei Aspekte müssen sowohl in der strategischen Planung als auch im Unternehmensalltag gleichermaßen berücksichtigt werden. Selbst wenn die eingesetzten Mittel – also Investitionen in Sicherheitstechnologien – noch so ausgefeilt und auf dem aktuellsten Stand der Technik sind, werden sie nicht die optimale Wirksamkeit entwickeln können, wenn nicht zugleich auch alle Mitarbeiter geschult und regelmäßig trainiert werden.

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. Die Endverantwortung für IT- und Datensicherheit trägt letztendlich die Geschäftsführung.

Eine allgemeingültige Erfolgsformel für die Unternehmensstrategie gibt es dabei nicht, zu individuell sind die Anforderungen, gewisse Fixpunkte gibt es aber schon.

Bewusstsein schaffen – Sicherheitstraining

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 – Social Engineering nennt man diese Vorgehensweise. Schulungen und das Aufstellen von verbindlichen Verhaltensregeln sind unbedingt notwendig und auch gesetzlich vorgeschrieben.

Das richtige Verhalten während eines Sicherheitsvorfalles sollte zudem zumindest jährlich mit allen Mitarbeitern geübt werden. So ein Security-Update muss auch gar nicht knochentrocken daher kommen. Wie wäre es, wenn Sie zur Abwechslung ein Quiz daraus machen, bei dem es einen netten Preis zu gewinnen gibt?

Schnittstellen sichern – Einfallstore USB und WLAN

Es wäre alles so einfach, wenn man ein komplett in sich geschlossenes Computernetzwerk hätte. In Zeiten von USB-Sticks, mobilen Geräten und Cloudlösungen sind wir davon aber weit entfernt. Die folgenden Überlegungen sollten in die Sicherheitsstrategie einfließen.

USB-Sticks sind bequem, können aber böse Überraschungen bereithalten. Einerseits können vertrauliche Unternehmensdaten leicht gemeinsam mit dem USB-Stick verloren gehen. Andererseits können über die kleinen Wechseldatenträger auch alle denkbaren Arten von Schadprogrammen in das IT-Netzwerk eingeschleust werden. Im Rahmen der Sicherheitsstrategie sollte festgelegt werden, ob man solche Sticks z. B. komplett aussperrt oder nur gesicherte oder verschlüsselte Speicher des Unternehmens zulässt. Die Lösung sollte jedenfalls zum Unternehmen passen und auch wirklich umsetzbar sein.

Noch größer ist mittlerweile das Risiko des WLAN. Das kabellose Internet bietet viel Komfort, ist aber zugleich auch einer der anfälligsten Einfallpunkte für Angriffe auf Unternehmen. Beim Aufsetzen des Firmen-WLAN sind entsprechend abgesicherte Router-Einstellungen zu beachten. Unternehmensintern sollte der Zugriff auf besonders sensible Daten via WLAN besser nicht möglich sein. Für externe Personen (Gäste, Handwerker etc.) ist ein separates Netz (Gäste-WLAN) sinnvoll.

Mobiles Risiko – Smartphone und Cloud im sicheren Griff

„BYOD" (Bring Your Own Device) ist der Albtraum jedes Sicherheitsexperten, gleichzeitig aber aus dem Unternehmensalltag nicht mehr wegzudenken.

Vor allem Smartphones werden von Mitarbeitern oft sowohl beruflich als auch privat genutzt. Riskant daran ist das unkontrollierte Installieren von Apps aus unbekannten Quellen, die versteckte Schadcodes enthalten können. Zugleich kommt das Gerät weit herum und ist dabei oft auch in unsicheren Netzwerken (z. B. öffentliches WLAN) unterwegs. Überlegenswert wäre daher, eine Trennlinie zwischen privater und beruflicher Nutzung zu ziehen. Dafür gibt es spezielle Software, mit der auch Geräte unterschiedlicher Betriebssysteme zentral verwaltet und der Zugang zu Firmendaten kontrolliert werden kann.

Mit Smartphone und Tablet haben auch verschiedene Cloud-Anbieter und -Dienste die Unternehmen erreicht. Große Dateien können so bequemer ausgetauscht und sogar gemeinsam bearbeitet werden. Allerdings kann auch diese Vorgehensweise zu beträchtlichen Risiken führen. 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. Viele Clouddienste bieten für den Business-Bereich gegen geringe Gebühren deutlich bessere Sicherheitseinstellungen als in der Gratis-Version. Hier empfehlen wir heimischen Anbietern mit einem Rechenzentrum innerhalb der EU der Vorzug zu geben.

Immer up-to-date – Sicherheits-Updates sofort installieren

Auf jedem 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 immer alle Sicherheitsupdates installiert sind, auch wenn die tagtäglichen Aktualisierungen auf den ersten Blick lästig erscheinen. Werden Schlupflöcher für Angriffe bekannt, erscheinen meistens innerhalb weniger Stunden bis Tage Updates, die die Gefahr für Geräte und Netzwerke bannen. Wer hier nicht ständig auf dem aktuellsten Stand ist, macht sich fahrlässig zur Zielscheibe. Im Besonderen sei noch die für Hacker besonders attraktive Zielscheibe namens E-Banking erwähnt. Achten Sie hier ganz besonders darauf, dass im Unternehmen das aktuellste Zugangsverfahren eingesetzt wird, das die Bank zum Einloggen und Unterzeichnen der Aufträge bereitstellt.

Sichere Passwörter

Es ist ein oft besprochenes Thema. Die beste Verschlüsselung und perfekt abgesicherte Schnittstellen, das alles nützt nichts, wenn das Passwort "123456" ist. Je komplexer - desto besser. Groß- und Kleinschreibung, Sonderzeichen, mindestens 8-12 Stellen, keine Wörter aus dem Wörterbuch – die besten Passwort-Tricks.

Mitarbeiter schätzen die unmerkbaren Zugriffsdaten meist nicht besonders und „erleichtern" sich die Arbeit indem sie Passwortphrasen auf Post-its notieren. Hier gibt es die Möglichkeit z.B. Passwort-Manager oder Tokens einzusetzen, damit dieses Kernstück jeder Sicherheitsstrategie wirklich in der Praxis umgesetzt wird.

Virenschutz, Firewall, Back-up: Die Basics nicht vergessen!

Virenschutz und Firewall zählen zu den technischen Mindestanforderungen für jedes Unternehmen. Virenschutzprogramme überprüfen jede neue Datei auf Anzeichen einer Infektion und verhindert so, dass Schadprogramme geöffnet und installiert werden. Da täglich neue Schädlinge auftreten können, muss die Antiviren-Software immer auf dem aktuellen Stand sein und daher regelmäßig upgedatet werden. Eine Firewall kontrolliert alle Daten, die zwischen internen Firmennetzwerk und externen Netzwerken ausgetauscht werden. Einige Betriebssysteme besitzen bereits eine integrierte Firewall. Weitere Praxistipps zu Virenschutz und Firefall.

Neben den grundlegenden Security-Elementen Virenscanner und Firewall gehört ein Back-up zu den Pflichtaufgaben jeder Unternehmerin und jedes Unternehmers. Der Gesetzgeber verlangt dabei, dass auf den gegenwärtigen Stand der Technik Rücksicht genommen wird. Back-up ist also Pflicht und nicht bloß eine Option und liegt auch in ihrem eigenen unternehmerischen Interesse. Das Back-up dient der Datensicherung, es stellt im Falle eines Hardware-Defekts oder Datenverlustes ein Medium zur Wiederherstellung der Daten bereit.