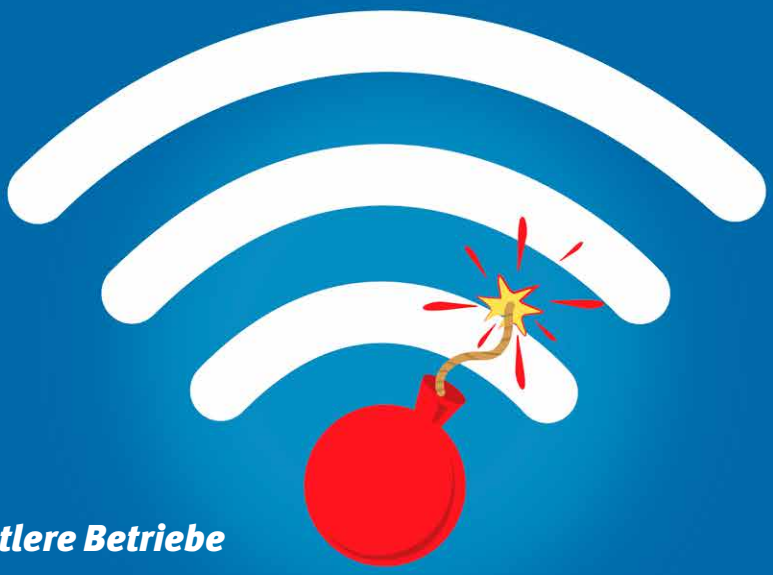


IT-Sicherheit für kleinere und mittlere Betriebe

Wie sich Unternehmen schützen können

Um ein Unternehmen, eine Behörde oder eine andere Einrichtung innerhalb kürzester Zeit in seiner Arbeitsfähigkeit empfindlich einzuschränken oder gleich ganz außer Gefecht zu setzen, braucht es heutzutage nicht viel. Beinahe jede Woche flimmern neue Meldungen über entsprechende Ereignisse über die Bildschirme – wenn man das Glück hat, über den eigenen Bildschirm noch eine Meldung flimmern sehen zu können!

In jüngster Zeit hat die Schadsoftware Emotet häufig für Schlagzeilen gesorgt. Unter anderem legte sie kürzlich mehrere Ämter der Stadtverwaltung Neustadt am Rübenberge lahm: Kraftfahrzeuge zulassen, Personalausweise beantragen und viele andere Services, die zu den Kernaufgaben einer Verwaltung zählen, waren tagelang nicht ausführbar. Noch bedrohlicher erscheint es, wenn Emotet auch vor medizinischen Einrichtungen nicht haltmacht, wie ebenfalls im September bei der Medizinischen Hochschule in Hannover geschehen.

▲ Der Dalldorfer Sicherheitsexperte Frank Bahn warnt vor Angriffen aus dem Netz.

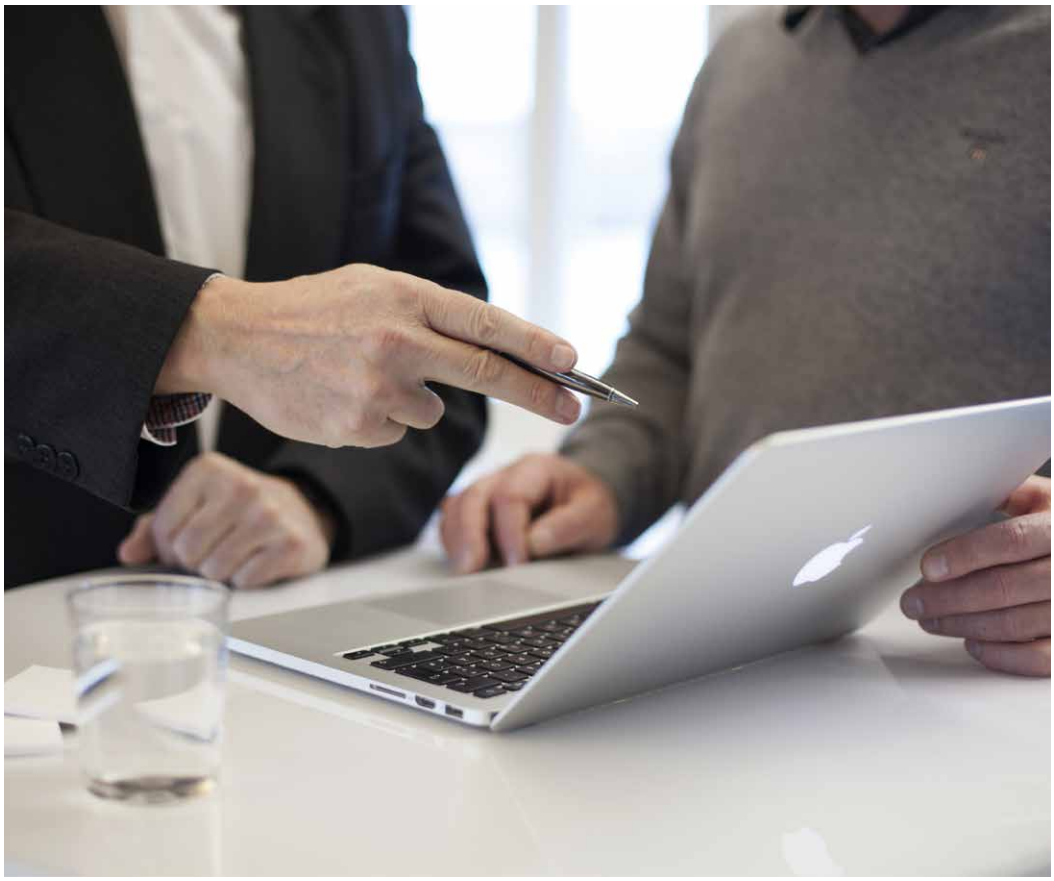
Hundertprozentige Sicherheit gibt es nicht

„Jedes Unternehmen kann Opfer eines gezielten Angriffs werden. Aktuelle Bedrohungsszenarien haben ein nie gesehenes professionelles Niveau erreicht“, weiß IT-Sicherheitsexperte Frank Bahn. Ein klassisches Antivirenprogramm garantiere ebenso wenig ausreichenden Schutz gegenüber solchen Angriffen wie eine Geldkassette im Laden. Darüber hinaus zeige die Erfahrung, dass es häufig nicht am Werkzeug mangele, sondern am fehlendem Sicherheitsbewusstsein der Verantwortlichen. „Mangelndes Sicherheitsbewusstsein belegt als Bedrohung für Unternehmen in den meisten Statistiken zur IT-Kriminalität die obersten Plätze. Diese Unternehmen sollten ihr Geld in erster Linie in die Schulung ihrer Mitarbeiter investieren und nicht in kostenintensive, aber relativ nutzlose Werkzeuge der sogenannten Schlangenöl-Industrie“, rät der Sicherheitsexperte.

Schritt 1: Relevante Unternehmenswerte identifizieren

Der erste Schritt für ein Sicherheitskonzept besteht darin, dass Unternehmen sich darüber klar werden, welche ihrer Werte besonders schützenswert sind. Diese Werte sind für jedes Unternehmen andere. Nur wer weiß, welches seine existenziell wichtigen Kernprozesse sind und versteckte Technologieabhängigkeiten kennt, kann diese gezielt und mit vertretbarem Aufwand sichern. Frank Bahn führt einige Beispiele an: „Während es für eine Arztpraxis oder ein Versicherungsunternehmen existenzbedrohend werden kann,

wenn Patienten- oder Versichertendaten durch einen Verschlüsselungstrojaner wie Emotet unwiederbringlich verloren sind, ist es für den Pizzabringdienst ein Riesenproblem, wenn das Bestellsystem oder die Kreditkartenbuchung per Internet nicht funktioniert. Ein Juwelier dagegen wird empfindlich getroffen, wenn seine teure smarte Alarmanlage mittels einfacher Manipulation der WLAN-Kommunikation außer Dienst gestellt wird und die Täter unbemerkt den Laden ausräumen. Eine Analyse mag aufwendig sein, doch am Ende spart sie viel Geld, schafft eine solide Sicherheitsbasis und lässt den Unternehmer ruhiger schlafen."



Schritt 2: Schwachstellen und Bedrohungen erkennen

Selbst für große Unternehmen, die überzeugt sind, viel Zeit, Geld und Know-how in ihre Unternehmenssicherheit investiert zu haben, ist es oftmals ein Schock, wenn sie sich einem Selbsttest durch einen externen Sachverständigen unterziehen. „Da passiert ein Unbefugter mit ein bisschen Frechheit und der Chipkarte eines ‚Kollegen' Sicherheitskontrollen und dringt in mehrfach gesicherte Räume vor. Ein geschickt platzierter USB-Stick mit der Aufschrift ‚Gehälter 2019', der leider auch Schadsoftware enthält, landet innerhalb von Minuten im Firmennetzwerk, und sensible Kundendaten auf dem Bildschirm eines Sachbearbeiters sind innerhalb von ein paar Sekunden auf dem Weg ins Internet. Vom berühmten Klick auf das

Werbung

Analyse relevanter Unternehmens-werte mittels CIA-Kriterien:

C wie Confidentiality (Vertraulichkeit): Betrifft zum Beispiel Unternehmen, die ihr Geld mit geheimem Wissen (Rezepte, Patente, Preislisten, wertvolle Kundendaten) verdienen und die einen großen wirtschaftlichen Schaden erleiden, wenn dieses Wissen das Unternehmen verlässt.

I wie Integrity (Integrität): Betrifft Unternehmen, die mit sensiblen Daten, auch von Dritten, arbeiten und deren Geschäftsmodell auf Vertrauen beruht (Manipulation der Buchhaltung zum Schaden der Kunden, betrügerische Finanztransaktionen zum Vorteil des Mitarbeiters und in Behörden unerlaubte Abfragen der Polizei- oder von Verwaltungsdatenbanken durch Beamte).

A wie Availability (Verfügbarkeit): Betrifft Unternehmen, die sich in starker Abhängigkeit zu Fremdsystemen und -dienstleistern befinden (Internet, Cloud, Telefon). Besondere Sicherheitsrisiken sind dabei beispielsweise mangelhafte Backupverfahren, die Nutzung von Cloud-Diensten (wenn Office 360 nur online funktioniert, der Zugriff auf Unternehmensdaten durch Externe gesperrt werden kann etc.). ■

Katzenfoto im Mail-Anhang ganz zu schweigen! Wer es darauf anlegt und ein bisschen geschickt ist, muss nicht viel Energie aufwenden, um ein Unternehmen empfindlich zu treffen“, weiß der IT-Sicherheitsexperte. Doch es gibt noch weitere klassische Handlungsfelder für Sicherungsmaßnahmen, die in vielen Unternehmen einen blinden Fleck bilden: „Sicherheitsrelevante Prozesse sind nicht oder nur unzureichend dokumentiert, Verantwortlichkeiten für IT und Sicherheit nicht klar geregelt, Abhängigkeiten sind nicht hinreichend bekannt und dokumentiert. Von Notfallplänen, wenn der Schaden erst eingetreten ist, ganz zu schweigen.“

Schritt 3: Gezielte Maßnahmen ergreifen

Als größtes Hindernis eines funktionstüchtigen Sicherheitskonzepts identifiziert Frank Bahn Bequemlichkeit und die Einstellung, dass Sicherheit teuer und lästig sei. „Die Geschäftsleitung muss das Thema Sicherheit vorleben und fördern. Die Botschaft muss lauten: Sicherheit schützt das Unternehmen und den eigenen Arbeitsplatz!“ Für ihn ist der menschliche Faktor sogar bei digitalen Selbstverteidigungsstrategien Dreh- und Angelpunkt eines jeden Sicherheitskonzeptes. „Mitarbeiter sind das Kapital des Unternehmens. Die Investition in ihre digitale Kompetenz erhalten Unternehmen doppelt und dreifach zurück“, ist sich Frank Bahn sicher.

Neben präventiven Maßnahmen müsse ein Sicherheitskonzept auch die Frage beantworten

können, wie Ausfälle von Teilen des Systems kompensiert werden können. „Für jede überlebenswichtige Ressource muss es ein Backup geben“, erklärt der Sicherheitsexperte. „Backup heißt Ausfallsicherheit. Es betrifft nicht nur wichtige Daten, sondern auch den Mitarbeiter mit einzigartigen Fähigkeiten oder Spezialwissen, es betrifft die überlebenswichtige Infrastruktur oder entsprechende Maschinen.“

Ein Notfallplan rundet das Gesamtkonzept ab. „Jedes Unternehmen sollte sich eine zentrale Frage stellen und beantworten können: Wo und vor allem mit was (Hardware, Daten etc.) machen wir morgen früh weiter, wenn heute Nacht die Hütte abbrennt? Dabei ist irrelevant, ob es sich wirklich um ein Feuer handelt oder um einen rein digitalen (Daten-)Verlust. Das Ergebnis kann dasselbe sein.“

Vorlagen für Notfallpläne gibt es sogar im Internet. Empfehlenswert sind diesbezüglich die Seiten des Bundesamtes für Sicherheit in der Informationstechnik unter www.allianz-fuer-cybersicherheit.de

Grafiken: Pixabay – GraphicsSC, Renee Gaudet, Christoph Meinersmann, bertholdbrodersen / Gesa Walkhoff

Zusammenfassung

„IT-Sicherheit ist in erster Linie keine Frage des Geldes, sondern des soliden Sicherheits-Bewusstseins“, sagt IT-Sicherheitsexperte Frank Bahn. „Die schlechte Nachricht lautet: Egal wie viel Geld ein Unternehmen in IT-Sicherheit investiert - ein Restrisiko wird immer bleiben. Die gute: Mit gesundem Menschenverstand, einem geschulten Sicherheitsbewusstsein und dem Wissen, was im Notfall getan werden muss, können Unternehmen viel für ihre Sicherheit tun, auch ohne Unsummen für IT-Sicherheitssysteme auszugeben.“ ■

Werbung