Cyber-Alarm – 10 Tipps, wie Sie Ihre Daten schützen

Kleine und mittelständische Unternehmen geraten zunehmend in das Visier krimineller Hacker. Schwerwiegende Angriffe werden immer häufiger. Kein Unternehmen kann zwischenzeitlich Cyber-Risiken ausschließen! Jeder kann Opfer von Spionage, Sabotage oder Datendiebstahl werden. Die kriminelle Bedrohung hat enorm zugenommen: Mittlerweile berichten Medien fast täglich über Cyber-Angriffe. Gerade die Cyber-Angriffe WannaCry und Petya haben gezeigt, wie verwundbar unser digitalisierte Gesellschaft ist und welches Schadenpotenzial für die Wirtschaft bei mangelnder Absicherung droht. Ein sicherheitsbewusster Umgang mit digitalen Endgeräten und Daten ist daher unerlässlich. Schließlich müssen Sie Ihre sensiblen Unternehmens- und Kundendaten jederzeit schützen.
Cybersicherheit ist Chefsache! Sich nicht kümmern kann teuer werden.

Folgende 10 Tipps für mehr IT-Sicherheit können Sie in Ihrem Unternehmen nahezu kostenfrei leicht umsetzen!

1 Verwenden Sie lange Passwörter – und für jede Anwendung ein eigenes. Ein sicheres Passwort spielt eine elementare Rolle für den Schutz Ihrer Daten. Es hat eine angemessene Länge von 8 Stellen, besser sind 10 bis 15 Zeichen. Außerdem sollte es sowohl Groß- und Kleinbuchstaben ohne Umlaute, als auch Ziffern von 0-9 und Sonderzeichen (z.B. #, $, &,?) enthalten. Vorsorgend sollten Sie auch darauf achten, dass Ihr Passwort keine personenbezogenen Daten (z.B. Namen von Familienmitgliedern oder von Haustieren) enthält. Achten Sie darauf, dass Sie Ihr Passwort in regelmäßigen Abständen (z.B. alle 6 Monate) ändern. Bei der Erstellung eines neuen Passwortes sollte kein bereits einmal verwendetes Passwort gewählt werden.

2 Machen Sie regelmäßig Updates der verwendeten Programme: So schließen Sie Sicherheitslücken. Diese Maßnahme schützt vorbeugend und effektiv. Denn ein Virenscanner kann immer nur auf bereits bekannte Viren reagieren. Auch ein aktuelles Betriebssystem und ein verantwortungsvoller Umgang mit dem Internet sind wichtig.

3 Führen Sie regelmäßige Backups durch – das schützt vor unwiderruflichem Verlust der Daten. Gründe für Datenverluste gibt es viele: Überspannung, normale Festplattenschäden, unabsichtliches Löschen oder Virenbefall. Überlegen Sie, welche Daten wirklich wichtig sind und unbedingt gesichert werden müssen. Sicherungsrelevante Daten

stellen oftmals kritische Daten wie Passwörter, Zugangsdaten, selbst entwickelte Programme, Software- Lizenzen und Kundendaten dar.

4 Seien Sie wachsam bei E-Mails. E-Mails von unbekannten Absendern oder mit einem verdächtigen Inhalt sollten Sie auf keinen Fall öffnen – auch die Anhänge nicht. Darin verstecken sich oft Viren, die auf Ihrer Festplatte Schäden anrichten können Falls Rechner von einem schädlichen Computerprogramm befallen sind, versenden diese Rechner automatisch E-Mails an das gesamte Adressbuch. Die Mails stammen somit nicht immer von unbekannten Absendern. Seien Sie demnach ebenfalls bei den Ihnen bekannten Absendern wachsam.

5 Rufen Sie Websites für Online Banking oder Finanzdienstleistungen jedes Mal direkt auf. Folgen Sie keinen Links in E-Mails. Auf diese Weise verhindern Sie, auf einer gefälschten Seite zu landen. Loggen Sie sich immer aus und schließen Sie die Anwendung sowie das Browserfenster jedes Mal am Ende Ihrer Sitzung.

6 Vorsicht im öffentlichen WLAN: Um sich vor Cyber-Angriffen zu schützen, sollten Sie entweder nicht in öffentlichen WLAN- Netzen surfen oder sich zumindest währenddessen nicht in Ihren E-Mail- Account einloggen. Wenn es sich jedoch nicht vermeiden lässt, achten Sie darauf, statt des öffentlichen WLAN die Internetverbindung Ihres Mobilfunknetzes zu verwenden. So können Sie vermeiden, dass Angreifer auf die Daten Ihrer Sitzung zugreifen können.

7 Schützen Sie sich vor der Bedrohung durch Erpresserprogramme. Ransomware breitet sich derzeit mit rasanter Geschwindigkeit aus. Dabei schleusen Angreifer Ransomware zum Beispiel über E-Mail- Anhänge in die Computer ein und lassen sie dort Dateien verschlüsseln. So werden Dokumente, Fotos, E-Mails oder sogar komplette Datenbanken unbrauchbar. Erst gegen Zahlung eines Lösegeldes (Ransom) werden die Daten wieder freigegeben. Das BSI (Bundesamt für Sicherheit in der Informationstechnik) rät ausdrücklich, kein Lösegeld zu zahlen, da so die Weiterentwicklung dieser Schadsoftware unterstützt und eine größere Verbreitung dieser Software gefördert wird.

8 Alle, die in Ihrem Büro arbeiten, sollten über Ihre IT-Richtlinien informiert sein. Viele Datenpannen passieren nicht wegen böser Absichten, sondern aufgrund von Unwissenheit und Sorglosigkeit. Deshalb sind regelmäßige Unterweisungen und Datenschutz-Schulungen sehr wichtig. Nur wenn Ihre Mitarbeiter verbindliche Vorgaben für die Nutzung und Sicherheit der Datenverarbeitung erhalten, sie verstehen

und umsetzen können, verbessert das die Sicherheit Ihrer Daten. Sorgen Sie für Transparenz, klare Richtlinien und Anweisungen.

9 Überwachen Sie externe Zugänge mobiler Endgeräte Smartphones usw. zum Netzwerk, um eine unbefugte Nutzung zu verhindern.

10 Beginnen Sie noch heute mit Ihrer persönlichen Cyber-Security-Offensive! Führen Sie aktiv schützende Maßnahmen zur Cyber-Abwehr durch. IT- Sicherheit ist kein Zustand, sondern ein Prozess: Achten Sie darauf, dass Sie notwendige Maßnahmen zur dauerhaften Gewährleistung Ihrer IT- Sicherheit in regelmäßigen Abständen wiederholen und gehen Sie verantwortungsbewusst mit Ihren Daten um. Der Aufwand lohnt sich.

Auch moderne und hochaktuelle Virenschutzprogramme und Firewalls können nicht jede Malware abwehren. Kein Unternehmen kann Cyber-Risiken mehr ausschließen! Keine Technik ist perfekt!

Sichern Sie sich gegen Folgen eines erfolgreichen Cyber-Angriffs mit einer Cyber-Versicherung ab. Sie können die finanziellen Folgen von Eigenschäden, Drittschäden und Erpressung / Lösegeld absichern.