Tipps und Hinweise

Cyber-Kriminalität und IT-Risiken:
Die wachsende Bedrohung für Unternehmen.

Cyber-Attacken gehören für Betriebe und Unternehmen zu den höchsten Risikofaktoren. Ein angemessenes IT-Sicherheitskonzept ist die Voraussetzung für eine wirksame Reduzierung der Gefahr durch Cyber-Kriminalität. Deswegen haben wir Ihnen einige Tipps und Hinweise zusammengestellt.

Grundsätze und Mindestanforderungen

- Datensicherheit ist Chefsache! Deshalb muss die Verantwortung für dieses Thema in der Geschäftsführung verankert sein.
- Verwenden und aktualisieren Sie regelmäßig Ihre Antivirensoftware. Lassen Sie den Virenscanner im Hintergrund laufen. Dateien werden so bei Zugriff gescannt.
- Verwenden Sie nur Software, die vom Hersteller regelmäßig gepflegt wird.
- Übernehmen Sie sicherheitsrelevante Patches (Updates) der Softwarehersteller über die automatische Update-Funktion.
- Sichern Sie Ihre Daten mindestens einmal wöchentlich auf einem separaten Datenträger. Bewahren Sie mindestens die letzten drei Sicherungen auf.
- Um zusätzliche Sicherheit zu gewährleisten, sollte darüber hinaus je Quartal mindestens eine Vollsicherung auf einem separaten Datenträger durchgeführt werden. Überschreiben Sie die längerfristige Datensicherung frühestens nach vier Quartalen.
- Testen Sie regelmäßig den Notfall: Können die gesicherten Daten auch wieder auf die Anlage zurückgespielt werden?
- IT-Risiken müssen klar kommuniziert werden. Sensibilisieren Sie Ihre Mitarbeiter.

W&W württembergische

Ihr Fels in der Brandung.

Darüber hinaus gibt es weitere Ansätze, um Ihre Daten und die Ihrer Kunden vor unliebsamen Überraschungen zu schützen.

Organisatorische Maßnahmen
- Verwenden Sie für jeden Nutzer und Administrator benutzerindividuelle, ablaufende Passwörter. Schützen Sie auch Ihre Daten auf mobilen Geräten mit einem Passwort. Sperren Sie Rechner und mobile Geräte bei Inaktivität automatisch.
- Datenschutz: Achten Sie auf die sichere Entsorgung von Papier und Datenträgern (Festplatten, USB-Sticks etc.).

Präventive Maßnahmen
- Öffentliche WLAN-Netze sind unsicher. Geben Sie keine vertraulichen Daten wie Passwörter und Kontodaten ein, solange Sie einen öffentlichen Netzwerkzugang nutzen.
- Schützen Sie Ihren Server im Idealfall durch eine physische Zutrittsbeschränkung zum Server-Raum.
- Prüfen Sie, ob Sie digitale Medieninhalte (beispielsweise Bilder) veröffentlichen dürfen.

Absicherung des IT-Netzwerkes
- Schützen Sie Ihren elektronischen Firmenzugang durch eine für Ihr Unternehmen geeignete Firewall, durch VPN-Zugänge oder ähnliches. Im Idealfall als eigenständige Hardware-Firewall, die nicht im DSL-Router integriert ist.
- Richten Sie für Ihr WLAN mindestens eine WPA2-Verschlüsselung ein.

Umgang mit mobilen Geräten
- Schalten Sie bei mobilen Geräten (Smartphone, Tablet, Laptop etc.) die Bluetooth- oder WLAN-Funktion Ihres Endgerätes nur ein, wenn Sie diese bewusst zur Kommunikation einsetzen.
- Schließen Sie keine USB-Sticks, SD-Karten und andere Speichermedien von nicht vertrauenswürdigen Quellen an einen Rechner an.

Tipps zu sicheren Passwörtern
- Ein gutes Passwort sollte mindestens acht Zeichen lang sein (je länger, desto sicherer) und aus Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern bestehen.
- Es sollte nicht in Wörterbüchern vorkommen, gängige Tastatur- oder Ziffernfolgen sind tabu.
- Die meisten Browser bieten die Möglichkeit, Passwörter für bestimmte Webseiten zu speichern. Darauf sollten Sie und Ihre Mitarbeiter verzichten, denn in der Regel werden die Passwörter unverschlüsselt auf dem Computer gespeichert.
- Den besten Schutz bieten Passwort-Manager. Sie erstellen auf Wunsch zufallsgenerierte Passwörter und speichern diese in einer verschlüsselten Datenbank ab.

Schutz vor Schadsoftware
- Verwenden Sie Software und Links nur aus vertrauenswürdigen Quellen. Gehen Sie mit Downloads von Programmen, Bildschirmschonern und Daten-Dateien aus dem Internet sorgsam um. Diese können Trojaner und Viren enthalten.

Sicherung der Daten
- Die Sicherungsdatenträger müssen eindeutig gekennzeichnet sein und der Zeitpunkt der Datensicherung nachvollziehbar dokumentiert werden.
- Die Sicherungsdatenträger sollten mit einem Passwort geschützt werden. Die Sicherungsdatenträger sollten nur zur Datensicherung mit dem Netzwerk verbunden werden und ansonsten vom Netzwerk getrennt sein.
- Lagern Sie Ihre Sicherungsdatenträger in einem anderen Gebäude oder in einem geeigneten Datensicherungsschrank.

Sicherheitsnetz mit der Cyber-Police
Die Einhaltung dieser Maßnahmen verringert zwar die Möglichkeit einer Cyber-Attacke, völlig ausschließen lässt sich diese Gefahr jedoch nicht. Die Cyber-Police der Württembergischen schützt Unternehmen vor den Folgen von Cyber-Risiken – sowohl finanziell als auch mit Rat und Tat an unserem Cyber-Service-Telefon.

Wir beraten Sie gerne.

Württembergische Versicherung AG

91472 [2] 11/2018