AS infotrack

IT-Sicherheit für Ihr KMU und Zuhause

Kundendaten, Personaldaten, Firmengeheimisse, Strategiepapiere, Konzepte, Bilder, Skizzen, Angebote – all das und noch viel mehr wollen Sie vor unbefugtem Zugriff schützen. Immer wieder werden Fälle bekannt, wo Daten aufgrund von Cyberkriminalität gestohlen, verschlüsselt oder horrende Summen für die Freigabe gefordert werden. Solche Unannehmlichkeiten und negative Schlagzeilen will man sich ersparen.

Vorab: Der perfekte Schutz gibt es nicht. Sie können jedoch die Sicherheit und somit die Hürden für einen Datenmissbrauch erhöhen. Oft wird nicht in Häuser eingebrochen, die eine Alarmanlage installiert haben, denn die Kriminellen wählen nach Möglichkeit den einfacheren Weg und nutzen Gelegenheiten.

Der Bund bietet Informationen für die Informationssicherheit von KMU und die Melde- und Analysestelle zur Informationssicherung (MELANI) informiert über aktuelle Vorkommnisse. Zudem geben Anbieter von Schutz-Software Empfehlungen zu Datenschutz und Datensicherung heraus. Wir haben Ihnen das Wichtigste kompakt zusammengestellt.

Bei der Wahl der Massnahmen gilt es immer zu entscheiden, ob Ressourcen aufgewendet werden sollen oder ob man das entsprechende Restrisiko auf sich nimmt. Bedenken Sie auch die Kosten, die bei einem Produktionsstillstand oder einem allfälligen Imageschaden entstehen können. Bei Unsicherheit empfehlen wir Ihnen auf Fachspezialisten zurückzugreifen, die Ihnen beratend und unterstützend zur Seite stehen können.

Auf organisatorischer Ebene sind vor allem die zwei nachfolgenden Punkte zu beachten.

1. **Regeln Sie die Verantwortlichkeiten für Ihre IT-Sicherheit**
   a. Wer ist für Ihre Mitarbeitenden der Ansprechpartner?
   b. Wer ist zuständig für die Datensicherung und kontrolliert diese regelmässig?
   c. Was machen Sie inhouse und wozu ist Ihr IT-Dienstleister zuständig?
   d. Wer schult Ihre Mitarbeitenden im Umgang mit der IT-Infrastruktur und sensiblen Daten?
   e. Wer ist für die Erteilung von Berechtigungen zuständig und werden Berechtigungen und Zugriffe regelmässig kontrolliert?
   f. Wer informiert sich über aktuelle Bedrohungen und mögliche Datenlecks?

2. **Stellen Sie IT- und Datenschutz-Reglemente, Checklisten und andere Hilfestellungen für Ihre Mitarbeitenden zur Verfügung.**
   a. Definieren Sie Passwort-Regeln (Anz. Zeichen; Kombination von Gross- & Klein-Buchstaben, Ziffern und Sonderzeichen).
   b. Verwenden Sie nach Möglichkeit eine Zwei-Faktor-Authentifizierung (z.B. eigenes Passwort & Code-Versand per SMS).
   c. Legen Sie den Prozess fest, falls Unregelmässigkeiten bemerkt werden (seltsame E-Mails & Anrufe, fehlende Daten, usw.).
   d. Geben Sie Ihren Mitarbeitenden Tipps und Checklisten zur Hand, wie sie mit der Hardware und den Daten umgehen sollen.

Auf technischer Ebene sind die folgenden Massnahmen in Kombination sinnvoll. Diese gelten ebenfalls für den privaten Gebrauch.

3. **Aktueller Virenschutz**
   a. Installieren Sie auf allen Geräten eine Virenschutz (z.B. Microsoft Defender, Kaspersky).
   b. Führen Sie regelmässig einen Systemscan durch, um mögliche Schadsoftware aufzudecken (wöchentlich, monatlich).
   c. Aktualisieren Sie regelmässig Ihren Virenschutz, um auch neuartige Angriffe zu erkennen.

4. **Regelmässige Datensicherung**
   a. Verfolgen Sie die 3-2-1 Backup-Regel (erstellen Sie 3 Kopien auf 2 unterschiedlichen Medientypen und lagern Sie 1 Kopie physisch aus).
   b. Machen Sie die Datensicherung täglich, wöchentlich und monatlich.
   c. Prüfen Sie regelmässig, ob die Datensicherung funktioniert hat.
   d. Bewahren Sie Vorgängerversionen für eine gewisse Zeit auf.
   e. Üben Sie das Einspielen von Backups oder holen Sie sich dafür Unterstützung.

5. **Aktualisieren Sie Ihre Software**
   a. Spielen Sie regelmässig Updates ein, um allfällige Sicherheitslücken zu schliessen.
   b. Beachten Sie ALLE Software (ERP, Betriebssystem für PC und Smartphones, Browser, CMS, Adobe Reader, Drucker-Software, usw.)
   c. Automatisieren Sie Updates nach Möglichkeit.

6. **Korrekter Umgang mit E-Mails**
   a. Blockieren Sie E-Mails mit potenziell schädlichen Anhängen.
   b. Öffnen Sie nur vertrauenswürdige Anhänge von bekannten Absendern.
   c. Informieren Sie sich bei MELANI über gefährliche E-Mail-Anhänge (z.B. ZIP, RAR, ISO)
   d. Seien Sie vorsichtig bei E-Mail Anhängen, die Makros enthalten könnten (z.B. Word, Excel, PowerPoint, PDF)

7. **Netzwerk schützen**
   a. Installieren Sie in jedem Netzwerk eine Firewall (z.B. WatchGuard, Cisco, FortiGate).
   b. Sichern Sie Remote-Zugänge von externen Mitarbeitenden und alle extern zugänglichen Dienste mit einem zweiten Faktor (z.B. One-Time-Password, Token)
   c. Gewähren Sie nur Fernzugriff, wenn dieser wirklich benötigt wird.

8. **Physische Zugänge schützen**
   a. Installieren Sie einen Einbruchschutz, eine Alarmanlage und einen Brandschutz. Verwenden Sie gegebenenfalls einen Schliessplan.
   b. Sperren Sie Computer und Smartphones, wenn Sie nicht vor Ort sind.
   c. Verwenden Sie sichere Passwörter und notieren Sie diese nicht.
   d. Lassen Sie den gesunden Menschenverstand walten. Geben Sie keine Passwörter bekannt, prüfen Sie Absender, Anrufer oder vermeintliche Servicetechniker, die ohne Terminvereinbarung auftauchen.

Wir wünschen Ihnen viel Erfolg bei der Umsetzung Ihrer IT-Sicherheits-Massnahmen.

Unser Angebot

Wenn wir Sie als IT-Partner bei der Analyse, Produkt-Wahl oder Umsetzung unterstützen können, sind wir gerne für Sie da.

Andreas Gurtner
Bereichsleiter ICT-Services

+41 62 768 50 60
andreas.gurtner@asinfotrack.ch