RAIFFEISEN

5 Punkte für Ihre Cybersicherheit

Mit diesen fünf Punkten können Sie für die Cybersicherheit in Ihrem Unternehmen sorgen:

---

1. **Technische Schutzmassnahmen vornehmen**
   Zu den Massnahmen zum Schutz Ihrer IT gehören einerseits Firewalls, Antivirus-Software sowie regelmässige Software-Updates, damit bekannte Sicherheitslücken geschlossen werden. Aber auch physische Vorkehrungen sind wichtig, etwa Zugangsbeschränkungen und Überwachungskameras in IT- und Server-Räumen sowie Systeme für Brand- und Wasserschutz.

2. **Regelmässige Backups der Daten erstellen**
   Regelmässige Datensicherung ist ein Muss. Am besten automatisieren Sie Ihre Backups und beachten die 3-2-1-Regel:
   - dreifache Kopie aller Firmendaten
   - zwei unterschiedliche Medien für die Speicherung (zum Beispiel Cloud und Festplatte)
   - eine aktuelle Kopie physisch ausserhalb der Firmenräume gelagert

   Prüfen Sie regelmässig, ob Ihre Daten vom Backup rasch wieder auf die Firmensysteme gespielt werden können.

3. **Bewusstsein für Cyberkriminalität schaffen**
   Eines der grössten Cyberrisiken in Ihrem Unternehmen sind Ihre Mitarbeitenden – etwa weil sie ungenügende Passwörter benutzen oder Links und Attachments in Phishing-Mails anklicken. Informieren Sie deshalb neue Mitarbeitende gleich beim Onboarding darüber, was in Sachen Cybersicherheit in Ihrem Unternehmen gilt. Führen Sie regelmässige Schulungen für alle durch. Erstellen Sie eine verbindliche Passwortrichtlinie und führen Sie für wichtige Zugangspunkte zu Ihrer Infrastruktur eine Zwei-Faktor-Authentifizierung ein. Vergessen Sie bei allen Sicherheitsvorkehrungen die mobilen Geräte nicht.

4. **Notfallplan erstellen**
   Falls doch einmal etwas passieren sollte, ist ein Notfallplan essenziell. Stellen Sie sicher, dass die ganze Belegschaft ihn kennt und weiss, welche Art Vorfälle ein Sicherheitsrisiko darstellen können. Ihr Notfallplan sollte insbesondere folgende Punkte enthalten:
   - Kontaktdaten der Person oder Stelle, die im bei einem Sicherheitsfall sofort informiert werden muss
   - Definition der verantwortlichen Personen für die verschiedenen Phasen bei der Bewältigung eines Notfalls wie Sofortmassnahmen, Untersuchung des Vorfalls, Wiederherstellung von Daten
   - Massnahmenplan für die Eindämmung des Sicherheitsvorfalls und die Wiederherstellung der Firmendaten
   - Kommunikationsplan und Sprachregelung für die Information von Mitarbeitenden, Kunden, Geschäftspartnern, Behörden und Medien
   - Dokumentation des Vorfalls, der Massnahmen dagegen und der Erkenntnisse aus der Analyse

   Planen Sie immer mal wieder Tests und Übungen, damit alle Beteiligten wissen, was sie im Notfall zu tun haben. Und aktualisieren Sie Ihren Notfallplan regelmässig, um auch gegen neue Cybergefahren gewappnet zu sein.

5. **Qualifikation des IT-Dienstleisters prüfen**
   Es gibt verschiedene Zertifikate, die IT-Spezialisten erwerben können. Die NIST-Zertifizierung (National Institute of Standards and Technology) und der ISO-Standard sind Zertifizierungen für grössere IT-Firmen. IT-Dienstleister mit Sitz und Kundenbasis in der Schweiz können das Cyberseal-Zertifikat erwerben, um ihre Kompetenz in Sachen Cybersicherheit auszuweisen. Eine Liste von Firmen mit diesem Gütesiegel finden Sie auf der Website von Allianz Digitale Sicherheit Schweiz.