10 IT-Sicherheits-Tipps für die Unternehmensführung

1. Stellen Sie Ihren Schutzbedarf fest

- Erfassen Sie alle für Sie wichtigen Daten und Systeme
- Definieren Sie jeweils Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit
- Berücksichtigen Sie dabei interne und externe Regularien

2. Konsultieren Sie IT-Sicherheitsexperten

- Nur interne oder externe IT-Sicherheitsexperten können verlässlich Risiken und Probleme in Ihrem Unternehmen finden und einschätzen
- Unabhängige Experten haben einen anderen Blickwinkel auf Ihr Unternehmen
- Eine gezielte Analyse Ihrer IT-Infrastruktur überprüft die tatsächliche Sicherheit

3. Sensibilisieren und schulen Sie Ihre Anwender

- Das größte Risiko ist meist der Mensch. Nur erfahrene und problembewusste Mitarbeiter können Auffälligkeiten und Angriffe erkennen und richtig darauf reagieren
- Schulen Sie den sicheren Umgang mit Informationssystemen

4. Nutzen Sie persönliche und separate Zugangskennungen mit minimalen Rechten

- Sorgen Sie dafür, dass Ihre Mitarbeiter jeweils über einen eigenen Account verfügen
- Die Vergabe von Zugriffsrechten muss regelmäßig überprüft werden

5. Verwenden Sie sichere und unterschiedliche Passwörter

- Das gleiche Passwort für mehrere Ihrer Accounts öffnet Angreifern Tür und Tor

6. Verschlüsseln Sie Ihre Daten

- Besonders bei mobilen Geräten ist eine moderne Verschlüsselung unabdingbar
- Denken Sie aber auch an die Gefahr eines Einbruchdiebstahls. Verschlüsselung kann daher auch für Server und andere interne Systeme notwendig sein

7. Prüfen Sie Ihre Sicherungskopien für den Ernstfall

- Prüfen Sie den Umfang, die Aktualität und Funktionsfähigkeit Ihrer Backups
- Lassen Sie daher Ihre Sicherungen (durch einen Experten) probehalber zurückspielen

8. Trennen Sie Ihre Netze

- Achten Sie auf eine aufgabenbezogene und echte Trennung Ihrer IT-Netzwerke
- Dadurch vermeiden Sie eine Verbreitung von Schadsoftware im Unternehmen

9. IT-Sicherheit ist Prozess und Produkt zugleich

- Kontinuierliche Arbeit ist notwendig, um Ihre IT-Sicherheit bestmöglich zu gewährleisten
- Nicht nur Ihr Wissen, sondern auch Ihre Infrastruktur muss aktuell gehalten werden

10. Pflegen Sie eine IT-Sicherheitskultur

- Schaffen Sie eine Kultur, in der man über Fehler und Unsicherheiten frei spricht
- Better safe than sorry – motivieren Sie Ihre Mitarbeiter, Fehler und Störfälle zu melden

DigiTrace
Kompetenz in IT-Forensik

Richtig reagieren bei einem IT-Sicherheitsvorfall

Sie haben einen IT-Sicherheitsvorfall? Oder Sie haben eine Auffälligkeit bemerkt, die vielleicht nur ein Störfall ist, dessen Ausmaß Sie noch nicht einschätzen können? Bewahren Sie Ruhe und prüfen Sie den Ernst der Lage.

Die nachfolgende Liste soll Ihnen helfen, bei einem möglichen IT-Sicherheitsvorfall bestmöglich zu handeln. Wir empfehlen Ihnen daher, diese Liste sicher und greifbar aufzubewahren.

1. **Erzeugen Sie möglichst keine Aufregung im Unternehmen.**
2. **Prüfen Sie welche Personen vertrauenswürdig bzw. voreingenommen sind oder möglicherweise im Fokus stehen.**
3. **Priorisieren Sie Ihr weiteres Vorgehen und weihen Sie nur erforderliche vertrauenswürdige Personen ein.**
4. **Stellen Sie wenn möglich betroffene Geräte, Daten und Backups sicher.**
5. **Verändern Sie die Daten nicht, um keine Spuren zu verwischen. Arbeiten Sie stattdessen mit geeigneten (forensischen) Kopien.**
6. **Dokumentieren Sie durchgeführte Schritte genau und umfangreich, z.B. durch Fotos und exakte Zeitangaben.**
7. **Informieren Sie gegebenenfalls weitere, für den Vorfall relevante Personen (z.B. Betriebsrat, Datenschutzbeauftragter, Rechtsanwalt).**
8. **Qualifizierte Fachexperten sollten rechtzeitig eingebunden werden. Bilden Sie gegebenenfalls ein Krisenreaktionsteam.**
9. **Sorgen Sie für eine verlässliche Unterstützung durch Ihren externen Dienstleister.**
10. **Entwickeln Sie unterschiedliche Szenarien:**
    - **Wie reagiert man auf einen Innentäter?**
    - **Wie reagiert man darauf, wenn Kundendaten in fremde Hände geraten sind?**
    - **Wie lassen sich verlorene Daten wiederherstellen?**
    - **Was ist, wenn die eigenen IT-Systeme nicht mehr vertrauenswürdig sind?**

DigiTrace GmbH | www.DigiTrace.de
0221-6778695-0 | info@DigiTrace.de

DigiTrace
Kompetenz in IT-Forensik