10 IT-Sicherheits-Tipps für IT-Anwender

1. Verwenden Sie sichere Passwörter

- Vermeiden Sie persönliche Informationen (Lieblingsverein, Geburtsdatum, Name des Partners, usw.)
- Erstellen Sie lange und komplexe Passwörter
- Ändern Sie regelmäßig Ihre Passwörter
- Nutzen Sie bei Bedarf einen Passwort-Manager zur Erstellung und Verwaltung Ihrer Passwörter

2. E-Mail Sicherheit

- Öffnen Sie niemals Dateianhänge und Links, die Ihnen verdächtig vorkommen
- Täter könnten sich bewusst als Autorität (Polizei, Bank, Partner, usw.) oder Bekannte ausgeben

3. Websicherheit

- Achten Sie bei der Übertragung von vertraulichen Daten im Internet auf das "HTTPS" in der Adressleiste
- Nehmen Sie Meldungen Ihres Browsers bezüglich ungültiger Zertifikate ernst

4. Halten Sie Ihre Software aktuell

- Installieren Sie stets Sicherheitsupdates
- Nutzen Sie immer die aktuellste Sicherheitssoftware (Virenschutz, Firewall, Backuplösung, usw.)

5. Schließen Sie keine Fremdhardware an

- USB-Sticks könnten bewusst platziert und mit Schadsoftware versehen sein
- Auch andere Geräte wie Maus und Tastatur könnten manipuliert sein

6. Prüfen Sie die an Ihren Rechner angeschlossenen Geräte

- Zwischen Tastatur und Computer könnten kleine Bauteile (Keylogger) installiert sein
- Diese speichern Ihre vertraulichen Daten (Passwörter, Bankdaten, E-Mails, usw.) und senden diese weiter

7. Schützen Sie Ihre Geräte vor Diebstahl und Zugriff

- Sperren Sie Ihren Computer wenn Sie Ihren Arbeitsplatz verlassen
- Schützen Sie Laptops und Datenträger vor unbefugter Nutzung und Diebstahl

8. Umgang mit persönlichen Daten

- Überprüfen Sie, welche Informationen Sie öffentlich zugänglich machen (z.B. soziale Medien)
- Täter könnten vertrauenswürdige Informationen von Ihnen abgreifen und verwenden (Social Engineering)

9. Umgang mit Unternehmensdaten

- Trennen Sie konsequent private und geschäftliche Daten
- Seien Sie bei der Herausgabe von wichtigen Unternehmensdaten vorsichtig

10. Wenden Sie sich bei Fragen an das zuständige Fachpersonal

- Scheuen Sie sich nicht, andere um Rat zu fragen

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 lassen Sie den Ernst der Lage prüfen. Egal ob ein "unachtsamer Klick" oder eine fortgeschrittene IT-Attacke - nur mit Ihrer rechtzeitigen Unterstützung und Mitarbeit können Experten den Fall aufklären und lösen.

Better safe than sorry - Ein Fehlalarm ist besser als ein übersehener Sicherheitsvorfall.

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. Reagieren Sie überlegt aber zügig

Weder auf die lange Bank schieben noch Panik sind gute Lösungen.

2. Holen Sie frühzeitig Expertenrat ein

Wenden Sie sich zuerst an Ihren IT-Administrator, möglicherweise sollte aber direkt ein Sicherheits-Experte hinzugezogen werden.

3. Prüfen Sie, ob alle wichtigen Daten in einem funktionsfähigen Backup vorhanden sind

Achten Sie auf die Vollständigkeit, Aktualität und Integrität der Daten.
Lassen sich Daten wirklich öffnen und zurückspielen?

4. Wenn das Smartphone abhanden gekommen ist

Prüfen Sie, ob verbundene Dienste oder Accounts abrufbar sind und sperren Sie diese bei Bedarf.

5. Dokumentieren Sie den Vorfall sorgfältig

Dokumentieren Sie durchgeführte Schritte und Ihre Beobachtungen umfangreich und genau, z.B. durch Fotos und exakte Zeitangaben.

Beispiel: Am 01.04. um ca. 14:30 Uhr habe ich eine E-Mail mit einem angehängten Lieferschein erhalten. Die ZIP-Datei habe ich geöffnet aber nicht gespeichert. Es öffnete sich kurz ein schwarzes Fenster. Ansonsten ist nichts passiert. Am darauf folgenden Tag konnte ich keine Word-Dateien mehr öffnen. Auf meinem Bildschirm erschien eine Warnung des FBI bezüglich illegaler Aktivitäten mit einer Zahlungsaufforderung. Anbei befindet sich ein Foto von der Warnung, das ich mit meinem Handy erstellt habe.

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

DigiTrace
Kompetenz in IT-Forensik