



Mit InfraNet auf Nummer sicher! Nutzen Sie unser IT-Sicherheits ABC als Checkliste für mehr Datensicherheit.

Adminrechte

Administratorenrechte sollten nicht an Mitarbeiter vergeben werden.

Dokumentation

Sämtliche IT-Prozesse, Geräte und Anwendungen sollten vollständig und regelmäßig dokumentiert werden.

Geräte

PCs sollten beim Verlassen des Arbeitsplatzes gesperrt werden. Wenn Geräte ersetzt werden, ist auf ein sicheres Löschen der Daten zu achten. Besondere Vorsicht gilt bei mobilen Geräten.

Klare Sicherheitsrichtlinien

Die Unternehmens-IT sollte klare und verbindliche Sicherheitsrichtlinien definieren. Nur bei genauen Vorgaben wissen die Mitarbeiter, was sie dürfen und was sie nicht dürfen.

Notfallplan

Ein Notfallplan für Systemausfälle und Angriffe hält die Ausfallzeiten gering.

Quellen

Vor dem Öffnen von E-Mail-Anhängen und Links unbedingt die Quelle prüfen. Zweifelhafte Anhänge sofort löschen.

Technische Sicherheit

Alle Komponenten sollten technisch auf dem neuesten Stand sein, damit sie optimal vor Zugriffen von außen schützen können.

Weitergabe

Vertrauliche Daten dürfen niemals weitergegeben, Passwörter nicht notiert werden.

Backups

Alle Daten sollten regelmäßig auf einem Netzlaufwerk gespeichert und zusätzlich auf externen Datenträgern gesichert werden.

E-Mail-Verschlüsselung

E-Mails sollten bei sensiblen Inhalten verschlüsselt verschickt werden (zum Beispiel über PGP).

Herkunft der Software

Generell sollte keine Software fragwürdiger Herkunft installiert werden. Mitarbeiter dürfen keine eigene Software installieren.

Logfiles

Eine kontinuierliche Kontrolle der Logfiles schützt vor unbefugten „Besuchern“.

Outsourcing Datensicherung

Die betrieblichen Daten sollten zusätzlich extern gespeichert werden.

Rechte

Die Vergabe von Zugriffsrechten besonders auf sensible Daten sollten sehr dosiert und gezielt erfolgen.

Unternehmensvorgaben

Es dürfen nur von der Unternehmens-IT freigegebene Daten, Programme und Anwendungen eingesetzt werden.

Zugangskontrolle

Bei zentralen Bereichen sollte der Zugang sorgfältig - bei Bedarf auch mit biometrischen Faktoren - kontrolliert werden.

Check

Alle Sicherheitseinstellungen sollten regelmäßig überprüft werden.

Firewalls

Die Internetverbindung sollte durch Firewalls abgesichert werden.

Intervalle für Softwareupdates

Software- und Sicherheitsupdates müssen regelmäßig durchgeführt werden.

Monitoring

Eine permanente Überwachung der Netzwerkkomponenten gibt Aufschluss über Auffälligkeiten und ermöglicht frühzeitiges Reagieren (z.B. bei Malware).

Passwörter

IT-Sicherheit beginnt beim Mitarbeiter. Passwörter sollten so komplex wie möglich sein und aus Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen bestehen.

Software

Bei Software auf Aktualität achten. Ältere Versionen haben zum Teil größere Sicherheitslücken.

Virenschutz

Antivirenprogramme am Endgerät und am Internetgateway schützen vor Malware.

Haben Sie Fragen zur IT-Sicherheit?

InfraNet AG
Telefon +49 89 743523-0
info@infra.net