Die 10 Gebote für IT-Sicherheit

I. Du sollst nur vertrauenswürdigen Personen Zugriff zum Firmennetz gestatten

Nur befugten Personen von externen Firmen Zugriff aufs Netzwerk und sensible Daten gestatten. Durchgeführte Arbeiten dokumentieren.

II. Du sollst Benutzerzugriffe auf das Nötigste beschränken

Die Benutzerrechte an die jeweiligen Zuständigkeiten der Mitarbeiter anpassen. Jeder Benutzer hat eine eigene Anmeldung zur eindeutigen Identifikation. Zugriffe auf das Nötigste beschränken und nur befugte Mitarbeiter einrichten.

III. Du sollst sichere Kennwörter verwenden

Alle Kennwörter an festgelegte Richtlinien orientieren, mit Mindestlänge, Groß-/Klein-schreibung, Kombination von Buchstaben, Zahlen und Sonderzeichen. Kennwörter in regelmäßigen Abständen ändern. Nur befugte Personen haben Zugriff auf entsprechende Kennwörter.

IV. Du sollst Verbindungen durch Firewall/Verschlüsselung schützen

Verbindungen, die über das Firmennetz hinausgehen, zuverlässig sichern.
Dazu gehört eine Firewall, die nur vertrauenswürdige Verbindungen zulässt. Daten, die über eine solche Verbindung übermittelt werden, stets verschlüsseln. Fernzugriffe z.B. per VPN absichern.

V. Du sollst Soft- und Hardware auf dem aktuellen Stand halten

Betriebssysteme und Anwendungen werden von Herstellern laufend aktualisiert, häufig um Sicherheitslücken zu schließen, die von Angreifern gezielt ausgenutzt werden.

VI. Du sollst externe Datenträger nur nach Überprüfung in Firmennetz integrieren

Thin-Clients einsetzen, um den unkontrollierten Datenimport zu begrenzen.
USB-Sticks, externe Festplatten und sonstige Datenträger nur vom Administrator geprüft verwenden. Schadsoftware wird häufig über externe Datenträger verbreitet. Aktuelle Antivirensoftware überprüft auch externe Datenträger.

VII. Du sollst aktuelle Virenscanner verwenden

Die Nutzung einer Antivirensoftware ist ein „Muss“ auf jeglicher Hardware.
Als Virenschutz nur vertrauenswürdige Software einsetzen, die automatisch mit aktuellen Virendefinitionen versorgt wird.

VIII. Du sollst E-Mail Eingänge kritisch überprüfen

E-Mail-Eingänge nur von bekannten und vertrauenswürdigen Absendern öffnen. Im Zweifelsfall einen Administrator hinzuziehen. Schadsoftware wird oft über E-Mails verbreitet.

IX. Du sollst Downloads nur von vertrauenswürdigen Webseiten durchführen

Downloads nur von bekannten und vertrauenswürdigen Anbietern vornehmen. AGB`s und sonstige Informationen auf der Webseite des Herstellers beachten! Erfahrungsberichte helfen unter Umständen bei der Einschätzung des Anbieters. Im Zweifelsfall einen Administrator hinzuziehen.

X. Du sollst eine Datensicherung verwenden

Die Nutzung einer Datensicherung ist ein „Muss“.
Die Datensicherung sollte unterschiedliche Generationen (täglich, wöchentlich, monatlich) umfassen. Die Sicherung regelmäßig auf Vollständigkeit und Benutzung überprüfen.
Backups an unterschiedlichen, sicheren Örtlichkeiten aufbewahren.