Stand der Technik

Als „Stand der Technik" anzusehen und mindestens zu befolgen sind folgende Themenbereiche. Das Unternehmen muss generell Informationen zur Einhaltung bzw. Umsetzung der Forderung dokumentieren.

Technische Standards

- **Passwörter**: Mindestanforderungen (mindestens 12 Zeichen und Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen) sowie Speichern als Hash-Wert
- **Multifaktor-Authentifizierung**: Zweiter Faktor (zusätzlicher bzw. anderer) neben Passwort für Zugriff
- **Verschlüsselung von Festplatten**: symmetrische Verschlüsselung mindestens AES-256, keine Speicherung der Schlüssel in der Cloud (auch nicht zu Backupzwecken)
- **Objektverschlüsselung**: Verschlüsselung von Dateien und Ordnern (beispielsweise bei der Verwendung von Clouddiensten)
- **Verschlüsselung von E-Mails**: Transportverschlüsselung (mindestens TLS 1.2) sowie Möglichkeit der Ende-zu-Ende Verschlüsselung (S/MIME oder PGP)
- **Backups**: Regelmäßige Sicherung von Daten zur möglichen Wiederherstellung
- **Mobile Device Management (MDM)**: Zentrale Administration und Konfiguration mobiler Endgeräte (Notebooks, Tablets, Smartphones)
- **Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)**: Netzwerküberwachung zur Erkennung des Eindringens von Schadsoftware vor Schadenseintritt
- **Web Application Firewall (WAF)**: Schutz von Webanwendungen (Homepages, Online-Shops etc.) vor Angriffen.
- **Endpoint Detection and Response (EDR)**: Schutztechnologien um verschiedene Arten von Cyber-Angriffen auf Client und Server betriebssystemübergreifend zu stoppen.
- **Security Information and Event Management (SIEM)**: Auswertung von Anomalien und Erkennen von Angriffen der Unternehmensinfrastruktur
- **Sandboxing**: Sandbox-Technologie wird genutzt, um potenziell gefährliche Dateien in einer isolierten Umgebung auszuführen und auf schädliches Verhalten hin zu überprüfen.
- **Netzwerksegmentierung und Separierung mit internen Firewalls**: Aufteilung von Netzwerken zur effektiven Reduktion von Bedrohungen durch Einschränkung des Zugriffs auf Systeme und Daten.

Organisatorische Standards

- **Patchmanagement**: Alle Bestandteile der IT-Landschaft (wie Server, Notebooks, Mobile Devices) sollten durchgängig auf dem aktuellen Stand sein und sicherheitsrelevante Patches umgehend (innerhalb von 72 Stunden) eingespielt werden.
- **Sensibilisierung der Mitarbeiter**: Mitarbeiter sollten laufend aufgaben- und anlassbezogen sensibilisiert werden, was bspw. durch Schulungen oder Richtlinien erfolgen kann.
- **Risikoreduzierung durch Nutzungseinschränkung**: Die Nutzung der Unternehmenshardware für private Zwecke, die Nutzung von unternehmensfremder Hardware für Zwecke des Unternehmens und die private Nutzung des geschäftlichen E-Mail-Accounts sollte verboten werden.

Server und Betriebssysteme

- Kein Einsatz von Systemen, die außerhalb des Wartungszyklus der Hersteller liegen
- Unverzügliches Patch-Management für sicherheitsrelevante Patches
- Patch-Management für nicht sicherheitsrelevante Patches
- Backups (mindestens mit AES-256 Verschlüsselung)
- Multi-Faktor-Authentifizierung und Passwörter mit mindestens 12 Zeichen
- Malwareschutz mit Sandboxing und IDS/IPS
- Firewall / Next Generation Firewall
- Server baulich und technisch abgesichert, sowie zutrittsgeschützt in Hinsicht auf die Mitarbeiter

Endgeräte und Betriebssysteme

- Kein Einsatz von Systemen, die außerhalb des Wartungszyklus der Hersteller liegen
- Unverzügliches Patch-Management für sicherheitsrelevante Patches
- Patch-Management für nicht sicherheitsrelevante Patches
- Verschlüsselung (Notebooks/mobile Devices)
- Virenschutz
- Firewall

E-Mail/Internet

- TLS-Mail-Verschlüsselung
- HTTPS-Verschlüsselung (mindestens mit TLS 1.2, empfohlen TLS 1.3 und PFS)
- Virenscanner
- Spamfilterung