LU05c - Beispiel eines einfachen Konzepts

Netzwerk-Sicherheitskonzept und Nutzungsregeln der Firma XY-Trading

1. Einführung und Zielsetzung

Dieses Netzwerk-Sicherheitskonzept wurde entwickelt, um die Netzwerksicherheit der Firma zu gewährleisten. Unsere Ziele sind die Verhinderung von unbefugtem Zugriff, die Aufrechterhaltung der Verfügbarkeit unserer Dienste und die Sicherung unserer vertraulichen Daten.

2. Netzwerktopologie und Ressourcen

Unsere Netzwerktopologie umfasst

- Zentrale Server-Infrastruktur am Hauptsitz der Firma in Zürich
- 2 Bürostandorte in Bern
- 1 Bürostandort in Luzern
- 1 Bürostandort in Chur
- Remote-Zugriff für Mitarbeiter im Home Office

Kritische Ressourcen sind unsere Server und Datenbanken.

3. Risikoanalyse und Bedrohungsidentifikation

Identifizierte Bedrohungen sind

- Malware
- Phishing-Angriffe
- Unbefugter physischer Zugang zu Servern
- Datenlecks

4. Sicherheitsziele und -anforderungen

- Implementierung einer Firewall-Infrastruktur
- Verschlüsselung aller Datenübertragungen
- Tägliche automatische Datensicherung
- Zugriffskontrollen für sensible Daten

5. Netzwerksicherheitsmassnahmen

- Einsatz von Hardware-Firewalls an den Netzwerkgrenzen
- Regelmässige Aktualisierung von Betriebssystemen und Anwendungen
- Verwendung von VPNs für sichere Remote-Zugriffe
- Segmentierung des Netzwerks für isolierte Bereiche

- Das Funknetzwerk (WLAN) für Kunden und Besucher ist komplett vom Firmennetzwerk (LAN) getrennt

6. Nutzungsrichtlinien und Verhaltensregeln

- Alle Mitarbeiter müssen starke Passwörter verwenden und diese regelmässig ändern
- Die Nutzung von Unternehmensgeräten für private Zwecke ist nicht gestattet
- Verdächtige Aktivitäten oder Sicherheitsverletzungen müssen sofort dem IT-Support gemeldet werden
- Das Kunden-WLAN darf nicht von Mitarbeitern verwendet werden

7. Schulung und Sensibilisierung

- Alle Mitarbeiter erhalten jährliche Schulungen zur Netzwerksicherheit
- Alle Mitarbeiter sind über aktuelle Bedrohungen informiert
- Bei grösseren Systemwechseln (z.B. neues Betriebssystem der Clients) werden alle Mitabeiter über relevante Punkte informiert und geschult

8. Überwachung und Bewertung

- Das Netzwerk wird kontinuierlich überwacht
- Es werden regelmässige Sicherheitsaudits durchgeführt, um Schwachstellen zu identifizieren und zu beheben

9. Incident Response Plan

Ein umfassender Incident Response Plan ist verfügbar und legt die Schritte fest, die im Falle eines Sicherheitsvorfalls unternommen werden müssen.

- Ein Ausfall eines Systems, bei dem **keine** Ausweichmöglichkeit (Ersatz) besteht, z. B. Server, Netzwerk, darf der Ausfall des betroffenen Systems maximal 24 Std. (Mo.–Fr.) dauern
- Ein Ausfall von Systemen, bei dem eine Ausweichmöglichkeit (Ersatz) besteht, z. B. AP-PC, Drucker etc., darf der Ausfall des betroffenen Systems maximal 72 Std. (Mo.–Fr.) dauern

10. Compliance und gesetzliche Anforderungen

Dieses Netzwerk-Sicherheitskonzept stellt sicher, dass alle geltenden gesetzlichen und regulatorischen Anforderungen im Bereich der Netzwerksicherheit erfüllt werden.

---

m117