Schritt für Schritt zu mehr Netzwerksicherheit

Was Sie sofort für eine höhere Netzwerksicherheit tun können

Heutzutage ist keine Branche oder Unternehmensgröße mehr vor Cyberattacken gefeit. Die sonst so positive steigende Digitalisierung von Arbeitsprozessen macht das Thema Netzwerksicherheit zu einer noch größeren Herausforderung. Lesen Sie hier, wie Sie sich bereits mit den Ihnen unmittelbar zur Verfügung stehenden Ressourcen sofort besser gegen Hackerangriffe wappnen können:

1

Router- und Firewall-Einstellungen, die Ihre Netzwerksicherheit erhöhen

- ◯ Nur verschlüsselte Internetprotokolle wie HTTPS oder SSH erlauben und unnötige oder unverschlüsselte Internetprotokolle wie HTTP oder telnet deaktivieren
- ◯ Jegliche Zugriffsmöglichkeiten auf eigene Geräte von außen blockieren und selbst für RemoteKonfigurationen der Router/Firewalls stets eine VPN-Verbindung verwenden
- ◯ Ungenutzte Ports in der Router-Firewall/Firewall schließen
- ◯ Jeglichen internetbasierten Zugriff auf Endgeräte, die direkt mit dem Router verbunden sind (z.B. Drucker), blockieren und unsichere Eintrittspunkte schließen
- ◯ Entsprechend der neuesten Sicherheitsempfehlungen IKEv2 als VPN-Protokoll mit AES-GCM und mindestens SHA-256 als Verschlüsselungsalgorithmen nutzen (inzwischen veraltet und dadurch unsicher: Protokolle wie PPTP oder Algorithmen wie MD-5 oder SHA-1!)

2

So sichern Ihre Switches Ihr Netzwerk ab

- ◯ Jegliche unverschlüsselte und ungenutzte Ethernet-Ports deaktivieren
- ◯ Netzwerke für unterschiedliche Applikationen oder Abteilungen mithilfe von VLANs segmentieren: Konfigurations-Ports in separiertem Management-VLAN verwalten und Endnutzer-Netzwerke und -Endgeräte in eigenes VLAN ausgliedern
- ◯ Ethernet-Port-Endgerät-Verbindungen prüfen und offene Ports schließen
- ◯ Zur Übersicht und Kontrolle der Port-Nutzung Port-Authentifizierung via IEEE 802.1X-Zertifikate oder MAC-Adressen-Authentifizierung einführen
- ◯ Unnötige und unsichere Fernkonfigurationswege abschalten

3

So unterstützen Ihre Access Points ein sicheres Firmennetzwerk

- ◯ Neuesten Verschlüsselungsstandard WPA3 nutzen
- ◯ Sendeleistung der Access Points auf ein notwendiges Minimum reduzieren: Eigenes Netzwerk kann nicht außerhalb der eigenen Räumlichkeiten empfangen werden
- ◯ WLAN in mehrere SSIDs für bestimmte Nutzergruppen trennen
- ◯ PPSK / LEPS: Mit Private Pre-Shared Keys (PPSK) für die Benutzer oder – bei LANCOM Geräten – mit LEPS Berechtigungen von Endgeräten einschränken und besser überwachen oder individuelle Mitarbeiterschlüssel bei Firmenaustritt aus der Datenbank entfernen

---

4

Erhöhen Sie das allgemeine Bewusstsein in der Firma für IT-Security

- ◯ Regelmäßige Schulungen für Mitarbeiter anbieten, z.B. zum Umgang mit Phishing Mails oder sicheren Passwörtern
- ◯ Verwendung von ungeprüften USB-Sticks und Anschluss privater Datenträger an das Firmennetz unterbinden
- ◯ Alles auf dem neuesten Stand halten und regelmäßig die neuesten Sicherheitsupdates für Software und Geräte installieren
- ◯ Tägliche Daten-Backups einrichten
- ◯ Maßgeschneiderte, professionelle UTM-Firewall (Unified Threat Management) einsetzen
- ◯ Cybersecurity-Gesamtkonzept mit IT-Administratoren und Fachhändlern entwickeln und entdeckte Schwachstellen beseitigen

LANCOM SYSTEMS

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de
lancom-systems.de