Konzeption und Realisieren einer IT-Infrastruktur, Testszenarien

Ausgangssituation

Komplexe Netzwerkumgebungen erfordern ein hohes Maß an Sicherheit und Überwachung.
Ein Zusammenwachsen von Office Umgebungen und Industrie 4.0 – Infrastrukturen verschärft diese Situation.

Daher ist es notwendig automatisierte Systeme zur Überwachung und spezielle Tools zur aktiven und passiven Überprüfung der Sicherheit einzusetzen.

Aufgabenstellung

Die folgenden Themengebiete wurden als Anhaltspunkt vorgegeben und auf zwei Bereiche wie folgt aufgeteilt, getrennt bearbeitet und im Anschluss über vordefinierte Schnittstellen zusammengeführt:

Themenbereich 1:

- Radius Server
- VPN Server (SSL)
- Netzwerkmonitoring
  (SNMP, PRTG, Syslog, Nagios etc.)

Themenbereich 2:

- Proxy Dienst
- Firewall (Packet Filter, Application specific)
- Intrusion Detection (LAN, WLAN, WAN, DMZ)

Gemeinsamer Inhalt:

- Erstellen von Schulungszenarien (Dokumentation)

Vorgehen

- Aktives Überwachen der Sicherheit durch Penetration Tests und Vulnerability Scan
- Erkennen von Angriffen durch Intrusion Detection Systeme
- Sperren der nicht benötigter Ports sowie Geo IP‘s und Einstiegsknoten zum Tor Netzwerk
- Umleiten des HTTPS Traffics zu einem Proxy Server mit SSL Interception und Virenprüfung
- Monitoring von Netzwerkdiensten
- Überwachen von Sensoren
- Host-Alive Erkennung

Ergebnisse / Testszenarien

- VPN Einwahl über simulierten ISP (Cisco Router)
- Access Control durch PfSense Firewall mit IDS System Snort; OpenVPN Server; PfBlockerNG; FreeRadius Server; Squid Proxy Server
- Network Monitoring durch Icinga
- Penetration Tests und Vulnerability Scan mit Kali Linux
- Radius Verbindung zur Einwahl über Access Point