NÖM konkret

So setzen wir IT-Security um

High-Level

NÖM konkret Eckdaten

Alltag in der NÖM - Eckdaten

- ~ 600 Mio Umsatz 800 MA (250 W/550 B)
- IT MA -> ~ 10

- Anzahl Netzwerk-Endgeräte: ~2.000 (IP-Adressen)

- Anzahl Netzwerk-Switche: 62 -> max. 2.976 Ports

- Anzahl PCs/Notebooks: 300

- Anzahl Server: 180

- Genutztes Speichervolumen: ~130 TB
- ~ 37.000 Stunden Videomaterial oder
- ~ 13 Mrd. Mails

Alltag in der NÖM - Security

- Perimeter-Sicherheit „Außenwelt“
  ~400 zufällige Attacken/24 Stunden
- Endpunkt-Sicherheit „Endgeräte“
  ~1500 Untersuchungen/24 Stunden
- Netzwerk-Sicherheit „Netzwerk-Datenverkehr“
  ~35 TB/24 Stunden
- Mail-Sicherheit „empfangene Mails“
  ~1.100 blockierte Mails/24 Stunden
  --> entspricht 46% der empfangenen Mails

Wie machen wir es konkret?

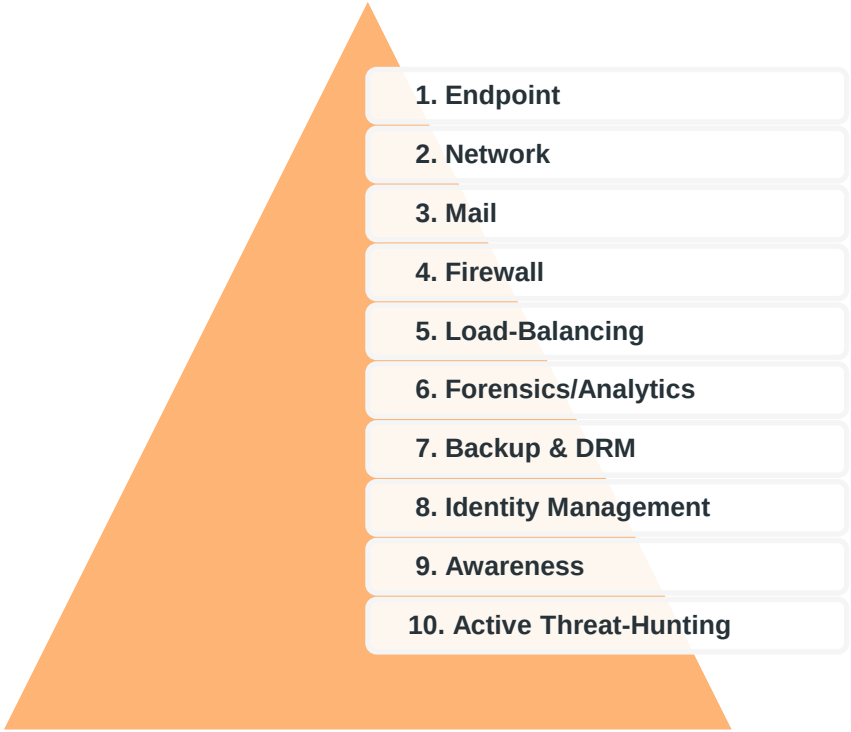
Conclusio

- Viel Theorie – wenig konkretes
- Beratungshäuser sehr herstellerlastig (eher immer ein Produkt)

- Typische Konzepte
  - Endpoint-Protection (meist noch signaturbasiert)
  - Klassische Firewalls
  - Port-Security
  - VPN für Remote-Office

→ so sind die meisten Firmen aufgestellt

Konkretes IT-Security Konzept



Konkretes IT-Security Konzept NÖM (1/5)

1. Endpoint

- MDR (Managed Detection & Response) für Endpoints
- Application Control für Endpoints
- MDM (Mobile Device Management)

2. Network

- Netzwerkdokumentation & Bereinigung
- NDR (Network Detection & Response) mit Auto-Response (Cyber-AI)
- OT-Security (Visibilität)
- Network Access Control im Office-Bereich
- Zentrales Management für Netzwerkkomponenten

Konkretes IT-Security Konzept NÖM (2/5)

3. Mail

- Mail-Security (Sandboxing, etc.)
- Mailverschlüsselung & Signierung

4. Firewall

- Ruleset-Bereinigung
- Firewall mit IDS/IPS
  - Getrennt für Perimeter und Datacenter
- Standortvernetzung mittels SD-WAN
- MFA-VPN für Lieferanten (keine Ausnahmen)
- (Secure-DNS)
- (DDoS high-volume Schutz)

Konkretes IT-Security Konzept NÖM (3/5)

5. Load-Balancing

- Reverse-Proxy
  - Externe Dienste
  - Interne Dienste

6. Forensics/Analytics

- SIEM Log-Management
  - Sammlung und manipulationssichere Speicherung von Logs
  - Automatisierte Alarme & Auswertungen
  - Server, Netzwerk-Komponenten, Firewalls, etc.
  - Nutzung sinnvoller Zusatz-Tools wie Sysmon
    - Zuordnung von Prozessen zu IP-Verbindungen und DNS-Auflösungen

Konkretes IT-Security Konzept NÖM (4/5)

7. Backup & DRM

- Backup-Umgebung
  - Backupserver nicht in der AD-Domäne
  - Mehrstufige Sicherung inkl. Offline-Stage (Tape)
  - VMs, Konfiguration von Hardware-Komponenten

- Desaster Recovery Management
  - IT-Betriebshandbuch
    - System- und Prozessdokumentation
  - IT-Notfallhandbuch
    - Checkliste für Desaster-Fall
    - Vorgehensweise in Bezug auf Blackout-Thematik
  - Restore-Tests (auch mit redundanten Komponenten)

Konkretes IT-Security Konzept NÖM (5/5)

8. Identity Management

- Admin-User Konzept
- MFA
- AD/AzureAD/ADFS/CA/Exchange Härtung
  - Kerberos, Berechtigungen, etc.
- PAM (Privileged Access Management)

9. Awareness

- Phishing-Kampagnen zur Mitarbeiter-Sensibilisierung
- Schulungen

10. Active Threat-Hunting

- Penetration-Tests (Identifizierung von unbekannten Schwachstellen)
- Network Threat-Hunting (Beacons, Long TCP-Connections, etc.)

Was fehlt uns noch!

- **Vulnerability Management – in Umsetzung**
- **Mikro-Segmentierung – in Planung**
- **IT-Risikomanagement (SupplyChain, Business-Prozesse) – in Umsetzung**

Ergänzungen / Anmerkungen

1. Endpoint
2. Network
3. Mail
4. Firewall
5. Load-Balancing
6. Forensics/Analytics
7. Backup & DRM
8. Identity Management
9. Awareness
10. Active Threat-Hunting

Kontakt.

Ing. Dominik Achleitner, MSc MA
dominik.achleitner@noem.at
www.linkedin.com/in/dominikachleitner

Ing. Patrick Prohaska, CISSP
patrick.prohaska@noem.at
www.linkedin.com/in/patrickprohaska