Skriptum: IT-Security – Grundlagen, Konzepte und aktuelle Herausforderungen

Basierend auf dem Vortrag vom 04.11.2025

---

1. Einleitung & Motivation

- **Beispiel: Rosenbauer Panther 4x4 Flughafenfeuerwehr**
  - Österreichisches Fahrzeug, 6 km Glasfaserkabel, 6000-Liter-Tank, **vollständig fernsteuerbar**.
  - **Zero Security** – Annahme: Fahrzeuge stehen in bewachten Hallen.
  - **Vorfall vor einem Jahr:** Fahrzeuge in Chicago O'Hare lahmgelegt → Flughafenschließung → **Millionen betroffene Passagiere**.
  - **Impact:** Zeigt, wie physische und cyber-physische Systeme (OT-Security) miteinander verknüpft sind.
- **Ziel des Vortrags:**
  - Gemeinsames **Vokabularyset** schaffen → Tech-Sprech für Reifeprüfung.
  - Grundlagen wiederholen (640 Slides → „rucki zucki" durchgehen).
  - **NDR, EDR, SIEM, Compliance, NIS-2, Risk-Management** im Fokus.

---

2. Kernkonzepte der IT-Security

2.1. NDR – Network Detection and Response

- **Definition:** Alles, was **nach der First Line of Defense** (Firewall, Endpoint) im Netzwerk passiert.
- **Position:** Zwischen **Endpoint Security** und **Firewall**.
- **Herausforderung:** Idealerweise **100 % verschlüsselter Traffic** im LAN → NDR erschwert.
  - Früher: **N-Bar** (Network Based Application Recognition).
  - **EY-Studie:** < 1 % Traffic in Unternehmen verschlüsselt.
  - **Realität in AT:** Nicht mal Active Directory verschlüsselt → **GPO-Lösung (5 Klicks)** oder **IPsec über Netzwerkkarte**.
- **Fazit:** NDR bleibt in den nächsten Jahren **zentral**, da Verschlüsselung de facto **nicht umgesetzt** wird.

2.2. EDR – Endpoint Detection and Response

- **Definition:** Client-seitige Erkennung und Reaktion (ehemals EDR = Endpoint Detection Response).

- **Wichtigkeit: Erste Line of Defense** → Firewalls sind nicht mehr primär.
- **Voraussetzung:** EDR muss mit **SIEM** vernetzt sein → sonst nutzlos.
  - **Ausgeschlossene Lösungen:** Symantec, Kaspersky (keine Schnittstellen, geopolitische Risiken).
  - **Österreichisches Bundesheer:** Noch größter Kaspersky-Kunde → „Kopfschütteln".
- **Funktionen:**
  - **Clear-Text-Traffic** am Endpoint → z. B. Google-Suchbegriffe analysierbar.
  - **Automatisierte Response:**
    - Datei in Quarantäne.
    - Rechner aus Netzwerk verbannen.
    - Traffic-Pattern weitergeben.
- **Dilemma:**
  - **Isolation = gut** (kein Schaden), **aber schlecht** (keine Forensik möglich).
  - **Idealfall:** Angreifer weiter beobachten → **Outbreak vs. Analyse** → Teil der **Security-Strategie**.

---

3. Standardisierung & Kommunikation (CVSS, Interpol/Europol)

3.1. Common Vulnerability Scoring System (CVSS)

- **Ziel:** Standardisiertes Reporting von Cyberangriffen.
- **Hintergrund:**
  - **Konferenz in Wien (in 14 Tagen):** Interpol + Europol → **CVS (Common Vocabulary Set for Threats)**.
  - **Federführung Cyberkriminalität:** Österreichisches LKA (besser als Ruf).
  - **Best Practice:** Indonesische Polizei (FBI lernt von ihnen).
- **Problem:**
  - Früher: **Wöchentliche/monatliche Fallkonferenzen** → ineffizient.
  - Heute: **150–200 Incidents pro Tag → Automatisierung notwendig**.
- **Lösung:**
  - **Standard-Reporting-Formular** („Forms-Formular") → **~300 Fragen pro Incident**.
  - **Scoring:** 400 Unterpunkte → **1–10 Punkte**.
    - **0–4:** Normales Response-Team.
    - **8,5–9:** Nationaler Notstand.
- **Datenbanken:**
  - **MyTrade:** Bekanntestes, frei verfügbares CVE-Tool.

  - **OSINT:** Open Source Intelligence.
  - **Free-Versionen:** 48 Stunden verzögert.
  - **Pay-Versionen:** Echtzeit (Münzen, Scheine, Goldbarren, Latinum).
- **Herausforderung:**
  - **Rückwirkende Dokumentation:** Heutige Incidents müssen in zukünftige Systeme übertragbar sein.
  - **Fake-Incidents:** ~298 von 300 täglichen Incidents sind **inszeniert** (White-Hacker im Auftrag von Herstellern).
  - **Incident-Flooding:** Angreifer fluten Datenbanken mit Fake-Daten → **80–90 % Fake-Informationen**.

3.2. Markt & Hersteller

- **Herstellerinteressen:**
  - Kein Interesse an **standardisierten, lesbaren Security-Bulletins**.
  - **Goldpartner** erhalten Infos **24 Stunden früher** → Hierarchie: Gold → Non-Gold → Public.
  - **Microsoft:** Stundentakt-Updates (60–80 Seiten) → **eigene Abteilungen** nötig.
  - **KI-Zukunft:** KI von Microsoft und OMV „treffen sich virtuell“ → automatisierte Kommunikation.
- **Beispiele:**
  - **Cisco Umbrella:** Weltweit in Sekunden deploybar.
  - **Fortinet:** 80 Mitarbeiter (vor 3 Jahren: 50) → andere Vertriebsstrukturen.
  - **Trend Micro:** In keinem Krautszeug/Splunk integriert.

---

4. Reale Angriffsbeispiele

4.1. ÖBB – Manipuliertes Outlook-Deployment

- **Zeitpunkt:** Vor **2,5 Jahren**.
- **Angriff:**
  - IT-Dienstleister der ÖBB → **Deployment-Prozess infiltriert**.
  - **Outlook.exe ausgetauscht** → **Randomizer**: Nicht alle Notebooks betroffen.
- **Impact:**
  - **Zehntausende Notebooks** potenziell kompromittiert.
  - **Meldepflicht:** DSGVO, NIS, Sarbanes-Oxley → **alle Kunden informieren**.
- **Lektion:** Daten müssen **Jahre aufbewahrt** werden → **KI notwendig zur Auswertung**.

4.2. EVN – Smart Meter (Landis+Gyr)

- **Zeitpunkt:** Ab 2019, 250.000 Zähler.
- **Schwachstellen:**
  - **Default-Passwort:** `Landis123` → geändert zu `Landis123!`.
  - **14.000 unverschlüsselte Notebooks** für Techniker.
  - **Techniker-Verhalten:**
    - Notebooks im Auto liegen gelassen (Ottenschlag, 14 Uhr, Freitag).
    - **SIM-Karten dupliziert** → Zugriff auf **Power-Grid-Netz**.
- **Angriff:**
  - Notebook geklaut → Passwort → Zugriff auf Zähler.
  - **Erpressung:** 24 Stunden Zeit, sonst „Ausprobieren“.
- **Folgen:**
  - **Lastabwurf → Totalverlust Stromnetz**.
  - **BIOS-Bug:** Zähler ohne Auth abschaltbar.
  - **Attack-Surface-Reduktion:** Läuft noch (länger als 12 Monate).
- **Lage:**
  - Zähler **auf Grundstücksgrenze** (EU-Vorschrift).
  - **Mobilfunk (5G)** → auch in Kellern erreichbar.
  - **Gesetz:** Bis 2026 alle Zähler Smart (Strom), 2025 (Wasser).

4.3. Weitere Beispiele

- **ÖBB Signalangriff:**
  - Angreifer als Eisenbahnarbeiter → LAN-Stecker am Signal → **keine Segmentierung** → großer Netzwerkzugriff.
  - **>70.000 Patch-Panels** allein in Hauptbahnhof.
- **Wasserversorgung Wien:**
  - **86 Einstiegshäuschen** entlang Hochquellenleitung → Tür mit Tritt öffnen → **Vergiftung möglich**.
  - **Seit 2025 in Splunk überwacht**.

---

5. Security-Architektur & SOC

```
[Technische Sicht]
Endpoint (EDR) → NDR → SIEM → SOC
       ↓
[Rechtliche Sicht]
Datenschutz, NIS, DSGVO, SOX, Telekommunikationsgesetz, etc.
```

- **SOC (Security Operations Center):** Betrachtung **technisch + rechtlich**.
- **Rechtliche Aspekte:**
  - **Datenschutz:** Traffic-Aufzeichnung nur mit Zustimmung (Dienstvertrag).

  - **Compliance Officer:** Neuer Beruf → technisch + juristisch.
  - **EDU-Governance:** Schulen, Ministerien → NIS-2 betroffen.
- **NIS-2 (ab 1,5 Jahre):**
  - **Kritische Infrastruktur erweitert:** Gas, Wasser, Strom, **Bildung, Governance**.
  - **Kaskadeneffekt: Alle Zulieferer** von NIS-2-Betroffenen → ebenfalls betroffen.
  - **Beispiel:** EVN baut Rechenzentrum → Betonbauer (Thor) → Büromöbel → **alle NIS-2**.

---

6. SASE – Secure Access Service Edge

- **Problem:**
  - **17 Hersteller** (Switches, Firewalls, OS, EDR, SIEM) → **keine nahtlose Kommunikation**.
- **Lösung:**
  - **SASE:** Zentrales, standardisiertes System.
  - **Herstellerunabhängig?** → **Nein** (Cisco ≠ Fortinet).
  - **Juniper:** Erste Propagandisten.
  - **Fortinet:** Erster Anbieter mit SASE-Lösung.
- **Anwendungsfall:**
  - **ÖBB:** 200.000 Switches → nur 2 % nicht gehärtet = **4.000 Angriffsvektoren**.
  - **Lieferkette:** Signalhersteller → Zulieferer → **alle zertifiziert**.
  - **Ab Ende 2026 verpflichtend** → **Geschäftsführer haftbar**.

---

7. Grundlagen & Historie

7.1. CIA-Triade (16. Jh.)

- **Kerckhoffs' Prinzipien** (Franzose, Militär):
  - **Confidentiality, Integrity, Availability**.
  - **Geheimhaltung ≠ Maschine** → Enigma gescheitert.

7.2. Erweiterte Ziele

- **Risk Management**
- **Threat Intelligence & Information Sharing**
- **Threat Hunting**
- **Second Party Collaboration**
- **Incident Response Teams**
- **Resilienz** (seit 0,5 Jahr im Trend)

7.3. Standards

- **NIST (USA):** Framework-Updates (monatlich).
- **ISO 27001:** ISMS (Information Security Management System).
  - **Konkurrenz zu NIS** → ISO vs. NIS.
- **IEEE**

---

8. Begriffsdefinitionen

Begriff	Definition
Threat	Potential Danger gegen ein Asset
Vulnerability	Schwachstelle (in OS, App, Waschmaschine, Switch, etc.)
Exploit	Ausnutzung einer Vulnerability
Zero-Day	Unbekannter Exploit
CVE	Common Vulnerabilities and Exposures
CVSS	Scoring-System (1–10)
IOC	Indicator of Compromise
Attack Surface	Alles, was angreifbar ist (Signale, Drucker, WLAN, etc.)
Attack Continuum	Recon → Attack → Exfiltration → Cleanup (Durchschnitt: **2+ Jahre**)

---

9. Risk Management

- **Beispiel ÖBB:**
  - **Investition:** > 500 Mio. € (6 Jahre).
  - **Frage:** Transportiert das einen Kunden mehr? → **Nein**.
  - **Kalkül:**
    - 30 Min. Ausfall = akzeptabel (Speicherkraftwerk Weißsee).
    - **Menschenleben?** → Kein Wettbewerb → „Pein hart kalkuliert“.
- **Risk Manager:** Bewertet **Wahrscheinlichkeit × Auswirkung**.
- **Entscheidung:** Immer **Geschäftsführung** → aber **CISO droht Gefängnis**.

---

10. Angriffe & Cyber Kill Chain

1. **Zielauswahl**
2. **Reconnaissance** (OSINT, Shodan, HaveIBeenPwned)
3. **Weaponization**

4. **Delivery**
5. **Exploitation**
6. **Installation**
7. **Command & Control**
8. **Actions on Objectives**

- **Früherkennung: IOCs** vor Exploitation.
- **Dauer: 2+ Jahre** (von Recon bis Aufräumen).

---

11. Angreifer-Spektrum

Typ	Beschreibung
Script Kiddies	Einfache Tools
White Hat	Ethical Hacker
Black Hat	Kriminell
State-Sponsored	Iran, Vietnam, Indonesien (sehr professionell)
DDoS, Disclosure	Hauptangriffe

---

12. Fazit & Ausblick

- **Security ist ganzheitlich:** Technik + Recht + Prozesse + Awareness.
- **KI übernimmt:**
  - Incident-Reporting
  - Vulnerability-Management
  - Threat Intelligence
- **Berufsbilder:**
  - **Security Compliance Officer**
  - **Risk Manager**
  - **EDR/NDR Analyst**
  - **SOC Analyst**
- **NIS-2 = Game Changer: 80 neue Partner bei Fortinet in AT in 2 Jahren**.
- **Resilienz > Handling:** Systeme müssen **Angriffe widerstehen**.
- **Low-Level-Angriffe bleiben relevant:** DoS, Beam of Death → **Renaissance**.

Empfohlene Tools zur Vertiefung: - **MyTrade** (CVE) - **Shodan** (IoT-Suche) - **HaveIBeenPwned** (Credential-Check) - **Splunk** (SIEM) - **Icarus Live** (Threat Intelligence)

Abschlusszitat (Dozent): > „Wir brauchen nicht nur die besten Tools – wir brauchen Mitarbeiter, die nicht Vollidioten sind.“