NORTHWAVE
CYBER SECURITY

Einblicke in den Cyber Underground

Eileen Walther, Northwave Cyber Security, General Manager DACH

Tim Estermann, Funke Mediengruppe, CISO

Webinar

- Top Cyberbedrohungen
- Fallbeispielen der Funke Mediengruppe
- Lösungsansätze

Top Cyberbedrohungen

- Ransomware

- APTs: Spionage, Manipulation, Sabotage

- Massenkriminalität

Auf dem Spiel stehen immer Reputation & Kontinuität

Ransomware

Entwicklungen

Underground-Dynamik in den letzten 12 Monaten

- Weitere Verlagerung von der Datenverschlüsselung zur (reinen) Datenerpressungsangriffen.
- Führungsebene und Reputation im Fokus der Erpressung.
- Supply-Chain-Attacks
- LockBit Takedown

APTs

Entwicklungen

Geopolitische Spannungen

- Russland
  - Sabotage, Manipulation, politische Spionage.
- China
  - Wirtschaftsspionage: geringe Sichtbarkeit, große Menge an Zeit und Ressourcen.
  - U.a. Spear-phishing und legitime Verwaltungstools.
  - Verstärkter APT-Fokus auf OT

Massenkriminalität

Entwicklungen

Same, same, but different

- DDoS
- Insider threats
- Business Email Compromise

- Social Engineering powered by AI: WormGPT & co

Fallbeispiel Ransomware

Ransomware Angriff Funke Mediengruppe

Wie ist es dazu gekommen?

- Signaturbasierte Antivirus-Lösung
  - Keine verhaltensbasierende Erkennung
- Monitoring nicht ausreichend
- Kein MFA

Funke Mediengruppe

Was hat geholfen?

- Backups
  - integer
  - offline
- Eingespielte Notfallprozesse
- Externe Unterstützung
- Sofortiger Start des Wiederaufbaus

Fallbeispiel APTs

Angriffe 2022-2024

Krieg und politisch motivierte Akteure

- Koordinierte Angriffe 10 Tage vor Überfall auf Ukraine
- Angriffe nach kritischen Artikeln
- Austausch mit Behörden und anderen Unternehmen extrem wertvoll
- Mustererkennung durch Kooperation

Fallbeispiel Massenkriminalität

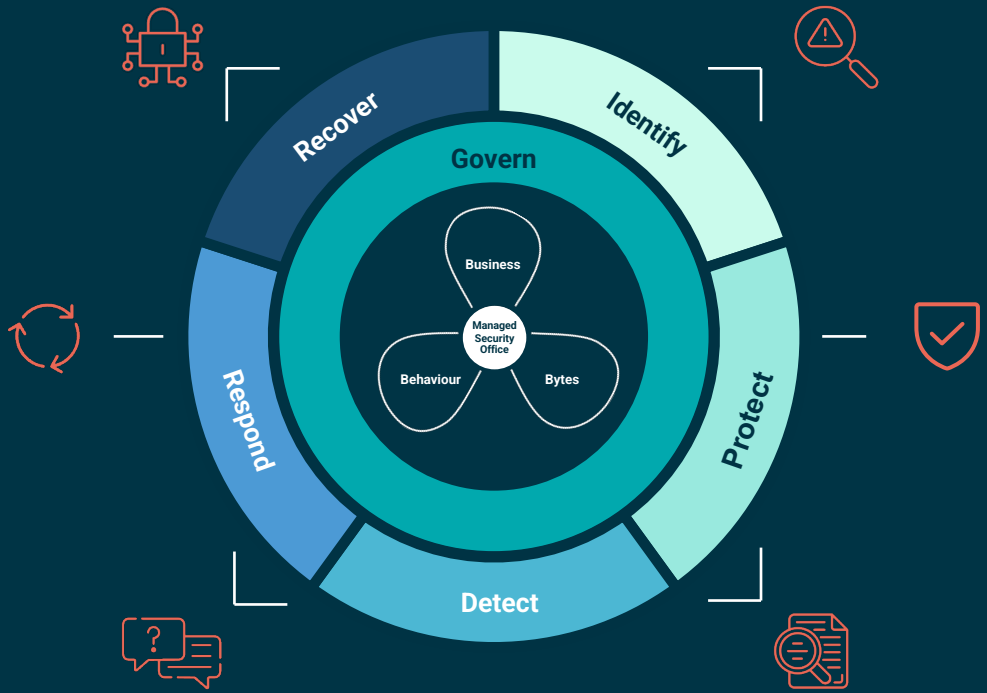
Ständige Angriffe

Aktuelle Angriffs-Trends

- DDoS immer noch täglich
- QR-Codes in Phishing-Mails zur Umgehung von Endpoint Protection
- Supply Chain Attacks – Angriffe über kompromittierte Unternehmen

Lösungsansatz

Intelligent Security Operations



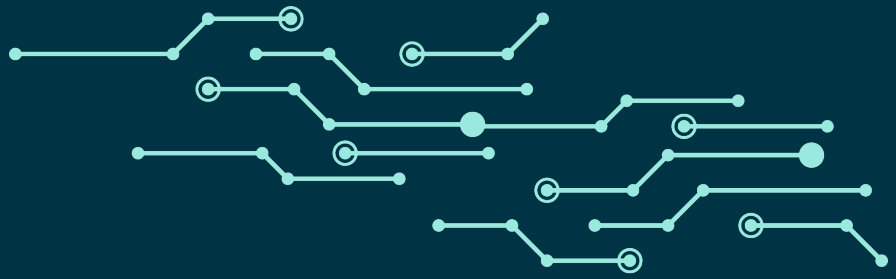
NIST Cybersecurity Framework (CSF)2.0

APT’s sind das Neue Problem

Ransomware ist nicht länger die Benchmark

- APT‘s treffen Unternehmen im strategischen Bereich.
- Cyberspionage soll in Ihr Risikomanagement einbezogen werden.
- APT’s haben Zeit. Mitarbeiter, IT-Anbieter und Lieferanten sind nützliche Trittbretter.
- APT‘s sind schwieriger zu erkennen.
- Zusammenspiel von organisatorischen, menschlichen und technischen Maßnahmen wird wichtiger.

NORTHWAVE
CYBER SECURITY



Have a safe digital journey!

northwave-cybersecurity.com

KONTAKT

NORTHWAVE DEUTSCHLAND GmbH

Maximilianallee 2, 04129 Leipzig, Deutschland

Tel: +31 (0) 30 303 1240

Email: info@Northwave-security.com

Website: northwave-cybersecurity.com

Sie sind aktuell von einemSicherheitsvorfall betroffen?

Rufen Sie uns Tag und Nacht an:

24*7 Computer Emergency Response Team: 00800 1744 000