secunet

Cyberangriff – Üben für den Ernstfall

Vortrag, 15. Mai, 15:00 Uhr Webinar

Jannik Pewny

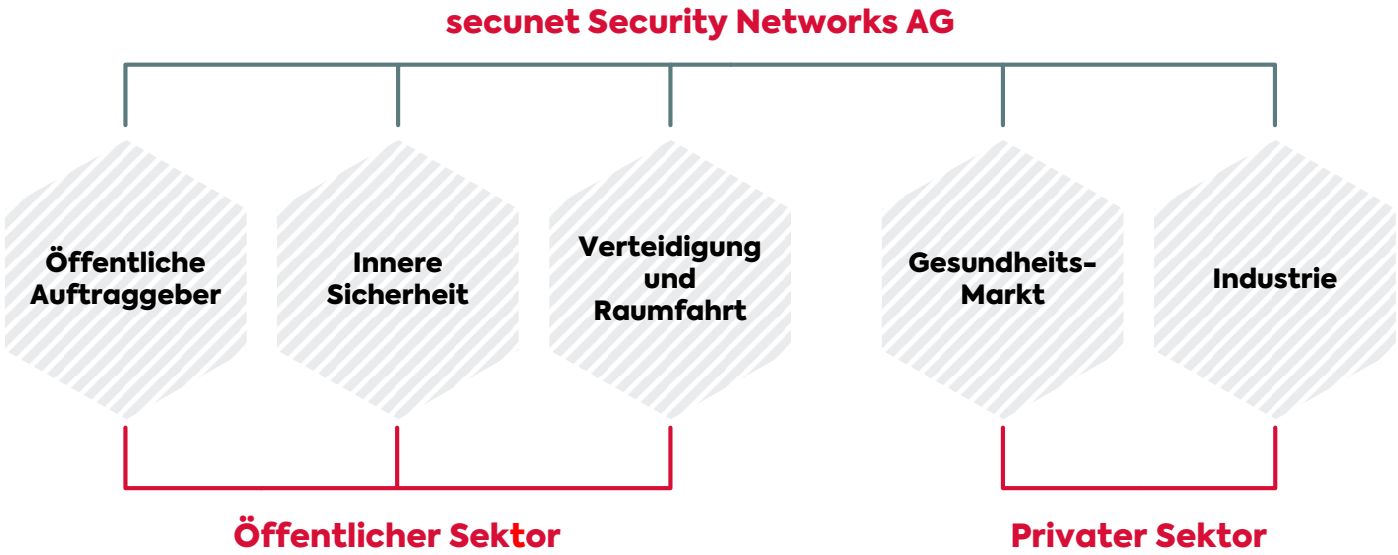
Teamleiter Incident Response

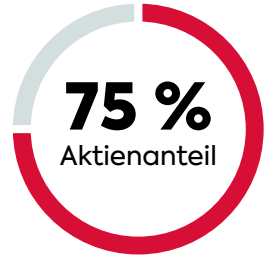
Alexander Kruse

Vertrieb Industrial & Mobility

secunet Security Networks AG

secunet auf einen Blick





Hauptaktionär:
Giesecke + Devrient

Joint Ventures

SecuStack
Cloud Operating System

Tochtergesellschaften

Stashcat
Secure Messenger

Syseleven
Cloud & Managed Kubernetes

347 Mio.*
Euro Umsatz

47 Mio.*
Euro EBIT

über 1.000
Sicherheits-experten

*Im Jahr 2022

Vortragender

- jannik.pewny@secunet.com
- B.Sc./M.Sc. IT-Sicherheit, B.Sc. Angewandte Informatik
- Penetrationstester, Teamleiter Incident Response
- Zugführer / Löscheinheitsführer in der Freiwilligen Feuerwehr

Selbstverständnis IT-Security

- Kein Selbstzweck
- Keine Arbeitsverhinderungsaktion
- Erhalten des Betriebs bei Angriffen
- Macht nur teurer, langsamer, komplizierter
- … bis zum Angriff

Grenze extern/intern wird überschätzt

- Ein falscher Klick
- Ein geöffneter Anhang
- Ein ungepatchtes Programm
  - … und der Angreifer ist eventuell drin.

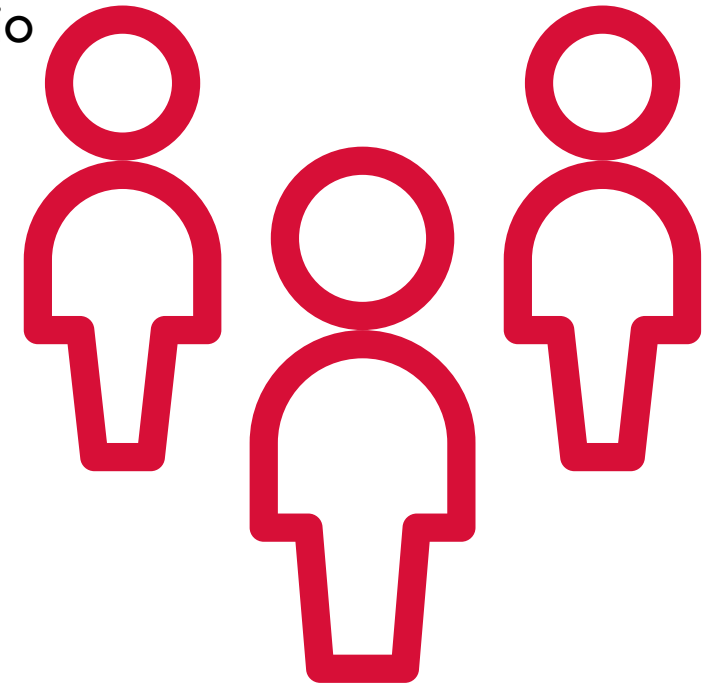
- Moderne IT-Security sollte annehmen,
  dass man früher oder später mal „gehackt“ wird.

1

Intro / Ablauf

Cyber War Gaming

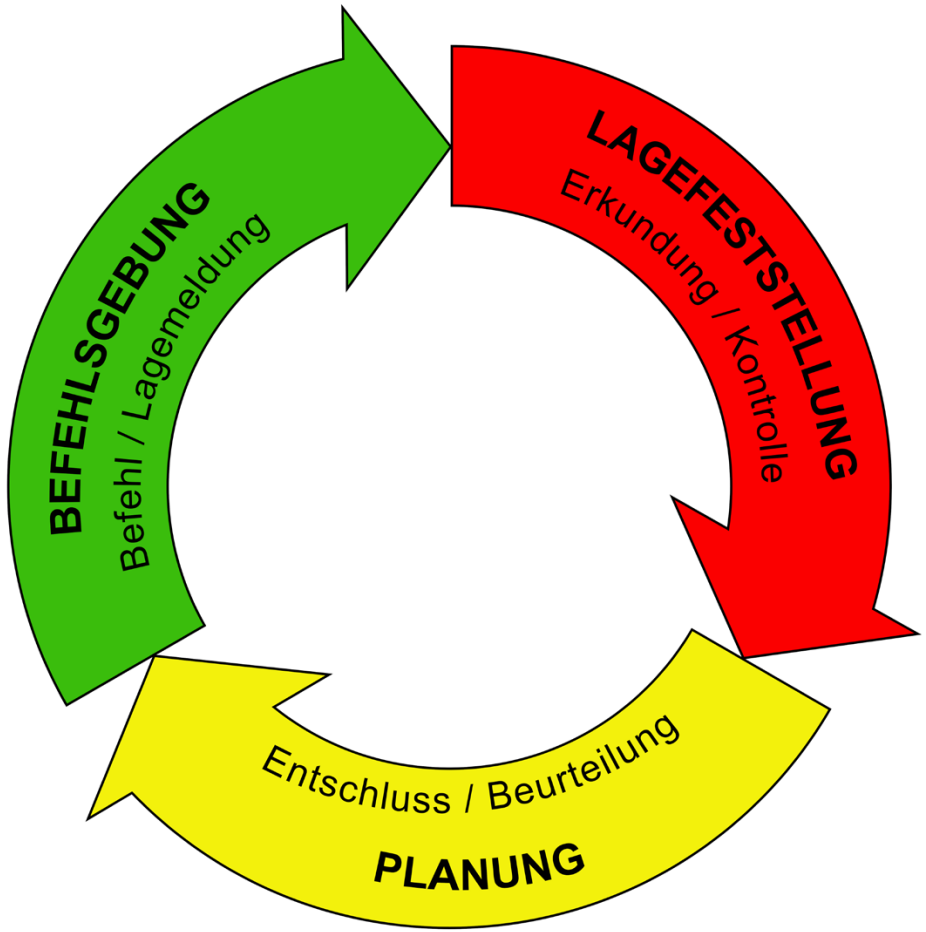
- Incident Response War Gaming = Spielleiter + Spieler + Szenario
  - Angemessenes Handeln für Incidents erarbeiten
  - Spielleiter: Leitet durch Prozess + Informationsquelle
  - Spieler: Spielen =)
  - Erkundung, Maßnahmen protokollieren, Nachbesprechen



- Szenarien
  - statisch vs dynamisch
  - Lehrinhalt vs Üben
  - 5 Minuten bis mehrere Tage

Führungskreislauf*

- Erkunden
- Planen
- Handeln



*Quelle: FwDV 100, Seite 25

Incident – Einleitung

- **Chaos-Phase**
- **„Kalte Lage“**
  - Assets, Netzaufbau, Security-Infrastruktur
  - Stand IT-Security
- **„Warme Lage“**
  - Was ist passiert?
  - Was wird bzw. könnte passieren?
  - Was tun wir jetzt?

Intermezzo – Pentest als „Stand IT-Security“

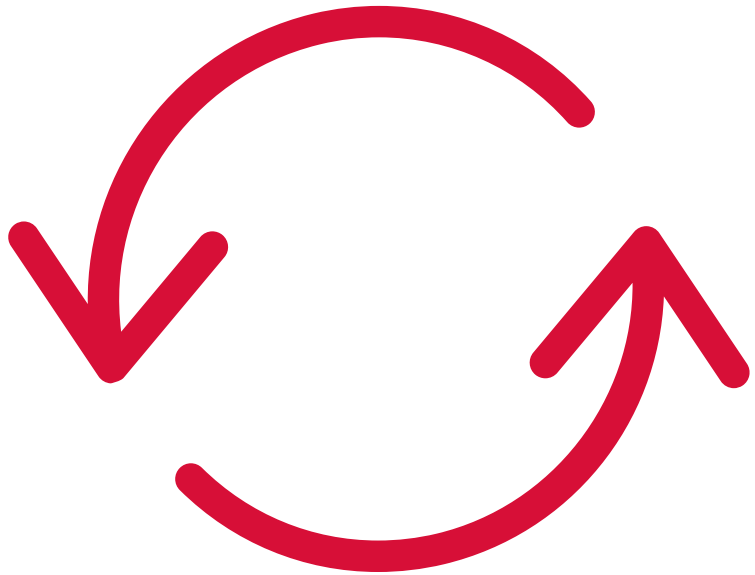
- Viele Schwachstellen findet man durch einfaches „draufgucken“
- Schwachstellenscan
- AD-Scan, Windows-Config
- Rollenkonzept / Netzaufbau
- Scoping extrem wichtig

2

Praktische Tipps

Erkundung

- Ansprechpartner
  - Macher. Nicht Manager/Abteilungsleiter/…
- Erkundungsmaßnahmen explizit erlaubt
- Erkundungslage vs Handlungslage
- Unvollständige Informationen / Post-Ante



Ansätze

- Sources / Eingänge
- Sinks / High-Value Targets
- Trails / IoCs

- Position in Kill-Chain beachten
- Nicht am eigenen Ast sägen

Erkennung

Ort

- Lokal
- Lokales Netz
- Zentralisiert

Methode

- Draufsicht
- Automatisch
- Detailanalyse
- Anomalie

Grobe Lage


Kritikalität
Grüne Wiese
Schaden
Bringt Nichts
Nichts
Nichts
Einzeln
Begrenzt
Komplett
Ausbreitung

Notfallplan – Ziel

- Hilfestellung für ernsthafte IT-Security-Incidents

Notfallplan – Zitate

- „A failure to plan, is a plan for failure.“

  (Winston Churchill)

- „Kein Plan überlebt den ersten Feindkontakt.“

  (Carl von Clausewitz)

- „Simple, clear purpose and principles
  give rise to complex and intelligent behavior.
  Complex rules and regulations
  give rise to simple and stupid behavior.“

  (Dee Hoch)

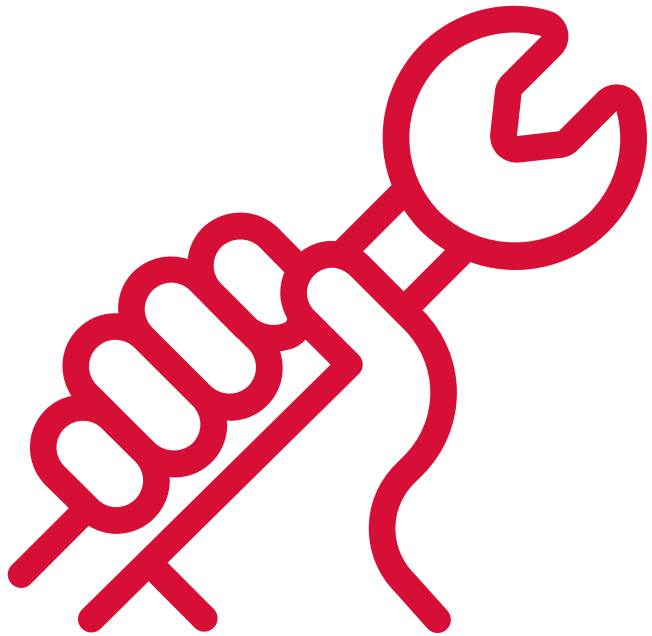
secunet

IT Security Incident Response Hotline

+49-(0)201-5454-1337

Probleme – Unausräumbar

- Chaos-Phase
- Unvollständige Informationen
- Kommunikation
- Stress

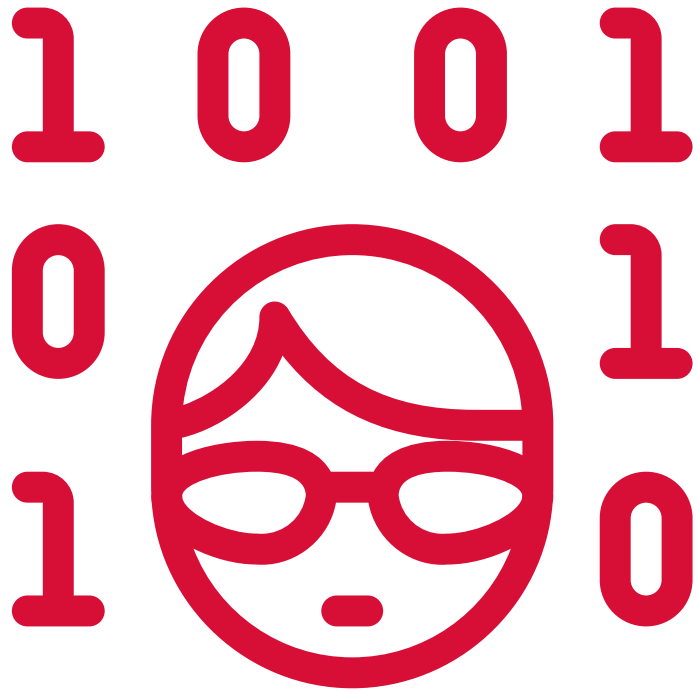


Ransomware – Ein Spektrum

- Falsche Drohung
- E-Mail mit Malware, nicht geklickt
- E-Mail mit Malware, geklickt, aber abgefangen
- 2003er-Ransomware
  (Single-Host, 500€ per PayPal)
- Beacons
- Aktive Verschlüsselung
  - teilweise
  - mit Backups
  - ohne Backups

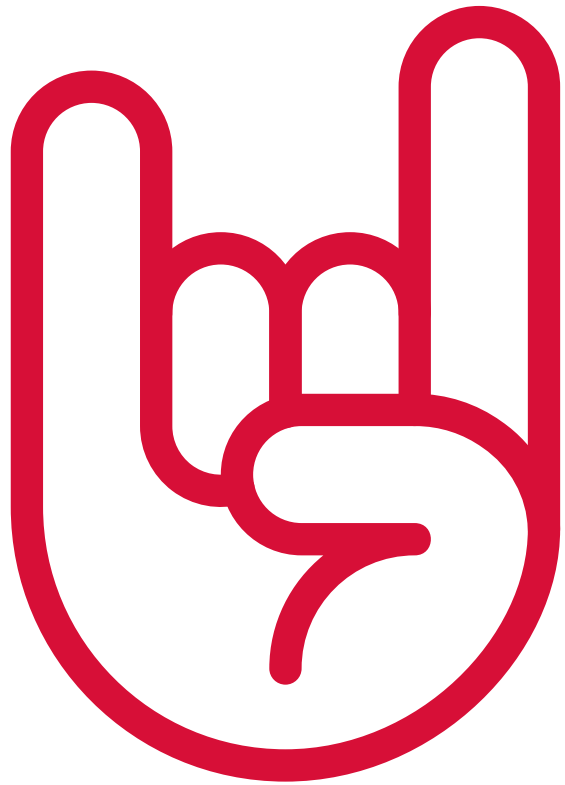
Aufgaben des Incident Managers

- Ruhe ausstrahlen
- Priorisieren
- Entscheiden / Entscheidungsoptionen klarstellen
- Arbeiten *lassen*
- Kommunizieren



Hilfreiche Konzepte

- Die Kunst des Machbaren
- Hypothesen-basiertes Arbeiten
- Trust, but Verify
- Gesunde Prozess-Skepsis / Ausnahmezustand
- Manchmal is' nix



Die folgenden Listen sollten

nicht

als vollständig angesehen werden.

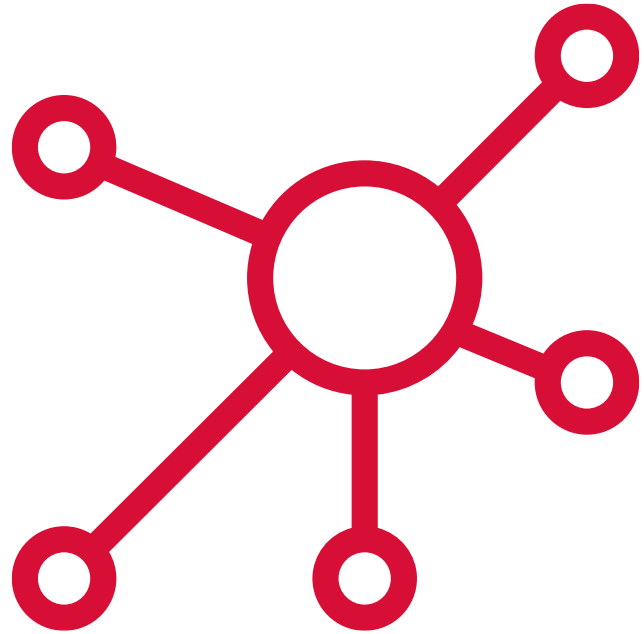
Optionen des Angreifers – Infiltration

- Phishing
- Social Engineering
- Exploits
- Web
- Supply Chain
- Waterhole
- BYOD
- WiFi
- Physical

Optionen des Angreifers – Ausbreitung

- Exploitation
- Phishing
- Dropped File
- MitM
  - LLMNR/NBNS/mDNS/IPv6/SNAC
  - ARP-Spoofing

- Credentials
  - Lokal: Cached
  - Lokal: Sessions
  - Lokal: Dateien
  - Lokal: E-Mails
  - Lokal: Keylogger
  - MitM
  - Ausprobieren
    - Spray / Stuffing / Re-Use
    - Weak



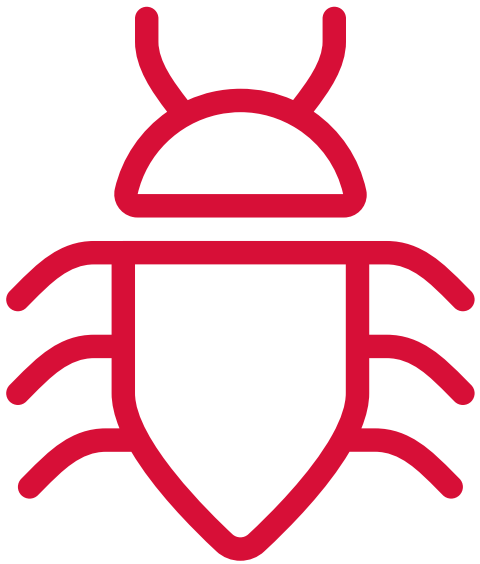
Optionen des Angreifers – Payload

- Endlos…

- Scans / Ungewöhnliche Verbindungen
- Nachladen
- Verbotene Aktionen
- Neue User anlegen
- Ransomware
- Crypto-Mining
- whoami

Optionen des Angreifers – Persistenz

- Endlos…



- Dateien / Infektion
- “Autostart”
- Services
- File-Less
- DLL-Injection
- Browser
- Mail-Regeln
- MBR
- BIOS / UEFI / PCI / Firmware…

Optionen des Angreifers – C&C / Exfiltration

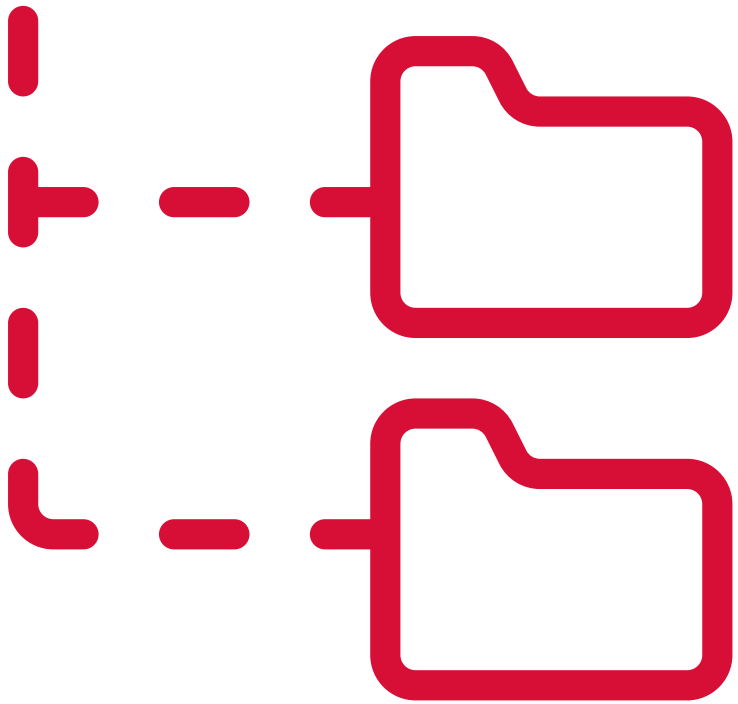
- Netzwerk / Internet
  - Steganographie
  - Obfuscation
  - Encrypted
  - Tunnel
- WiFi
- Physical
- Keine

3

Szenarien

Beispiel-Szenario – Gerüst

- Buchhaltung: „Rechnung mit falschen Kontodaten“
- ISP: „Kontakte zu C&C-Ips festgestellt“
- GF: „E-Mail droht mit Verschlüsselung, will Geld“



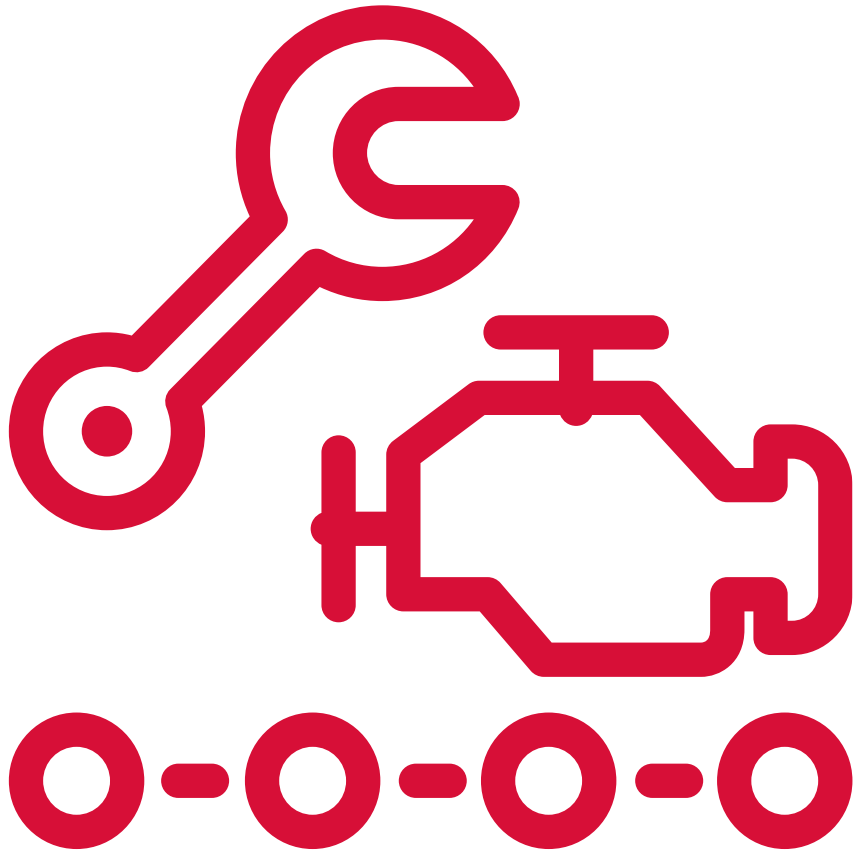
- Frage an die Spieler: Was nun?
- (Rest der Lage ist dem Spielleiter bekannt)

Beispiel-Incident – Glück im Unglück

- Soziales Unternehmen mit „Patienten“
- Abgeflossene E-Mails als Basis für Phishing
- Ca. 300GB zusätzlicher Traffic
  … entspricht Größe des Exchange-Servers
- Lizenz für Backup-Software ausgelaufen

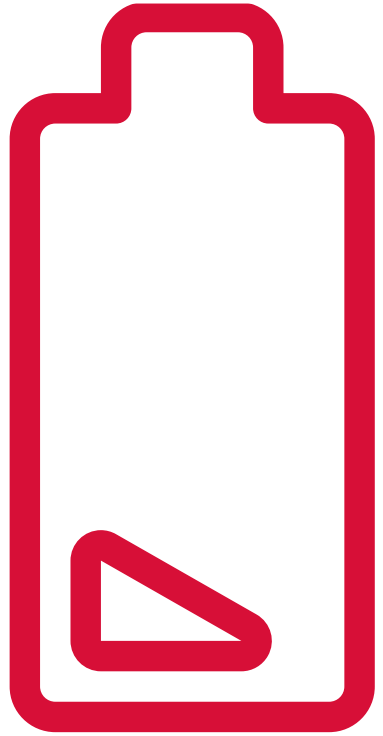
Beispiel-Incident – Grüne Wiese?

- Hersteller von Spezialmaschinen
- Vollverschlüsselt auf OS-Ebene
- Backups unverschlüsselt



Beispiel-Incident – Phishing-Welle

- KRITIS-Unternehmen
- Einer akuten Phishing-Welle ausgesetzt
- Mindestens zwei Mitarbeiter haben geklickt
- Mail-Signatur auch in vom Server ausgehenden Mails entdeckt



Kontakt für Fragen zu
Penetrationstests & Incident Response

Jannik Pewny

Teamleiter Incident Response

secunet Security Networks AG

jannik.pewny@secunet.com

Tel.: +49 (0) 201 5454-0

IT-Security Incident Response Hotline

+49-(0)201-5454-1337

secunet Security Networks AG

Save The Date – unsere Industrial Security Webinare

- **Online Demo Angriffserkennung gemäß IT-Sicherheitsgesetz 2.0**

  16. Mai, 15:00 – 15:30 Uhr

- **Für Versorger aus der Praxis – Online Workshop – „Wie umgehen mit der steigenden Bedrohungslage durch Cyber-Kriminalität?“**

  25. Mai, 9:30 – 12:00 Uhr

- **Online Demo Angriffserkennung gemäß IT-Sicherheitsgesetz 2.0**

  6. Juni, 11:00 – 11:30 Uhr

- **Cyber-Security on Board – Online Workshop Automotive & Mobility**

  23. Juni, 9:30 – 12:00 Uhr

Informationen und Anmeldung unter:
www.secunet.com/events-industry


secunet