secunet

Cyberangriff – Notfallplan für den Ernstfall

Jannik Pewny

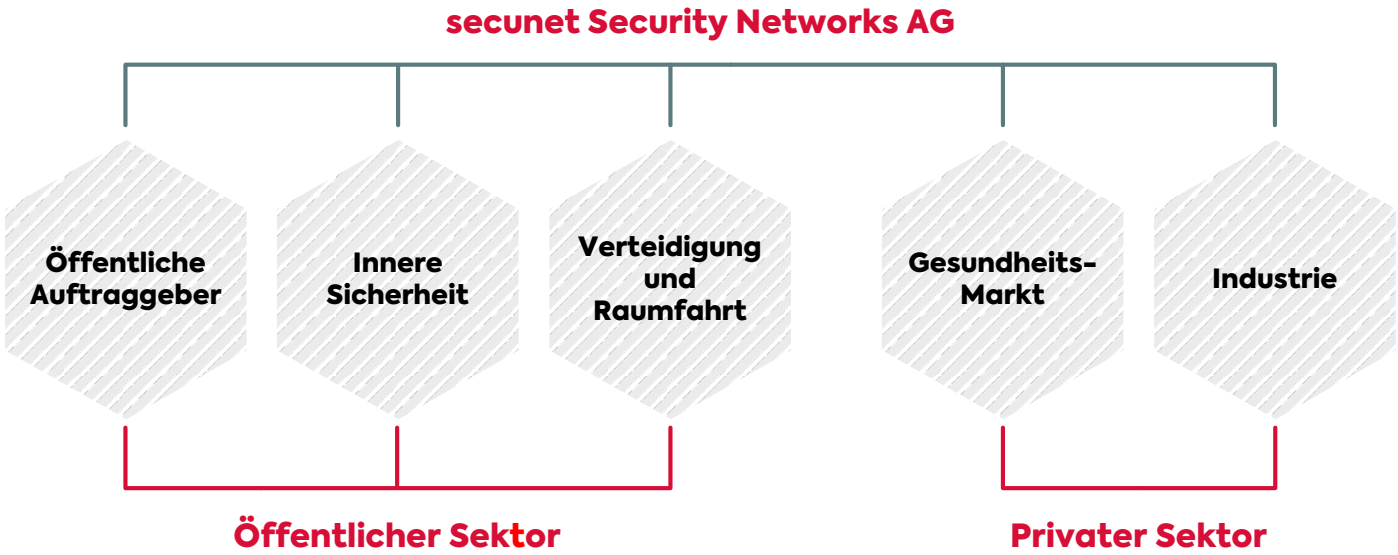
Teamleiter Incident Response

secunet Security Networks AG

Vortrag, 24. April, 15:00 Uhr

Webinar

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.

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)

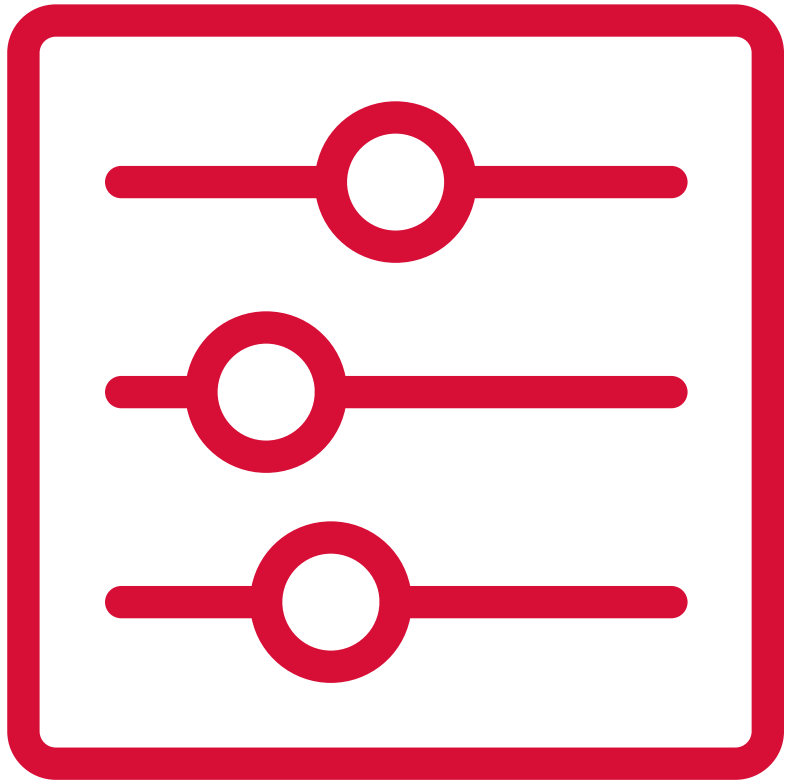
secunet

IT Security Incident Response Hotline

+49-(0)201-5454-1337

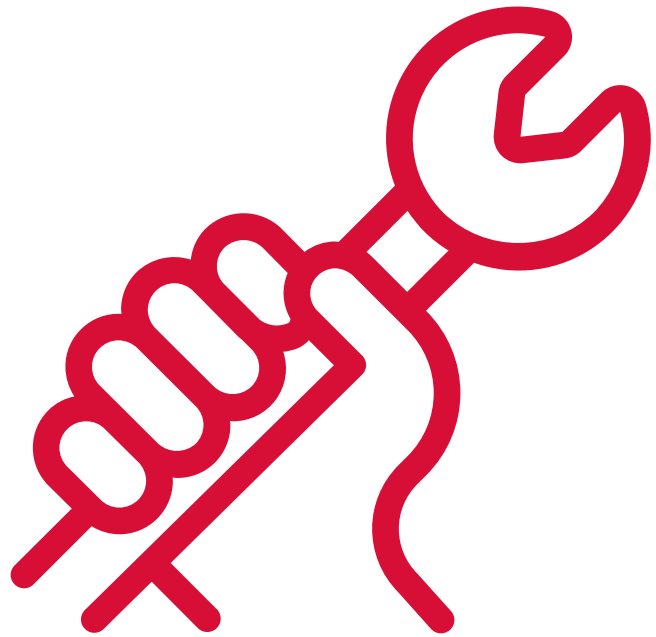
Notfallplan – Ein Spektrum

- Visitenkarte
- 15-20 Seiten
- Security-by-Compliance
  - BCM
  - ISMS
  - ISO27001



Probleme – Unausräumbar

- Chaos-Phase
- Unvollständige Informationen
- Kommunikation
- Stress

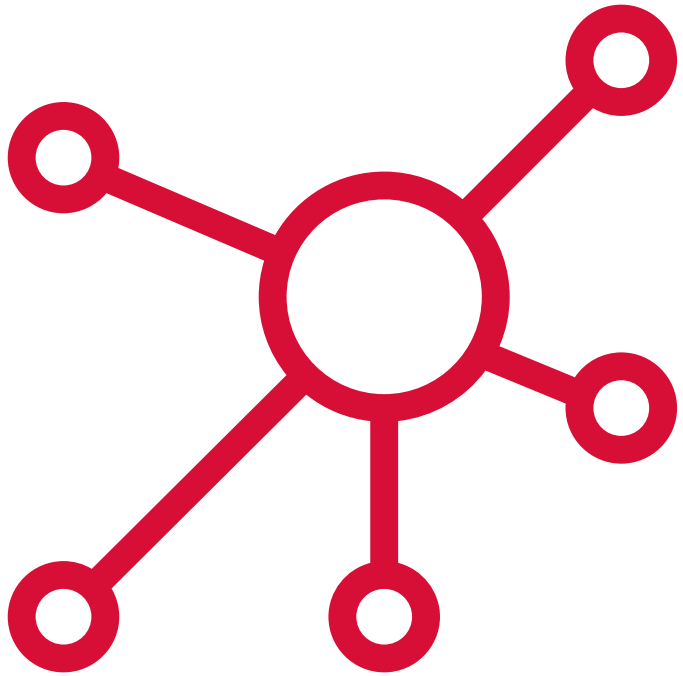


Incident – Einleitung

- **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?

Bereiche der IT-Security

- Prävention
- Detektion
- Reaktion



Security-Baseline (1/2)

- Passwortsicherheit
- Updates/Patches
- Social Engineering, speziell Phishing

- MitM / SMB-Signing
- Netzwerkseparation
- Rollenkonzept

Security-Baseline (2/2)

- Backups: WORM/"Offline"
- AV/EDR: Behaviour und zentrale Konsole
  - Besser: Whitelisting per AppLocker/DeviceGuard
- Logging
  - Detaillreich, Retention-Time, zentralisiert

- Schwachstellenscan
- Penetrationstest / Red Teaming / Purple Teaming
- "War Gaming"

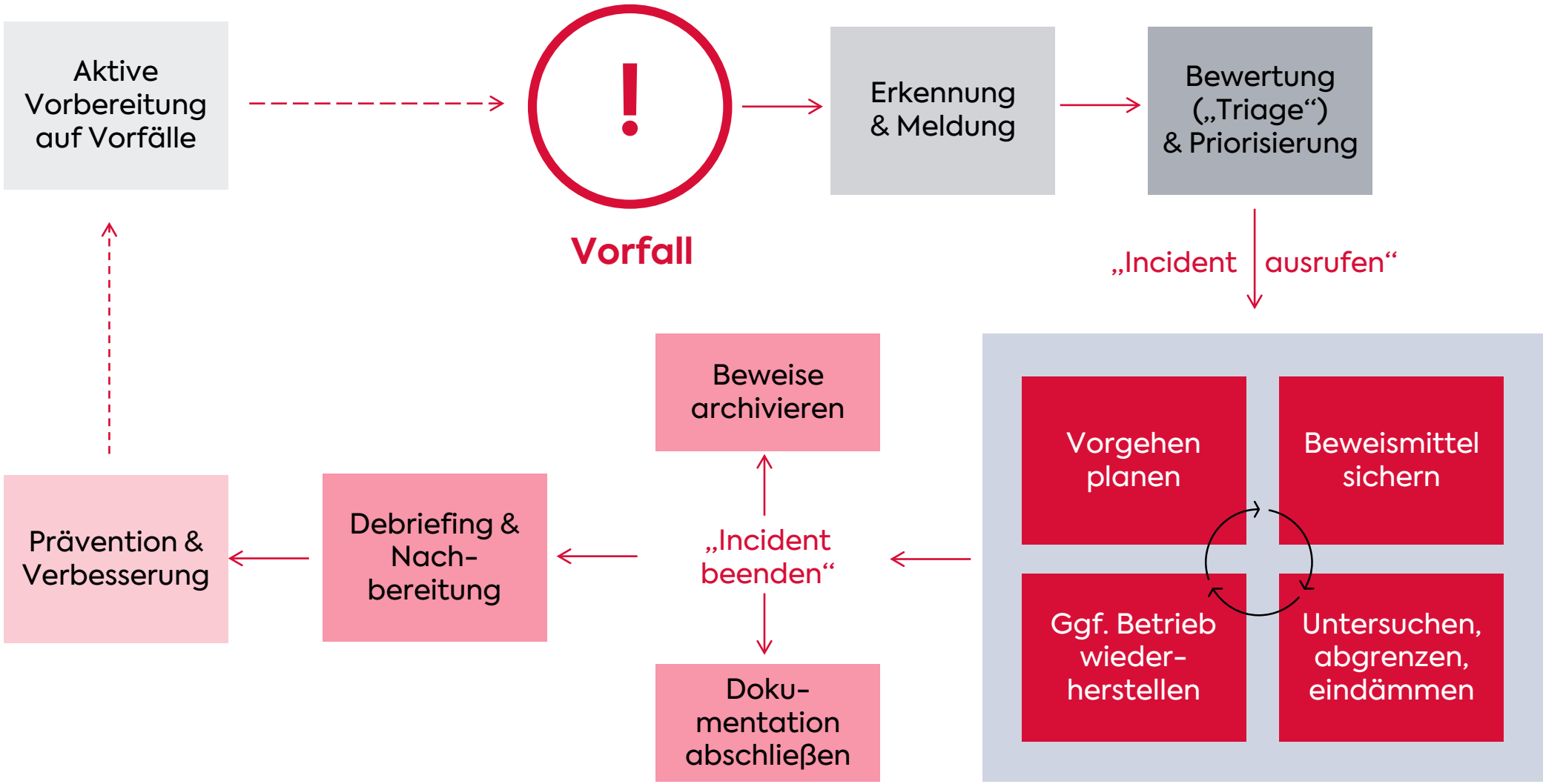
Intermezzo – Pentest als „Stand IT-Security“

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

Ransomware – Ein Spektrum

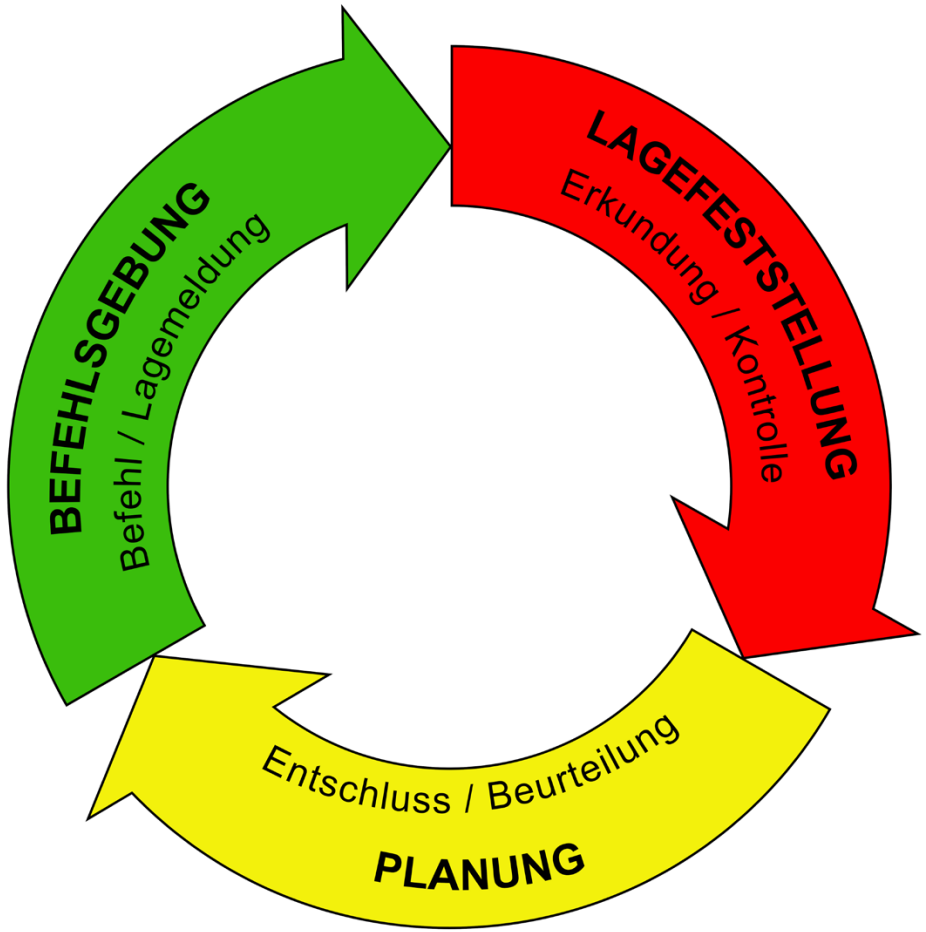
- Falsche Drohung
- E-Mail mit Malware, nicht geklickt
- E-Mail mit Malware, geklickt, aber abgefangen
- 2003er-Ransomware
  (Single-Host, 500€ per PayPal)
- Beacons
- Aktive Verschlüsselung
  - teilweise
  - mit Backups
  - ohne Backups

Generischer Ablauf



Führungskreislauf*

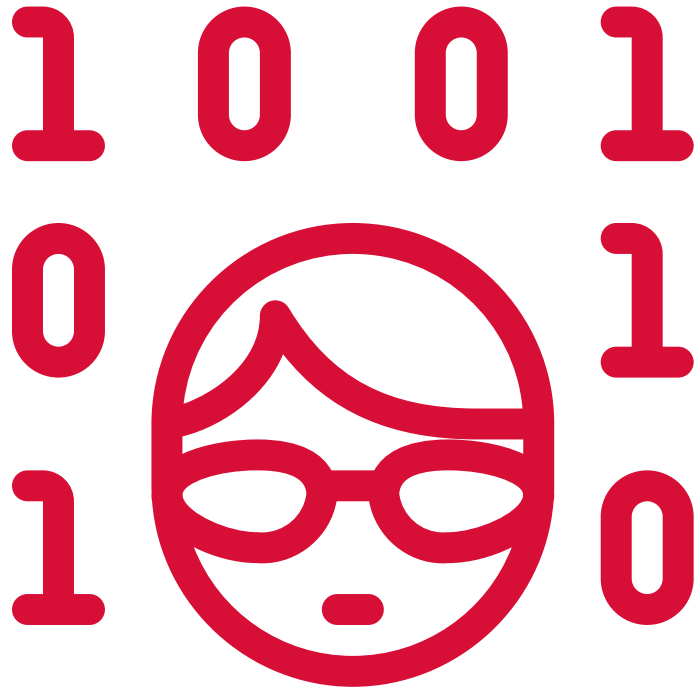
- Erkunden
- Planen
- Handeln



*Quelle: FwDV 100, Seite 25

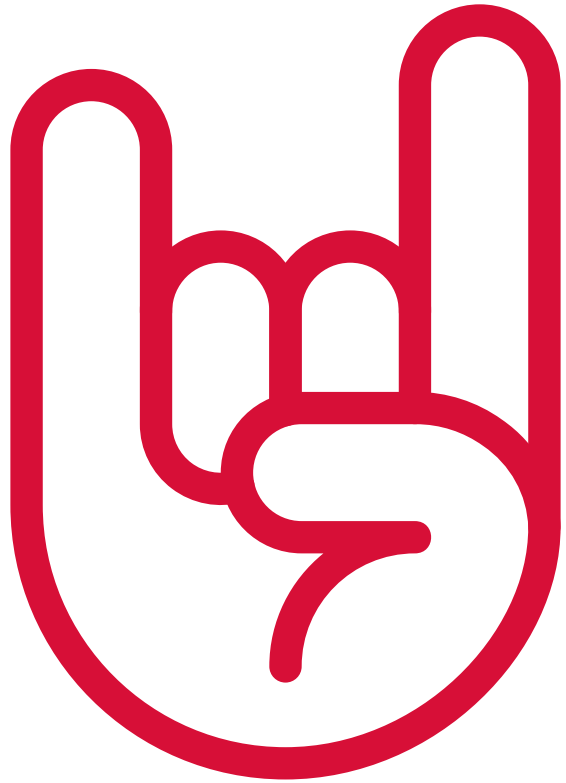
Aufgaben des Incident Managers

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



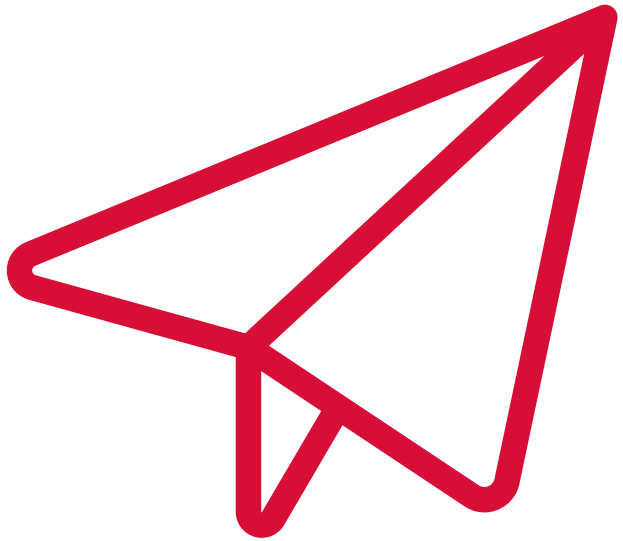
Hilfreiche Konzepte

- Die Kunst des Machbaren
- Szenarien-basiertes Arbeiten
- Trust, but Verify
- Gesunde Prozess-Skepsis / Ausnahmezustand
- Kein Live-Troubleshooting
- Delegation: Shift-Low
- Manchmal is' nix



Beispiel-Szenarien – Abgeflossene E-Mail

- Client 1-X kompromittiert
- Server kompromittiert
- Gegenseite kompromittiert
- Kanal kompromittiert
- Private Weiterleitung



Notfallplan – Tipps

- Kurz halten
- Aktuell halten
- Autor im Betrieb halten
- Mit Verstand lesen
- Nicht sklavisch dran halten

Notfallplan – Inhalte

- Ansprechpartner
  - Intern, Extern
- Informationspflichten
  - Behörden, Kunden, Mitarbeiter, Dienstleister…
- Nennung kritischer Businessprozesse
- Vielleicht ein paar Entscheidungen/Szenarien
- Anhang: Netzplan, Assets…
- Anhang: Kontaktadressen, Meldeformulare

Notfallplan – Anti-Patterns

- **DER.2.1.A2***
  - So MÜSSEN Verhaltensregeln für die verschiedenen Arten von Sicherheitsvorfällen beschrieben sein.
- **DER.2.1.A5***
  - Damit ein Sicherheitsvorfall erfolgreich behoben werden kann, MUSS der Zuständige zunächst das Problem eingrenzen und die Ursache finden.
- **Rahmen richtig wählen**
  - Jeder Monday-vor-Patch-Tuesday ein Sicherheitsvorfall?

*Quelle: BSI. DER.2: Behandlung von Sicherheitsvorfällen

Gerichtsfest/Gerichtsverwertbar

Anforderungen

- Lückenlose und detaillierte Dokumentation
  - Prüfsummen
  - Beweismittelformulare
  - Arbeitspapiere und Bericht
- Einhaltung der Beweismittelkette
- Vier-Augen Prinzip
- Wahrung des Datenschutzes
- Objektivität und Integrität

Zu beachten

- Wichtig bei strafrechtlich relevanten Vorfällen
- Darauf ~~kann~~ sollte in ~~manchen~~ den meisten Fällen verzichtet werden
- „Nachholen“ ist oftmals unmöglich

Notfallplan – Wie vorhalten?

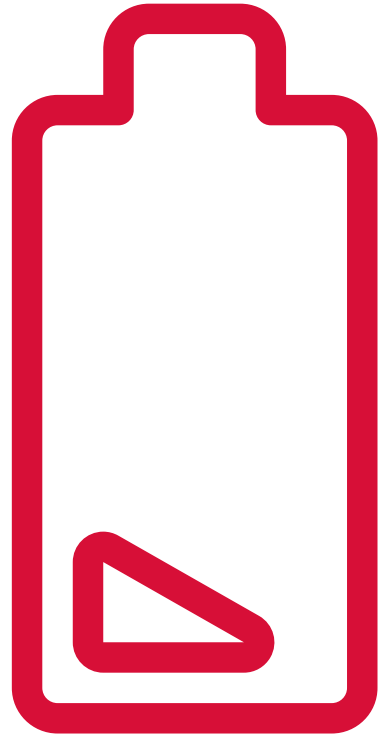
- Nicht (nur) Papier
- Nicht (nur) auf einem Share
- Offline-Laptop,
  1x pro Woche aktualisieren

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

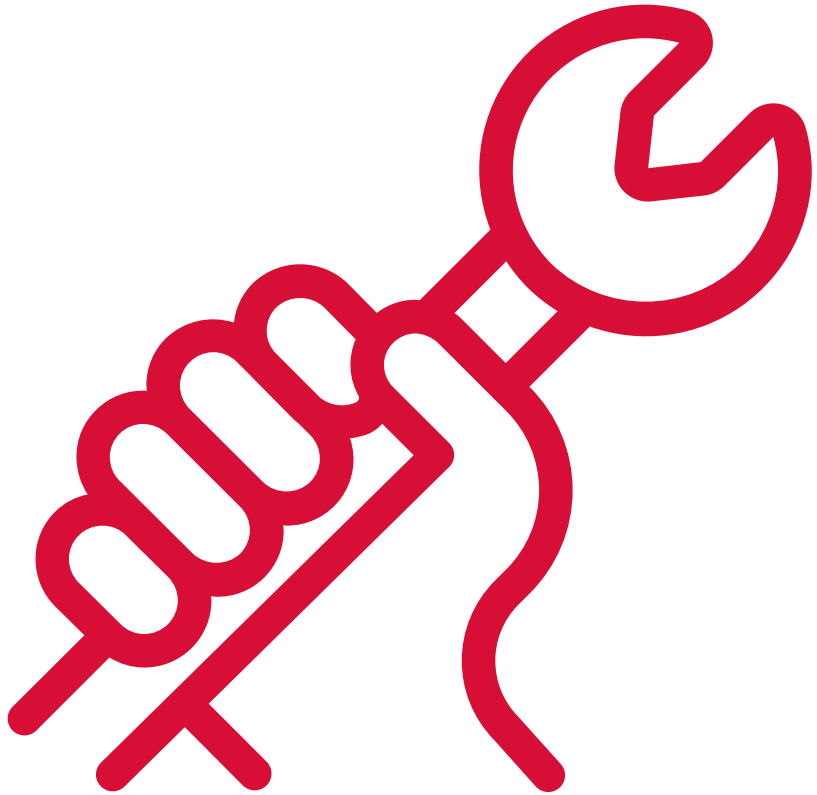
Beispiel-Incident – Phishing-Welle?

- KRITIS-Unternehmen
- Abgeflossene E-Mails als Basis für Phishing
- Mail-Signatur auch in vom Server ausgehenden Mails entdeckt



Beispiel-Incident – Manchmal is‘ nix

- Produzierender Betrieb
- Telekom meldet C&C-Traffic
- 3, 4, 5, 6 IPs – aus der OT
- lsass.dmp auf einem DC

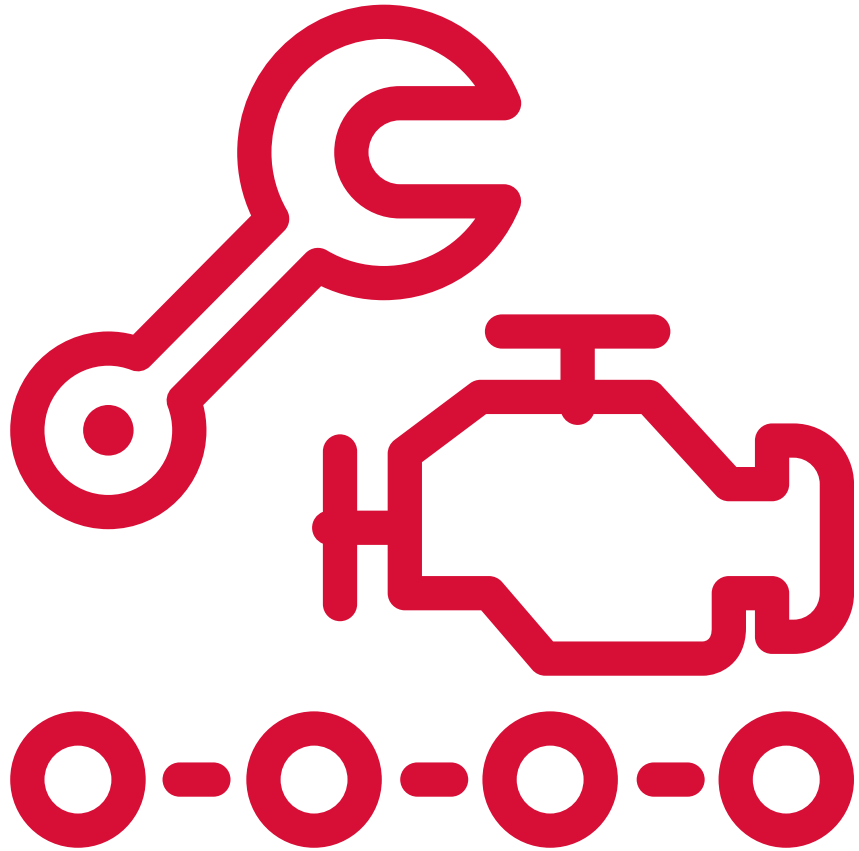


Beispiel-Incident – Grüne Wiese

- Betrieb mit vielen „Nutzern“
- Vollverschlüsselt auf Hypervisor-Ebene (Tag X)
- Backups beeinträchtigt
- Initiale Kompromittierung: ???
- Vollkompromittiert: X – 3 Monate

Beispiel-Incident – Grüne Wiese?

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

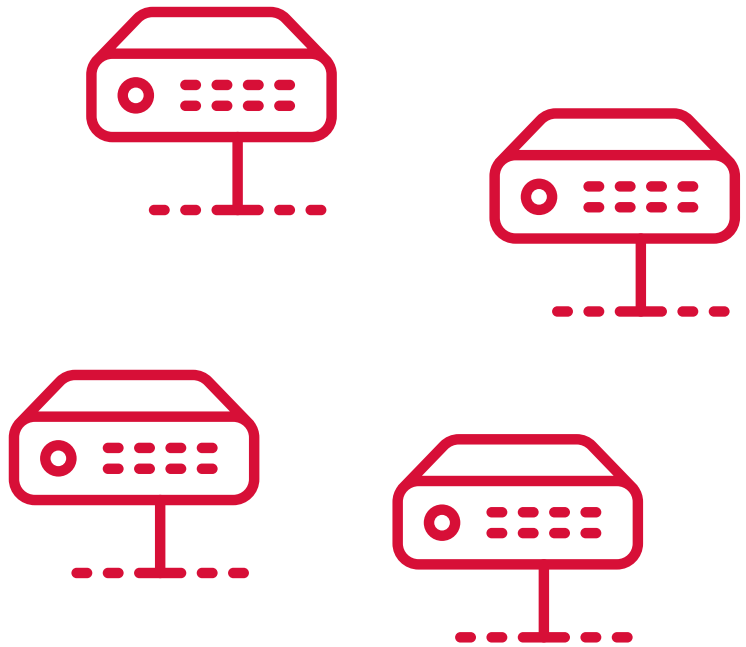


Beispiel-Incident – Payment Diversion

- Soziales Unternehmen
- Kontonummer geändert
- Abgeflossene E-Mails

Beispiel-“Incident“ – Notstromprobe

- Rechenzentrum
- Diesel-Generatoren fallen aus
- Akkus leer
- Überhitzung der Server
- Facility Management im kritischen Pfad



Kontakt für Fragen zu Penetrationstests, Incident Response & Notfallplan

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**

  2. Mai, 15:00 – 15:30 Uhr

- **Vorbereitung auf Cyberangriffe – Üben für den Ernstfall**

  15. Mai, 15:00 – 16:00 Uhr

Informationen und Anmeldung unter:
www.secunet.com/industrie


secunet