VSW
Bundesverband

Lessons Learned nach einem Cybervorfall

Erkenntnisse, die man vorher selten sieht / hat ?!

Referent: Peter Hecko

Die Realität:
Kein Plan überlebt den Erstkontakt

VSW
Bundesverband

- Playbooks ≠ Realität
- Zeitdruck, Unsicherheit, Informationslücken
- Unerwartete technische und organisatorische Abhängigkeiten
- Menschenfaktoren, die Prozesse überlagern

Kommunikation:
Der unterschätzte Brandbeschleuniger

VSW
Bundesverband

- Interne Kanäle plötzlich unsicher oder nicht verfügbar
- Ad-hoc-Krisenkommunikation ohne „abgestimmte Messages“
- Parallelkommunikation von IT, ISB, Geschäftsführung, KBR usw.
- Fehlende Kontaktlisten & Kommunikationsdiagramme

Rollen & Verantwortlichkeiten brechen sofort auf

VSW
Bundesverband

- Theoretische RACI vs. gelebte Realität
- Linienorganisation kollidiert mit Incident-Struktur
- Abwesenheiten, Urlaub, Schichtmodelle → Rollendefizite
- Entscheidungsträger nicht erreichbar oder nicht vorbereitet

Asset- & Netzwerk-Transparenz fehlen immer dann, wenn man sie braucht

VSW
Bundesverband

- Wie viele Systeme sind wirklich betroffen?
- Schatten-IT / vergessene Server / alte Testumgebungen
- Keine aktuelle CMDB / Asset-Liste
  - Was sind für uns Kritische Systeme?
- OT/MT-Geräte mit unbekanntem Patchstand

Incident-Dokumentation bricht unter Stress zusammen

VSW Bundesverband

- Ad-hoc-Entscheidungen ohne Protokoll
- Logs und Chatverläufe verstreut über verschiedene Chats, Mails usw.
- Fehlende einheitliche IR-Dokumentationsvorlage
- Beweissicherung wird vergessen oder zu spät gestartet

Unerwartete regulatorische Implikationen

VSW
Bundesverband

- Meldepflichten (NIS2, KRITIS, Datenschutz) kollidieren zeitlich
- Unterschiedliche Auslegungen bei Konzern, Legal, ISB
- Mitbestimmung / KBR muss früh eingebunden werden
- Versicherungen verlangen bestimmte Nachweise

Technische Hürden im laufenden Betrieb

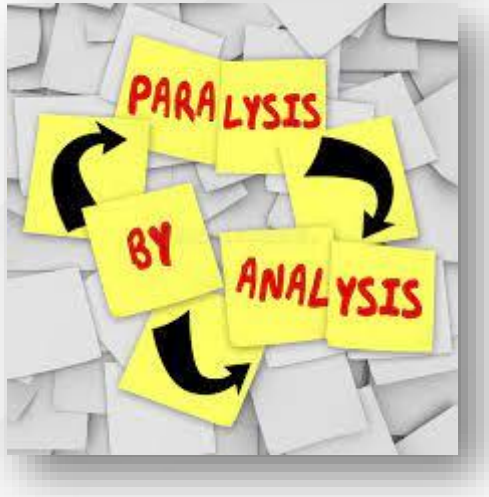
VSW Bundesverband

- Systeme dürfen nicht neu gestartet / gepatcht werden
- Forensik kollidiert mit Betriebsnotwendigkeiten
- „Wer darf was ausschalten?“
- Kritische Systeme ohne funktionierendes Backup

Entscheidungsdruck & psychologische Faktoren

VSW Bundesverband

- Führungskräfte werden nervös → Risiko hoher Fehlentscheidungen
- SOC/CDC-Teams arbeiten an der Belastungsgrenze
- „Analysis Paralysis“ im Forensik-Team
- Emotionaler Stress → Kommunikationsfehler



Lessons-Learned-Prozess selbst richtig gestalten

VSW Bundesverband

- Schnelle Auswertung innerhalb 72h
- Saubere Chronologie: Was wussten wir wann?
- Fokussiert auf Ursachen, nicht auf Schuld!
- Dokumentation in einer gemeinsamen Plattform
- Präsentation der Maßnahmen in die verschiedene Abteilungen
- Ableitung konkreter Maßnahmen für „Next Time Ready“
  - Maßnahmen in kurz- /mittelfristig- / langfristig
  - Übergeordnetes Projektmanagement ist wichtig

VSW
Bundesverband

Vielen Dank!

Fragen?