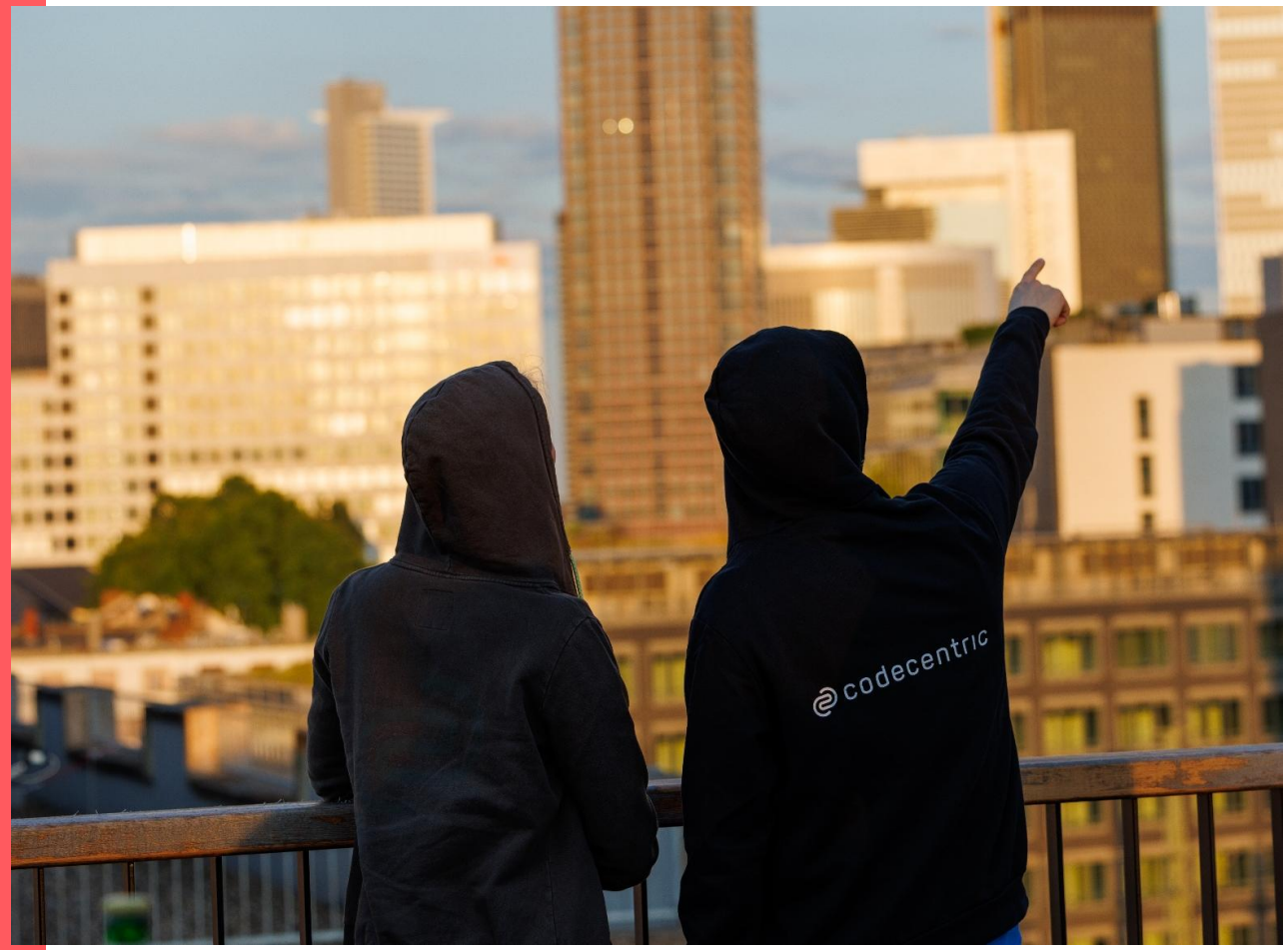
Kommunale IT-Security

Prävention und effektive Reaktionsstrategien



28.04.2026

codecentric
it security

Timo Rath

Service Lead IT-Security

- 35 Jahre
- Home Office in Osnabrück
- Seit 2017 in der IT-Security
- Fachliche Schwerpunkte Pentests und Assessments
- Teamführung

codecentric
it security

Motivation

Der IST-Zustand

Status quo

⚠ Juli 2021 - Landkreis Anhalt-Bitterfeld

Katastrophenfall durch Verschlüsselung der Verwaltung

National

Cyberangriff auf die Landkreisverwaltung Anhalt-Bitterfeld

Gefahrenkategorie

Technologische Gefahr

Hauptursache

Unzureichende Cybersicherheit

Auswirkung

Datenverschlüsselung, Einschränkung der Handlungsfähigkeit der Verwaltung

Ort

Anhalt-Bitterfeld (Sachsen-Anhalt)

Ereigniszeitraum

2. Juli 2021

Sektor

Staat, Verwaltung mit Kaskaden-Effekten auf andere Sektoren

Quelle: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

Status quo

- ⚠ Juli 2021 - Landkreis Anhalt-Bitterfeld

  Katastrophenfall durch Verschlüsselung der Verwaltung

- ⚠ 2023-2024: jede vierte Kommune betroffen

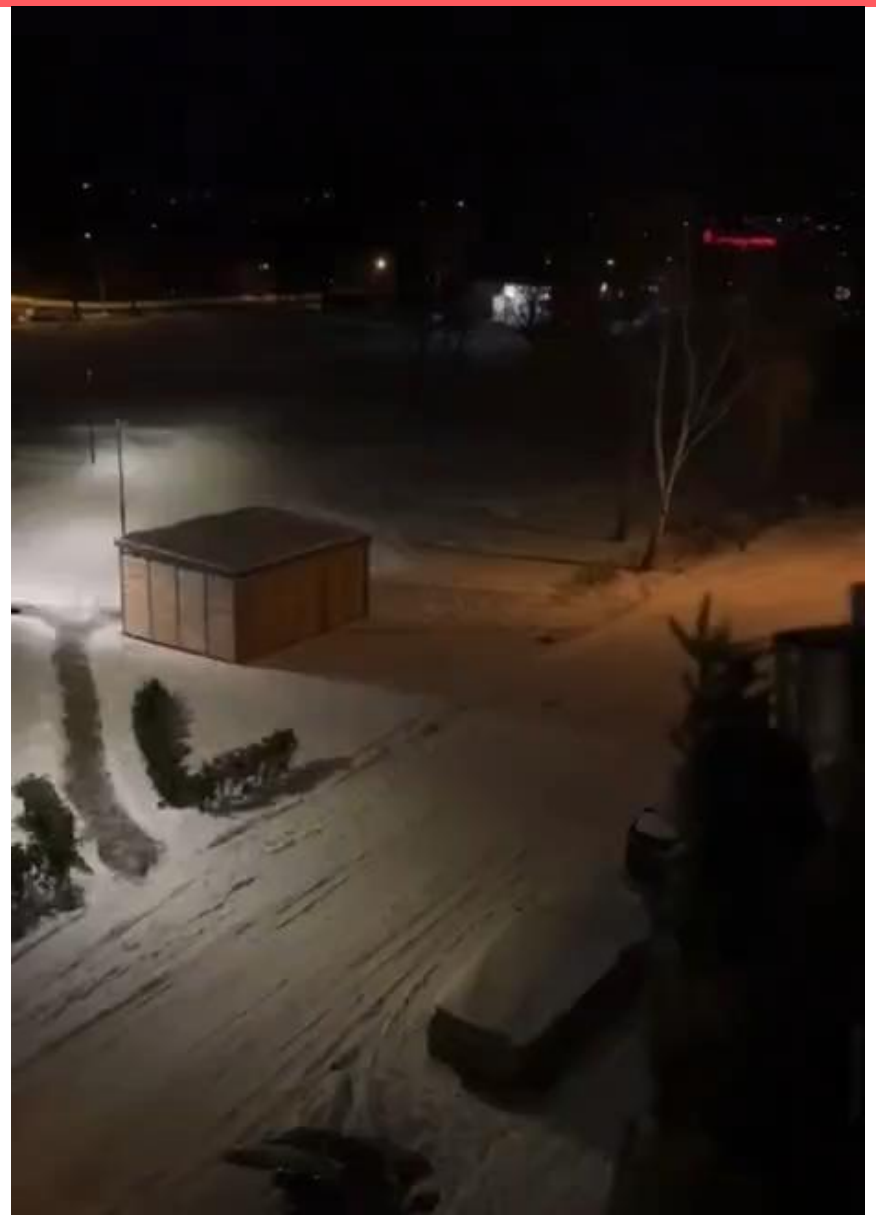
- ⚠ Jan 2026 - Stadtverwaltung Lübben & Falkenberg-Höhe

  Cyberangriff

- ⚠ Jan 2026 - Stadtverwaltung Halle: Cyberangriff

  Angriff auf Sirenenwarnsystem, Bevölkerung verunsichert

Status quo



„Active Shooter in progress. Lockdown! Lockdown! Lockdown!“

Status quo

- ⚠ Juli 2021 - Landkreis Anhalt-Bitterfeld
  Katastrophenfall durch Verschlüsselung der Verwaltung
- ⚠ 2023-2024: jede vierte Kommune betroffen
- ⚠ Jan 2026 - Stadtverwaltung Lübben & Falkenberg-Höhe
  Cyberangriff
- ⚠ Jan 2026 - Stadtverwaltung Halle: Cyberangriff
  Angriff auf Sirenenwarnsystem, Bevölkerung verunsichert
- ⚠ Jan 2026 - Stadtverwaltung Heinsberg: Cyberangriff
  Stadtverwaltung kompromittiert, mehrtägiger Ausfall
- ⚠ Jan 2026 - Stadtverwaltung Schorndorf: Datendiebstahl
  Daten von 20.000 Einwohnern gestohlen
- ⚠ Feb 2026 - Stadtverwaltung Konstanz: Datendiebstahl
  Mobile Device Management betroffen, Mitarbeiterdaten abgeflossen
- ⚠ Apr 2026 - Verbandsgemeindeverwaltung Sprendlingen-Gensingen: Ransomware
  Notbetrieb nach einer Woche, Ausfall dauert an

Quelle: https://kommunaler-notbetrieb.de

Kommunen als attraktive Ziele

Zahlungsdruck

- Bürgerservices müssen funktionieren
- Keine Alternative
- Politischer Schaden
- Sozialleistungen
- Höhere Lösegeldzahlung

Schache Defense

- Knappe IT-Budgets
- Veraltete Systeme
- Wenig Fachpersonal
- Kein SOC/SIEM
- Leichtes Ziel

Wertvolle Daten

- Meldedaten aller Einwohner
- Steuerdaten
- Grundbuch, Kataster
- Weiterverkauf an staatliche Akteure möglich

Bedrohungslandschaft

Script-Kiddies

- Keine gezielten Aktionen
- Funde durch Zufall
- Wenig Mittel

Hacktivisten

- Politisch motiviert
- DDos-Angriffe
- Zielgerichtet
- Hoher Zeiteinsatz

Cyberkriminelle

- LockBit, BlackCat, ...
- Finanziell motiviert
- Professionelles Businessmodell
- Keine gezielte Auswahl von Zielen

Staatliche Akteure

- APT-Gruppen
- Politisch motiviert
- Zielgerichtete, lang geplante Aktionen
- Nahezu unbegrenzte Mittel

Der Angriff

Was passiert bei einer Ransomware?

Angriffsverlauf

①	②	③	④	⑤
Erstkontakt	**Angriff**	**Initialer Foothold**	**AD-Kompromittierung**	**Exfiltration und Verschlüsselung**
Angreifer findet öffentlich erreichbares VPN-Gateway mit bekannten Schwachstellen	Ausnutzung der bekannten Schwachstellen und Übernahme des VPN-Gateways	Durch Brute-Forcing Übernahme eines Benutzers mit kurzem Passwort im Active Directory	Weitere Zugangsdaten werden auf Netzlaufwerk gefunden und sich darüber im Netzwerk ausgebreitet -> Domain Admin	Daten werden über HTTPS exfiltriert, Backups gelöscht und Daten verschlüsselt

💰 Erpressungssumme: 0.5 Millionen €

Angriffsverlauf

Angriffsverlauf

Chaos

Entdeckung des Angriffs

Unkoordinierte Phase

Evaluierung des Ausmaßes

Suche nach Hilfe

Eindämmung

Externe Hilfe

Triage

Systeme isolieren

Accounts sperren

Logs einsammeln

Analyse

Forensik

Angriffspfad identifizieren

Notbetrieb

Notnetz aufbauen

Priorisierte Dienste rudimentär aufbauen

Wiederaufbau

Systeme neu aufsetzen

Backups einspielen

Daten waschen

💰 Kosten: 2.5 Millionen €

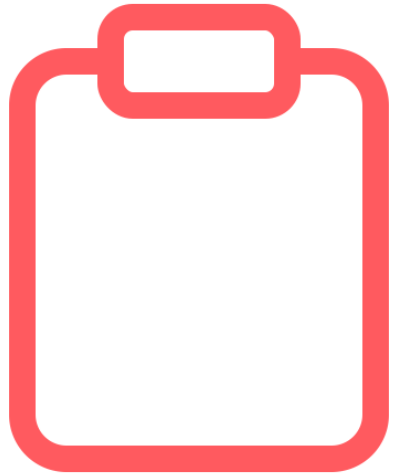
Präventive Maßnahmen

Angriffe verhindern

codecentric
it security

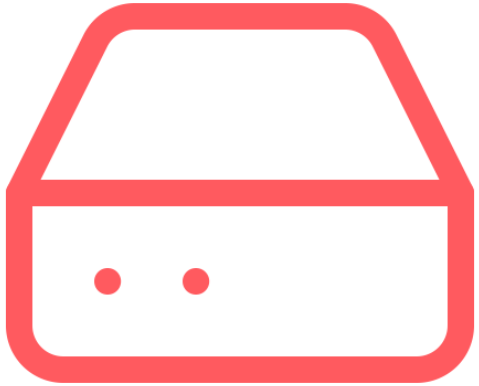
Prävention – Notfallplan

- Dokumentierter Prozess für den Ernstfall: Wissen, was wann wie zu tun ist
- Planung schafft Sicherheit und vermeidet Fehler
- Bestandteile:
  - Kontaktlisten und Eskalationsketten (intern und extern)
  - Rollen und Verantwortlichkeiten (Krisenstab, Presse, Bürgerbetreuung, …)
  - Priorisierung der Fachanwendungen
  - Wiederanlaufpläne der Fachanwendungen
- Analoge Kopie vorhalten
- Regelmäßige Tests durchführen
  - Ein Plan, der nie getestet wird, ist kein Plan – er ist eine Illusion.



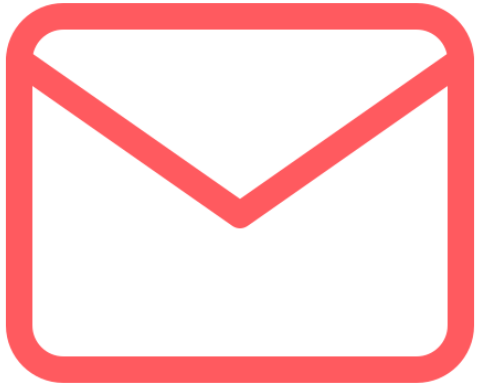
Prävention – Backups

- 3-2-1-Regel
  - 3 Kopien der Daten
  - 2 verschiedene Speichermedien
  - 1 Kopie offline oder zumindest Ransomware-sicher
- Immutable Backups (unveränderlich)
  - Ransomware kann Backups verschlüsseln
  - Schreibschutz auf Backup-Ziel
- Ausfallzeiten definieren
- Regelmäßige Wiederherstellungstests



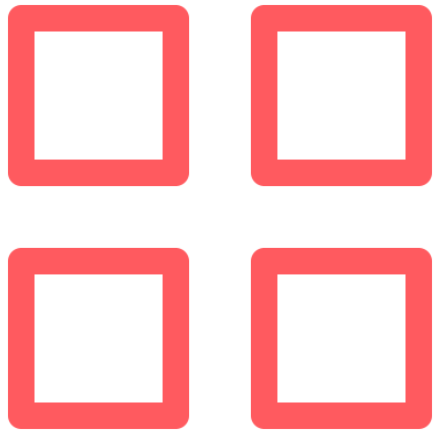
Prävention – Phishing & Social Engineering

- Häufigster Angriffsvektor
  - Der Großteil aller Cyberangriffe beginnt mit einer Phishing-E-Mail
  - Vishing per Telefon wird mit steigender KI-Nutzung zunehmen
- Technische Gegenmaßnahmen treffen
  - E-Mail-Server härten (SPF, DKIM, …)
  - Externe E-Mails klar kennzeichnen
- Mitarbeiter-Awareness
  - Regelmäßige Schulungen aller Mitarbeitenden
  - Simulierte Phishing-Kampagnen
  - Klare Meldewege etablieren
  - Sinnvolle Fehlerkultur sicherstellen
  - Kein technisches System ersetzt den geschulten Mitarbeitenden!



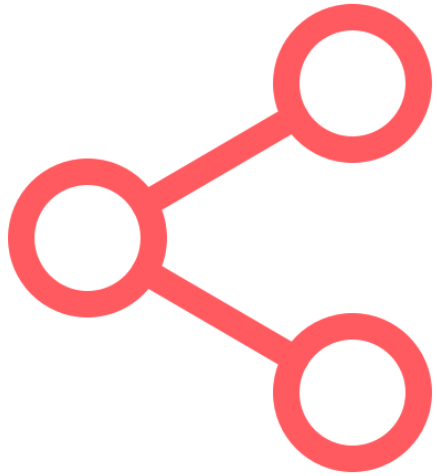
Prävention – Assetmanagement

- Man kann nur schützen, was man kennt
  - Vollständige Inventarisierung aufbauen (Hardware, Software, Cloud-Dienste, ...)
  - Automatische Discovery-Tools für unbekannte/neue Geräte im Netzwerk
- Schatten-IT verhindern
  - Private Geräte in Firmennetzen per Richtlinie verbieten
  - Assetliste mit Einkaufsprozess verknüpfen
- Lebenszyklusmanagement
  - Alte Systeme identifizieren und abschalten/isolieren
  - Ungepatchte Altsysteme sind beliebtes Einfallstor für Angreifer
- Patchmanagement aufbauend auf Assetliste
  - Patches müssen zeitnah bewertet und eingespielt werden
  - Prozess etablieren und leben
- Assetmanagement ist die Grundlage für weitere Sicherheitsmaßnahmen.



Prävention – Netzwerksegmentierung

- Netzwerkzonen definieren und trennen
  - Verwaltungsnetz, Bürgernetz, Gebäudetechnik, Administration, …
  - Ziel: ein kompromittiertes System darf nicht alle anderen gefährden
- Zugriffskontrolle im Netzwerk
  - Klare Zugriffsregeln etablieren
  - Need-to-know-Prinzip: Minimaler Zugriff, der wirklich benötigt wird
  - Nur autorisierte Geräte ins Netzwerk lassen
- In einem flachen Netz ohne Segmentierung kompromittiert ein Einbruch direkt alles.

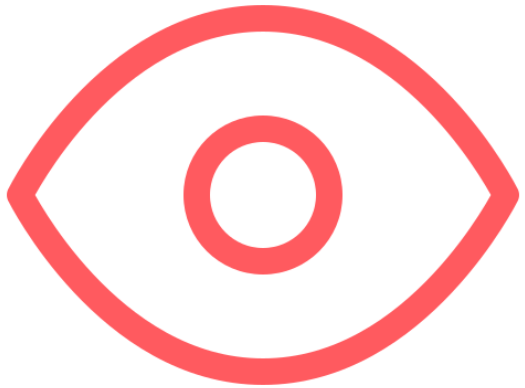


Prävention – Passwortrichlinie und MFA

- Starke Passwörter einführen
  - Mindestens 12 Zeichen, verschiedene Zeichenarten
  - Individuelle Passwörter pro Konto
  - Länge = Sicherheit
- Passwortmanager nutzen
  - Erleichtert die Nutzung individueller Passwörter
  - Erlaubt beliebig lange Passwörter
  - Sichere gemeinsame Nutzung von Passwörtern wenn notwendig
- Verpflichtende Multi-Faktor-Authentisierung
  - Alle Internet-erreichbaren Dienste absichern
  - Pflicht für administrative Tätigkeiten
- Schwache Passwörter und fehlende MFA begünstigen die Ausbreitung von Angreifern!

Prävention – IT-Sicherheitsmonitoring

- Angriffe frühzeitig erkennen
  - Angreifer halten sich teilweise sehr lang (> 200 Tage) in Netzwerken auf
  - Ziel: Erkennung innerhalb von Stunden, nicht Monaten
- Security Information & Event Management (SIEM)
  - Zentrale Sammlung und Korrelation aller Logs
  - Automatische Alarme bei Auffälligkeiten
  - Muss dauerhaft überwacht werden
- Endpoint Detection & Response
  - Verhaltenserkennung auf Clients
  - Automatische Isolierung betroffener Geräte, weitere Maßnahmen
- Security Operation Center
  - Bearbeitet Meldungen
  - Kann mehrere Kommunen gleichzeitig betreuen
- Pro Tag erscheinen über 100 neue Schwachstellen – ohne Monitoring ist man blind.



Prävention – Dienstleistersicherheit

- IT-Dienstleister als Einfallstor
  - Supply-Chain-Angriffe nehmen massiv zu
- Vertraglich absichern
  - IT-Sicherheitsanforderungen (präventiv und reaktiv) in Verträgen prüfen und
  - Auditrechte einräumen: Recht zur Sicherheitsüberprüfung des Dienstleister
  - Meldepflichten: Wann muss der Dienstleister Vorfälle melden
- Zugänge absichern
  - Wie greift der Dienstleister auf IT-Systeme zu?
- Redundanzen schaffen
  - Gibt es Ersatz für Dienstleister oder genutzte Services?
- Die eigene IT-Sicherheit ist nur so stark wie das schwächste Glied.

Reaktive Maßnahmen

Richtig auf Angriffe reagieren

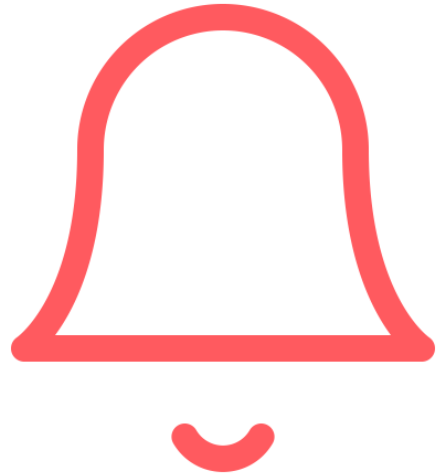
codecentric
it security

Reaktion – Situation einfrieren

- Ruhe bewahren, Panikreaktionen vermeiden
  - Unkontrollierte Handlungen zerstören Beweise
- Systeme isolieren
  - Netzwerkkabel ziehen -> Angreifer aussperren
  - Eingeschaltete Geräte bleiben eingeschaltet
  - Ausgeschaltete Geräte bleiben ausgeschaltet
- Auffindesituation dokumentieren
  - Fotos von Bildschirmen machen
  - Zeitleiste erstellen, Zeitstempel bei Veränderungen notieren
- Notfallplan aktivieren und auf externe Hilfe warten!

Reaktion – Notfallpläne aktivieren

- Krisenstab einberufen
  - Regelmäßige Lagebesprechung
- Meldeketten einhalten
  - BSI informieren
  - LKA / Polizei: Strafanzeige (bei Ransomware) erstatten
  - Datenschutzbehörde bei Datendiebstahl innerhalb von 72 h informieren
  - Landesministerium je nach Schwere des Vorfalls
- Externe Hilfe anfordern
- Notbetrieb aus Notfallplan vorbereiten
  - Auf vorbereitete analoge Prozesse zurückgreifen



Reaktion – Krisenkommunikation

- Kommunikation nach außen nur über Pressesprecher
  - Kommunikation bündeln, einheitliches Bild abgeben
  - Keine spontanen Kommentare von Mitarbeitenden
- Interne Kommunikation zuerst
  - Mitarbeitende informieren: Was sollen sie tun, was nicht?
  - Klare Anweisungen
- Externe Kommunikation: Bürger und Öffentlichkeit
  - Proaktiv kommunizieren: Schweigen erzeugt Gerüchte und Vertrauensverlust
  - Klare Botschaften: Was ist passiert? Was tun wir dagegen?
  - Keine Spekulationen über Täter
- Angreiferkommunikation
  - Nicht selbst mit den Tätern Kontakt aufnehmen, keine Links öffnen, keine Kommentare per Telefon
- Transparenz rettet Vertrauen

Fazit

Was bleibt?

Learnings

- Cyberangriffe passieren
- Prävention: Maßnahmen zeitnah umsetzen
  - Notfallplan erstellen
  - Backupstrategie
  - Sichere Passwörter und MFA einrichten
- Reaktion: Merken für den Ernstfall
  - Keine Panikreaktionen
  - Systeme vom Netzwerk trennen
  - Experten hinzuziehen

Kosten

- IT-Security ist kein Kostenfaktor – es ist Risikomanagement!
- Ein Ransomware-Angriff kostet im Schnitt 10-50x mehr als präventive Sicherheitsmaßnahmen.
- Cybersicherheit ist keine IT-Aufgabe – es ist eine Führungsaufgabe

codecentric
it security

codecentric AG
Hochstraße 11
42697 Solingen

Timo Rath
Service Lead IT-Security
timo.rath@codecentric.de
www.codecentric.de/it-security

+49 1514 626 714 3