sure[secure]

Game Over für Hacker -

Wie minimiert man den Impact von Cyberangriffen?

Ali Gülerman - CTO

IT-Security made with

DIGITALISIERUNG BRAUCHT INFORMATIONSSICHERHEIT

WARUM CYBERANGRIFFE PASSIEREN

Künstliche Intelligenz

Cloud Computing

Smart Cities

IoT

Robotik

Mobile Computing

Industrie 4.0

Digital Health

AI / VR

Digitalisierung als Treiber

- Digitalisierung betrifft **alle Lebensbereiche**
- Digitalisierung nutzt und produziert **schützenswerte Daten**
- Digitalisierung basiert auf **angreifbarer IT**

INOFRMATIONSSICHERHEIT ist essenziell für die DIGITALISIERUNG!

Ransomware as a Service

Das Geschäftsmodell hinter Cyberkriminalität

SIE WURDEN ALSO GEHACKT… UND NUN? LÖSEGELD ZAHLEN?

RANSOMWARE AS A SERVICE

Soll ich bezahlen…?!

NEIN!

1. Es gibt **keine Garantie**, dass Ihre IT hinterher wieder funktioniert.
2. Der Angreifer hat **weiterhin Kontrolle** über Ihre IT.
3. Das kriminelle System wird unterstützt und die **nächsten Angriffe finanziert**.

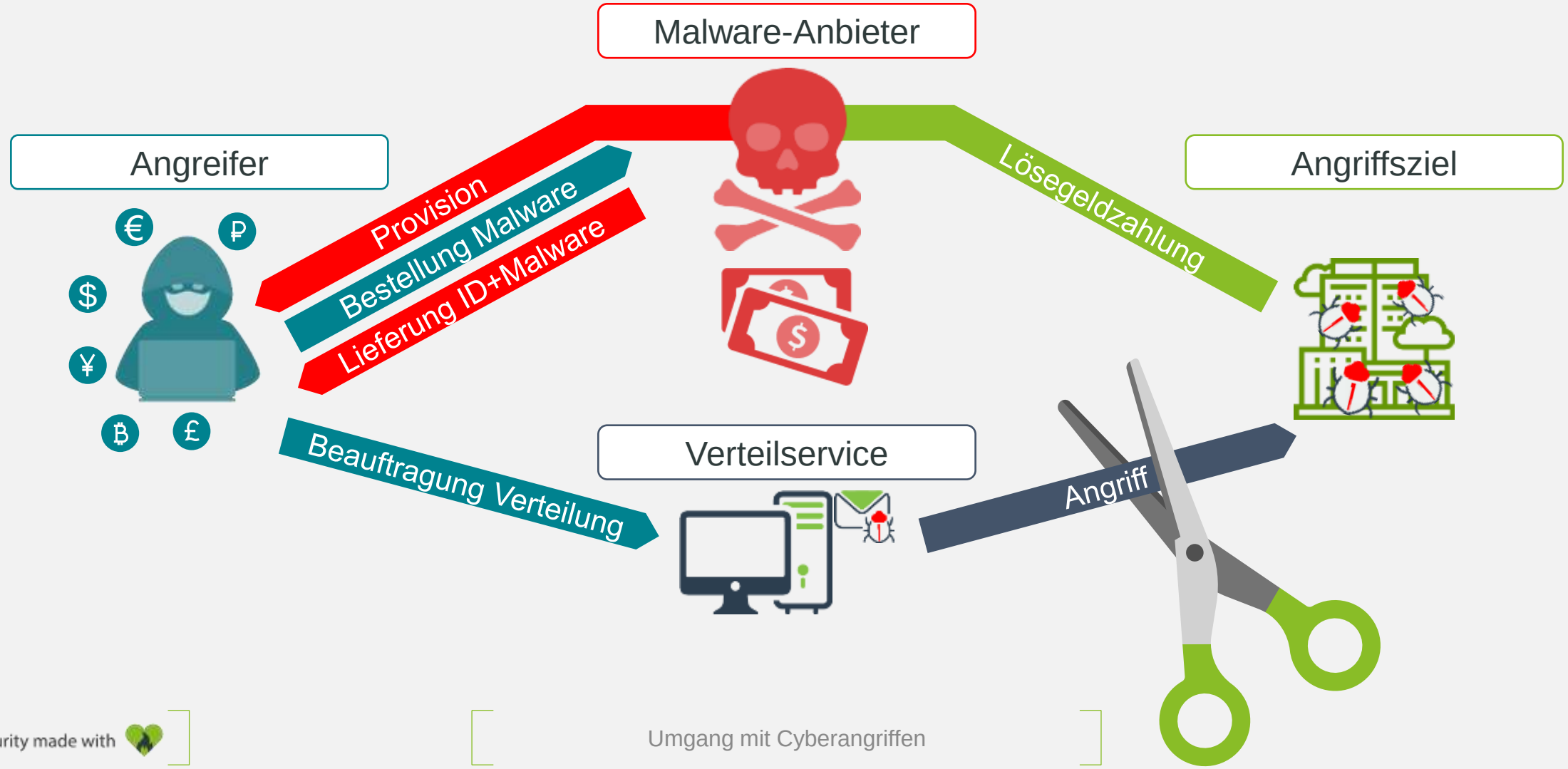
VIELE PLAYER, IDENTISCHE VORGEHENSWEISE

RANSOMWARE AS A SERVICE

Angriffstyp	Verschlüsselungstrojaner
Zielsetzung	Erpressung -> Lösegeldforderung
Druckmittel	Veröffentlichung oder Verkauf sensibler Daten
Business-Modell	As a Service

RANSOMWARE-ANGRIFFE ALS BUSINESS-MODELL

RANSOMWARE AS A SERVICE

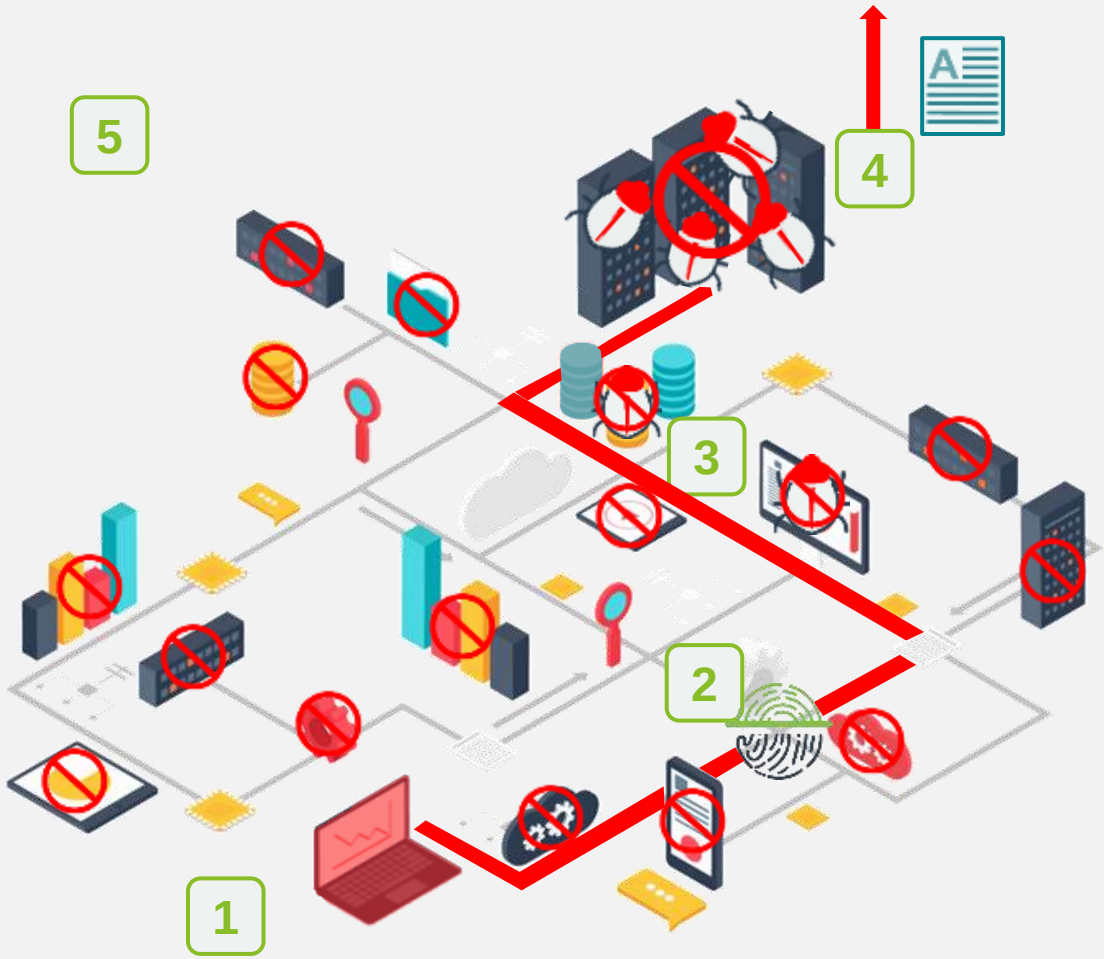


Aus dem Lehrbuch: Cyberangriff

Und daraus resultierende Schäden

ANGRIFF FINDET LANGE VOR DER VERSCHLÜSSELUNG STATT

PROTOTYPISCHER ANGRIFFSVERLAUF VOM EINDRINGEN BIS ZUM VERSCHLÜSSELN



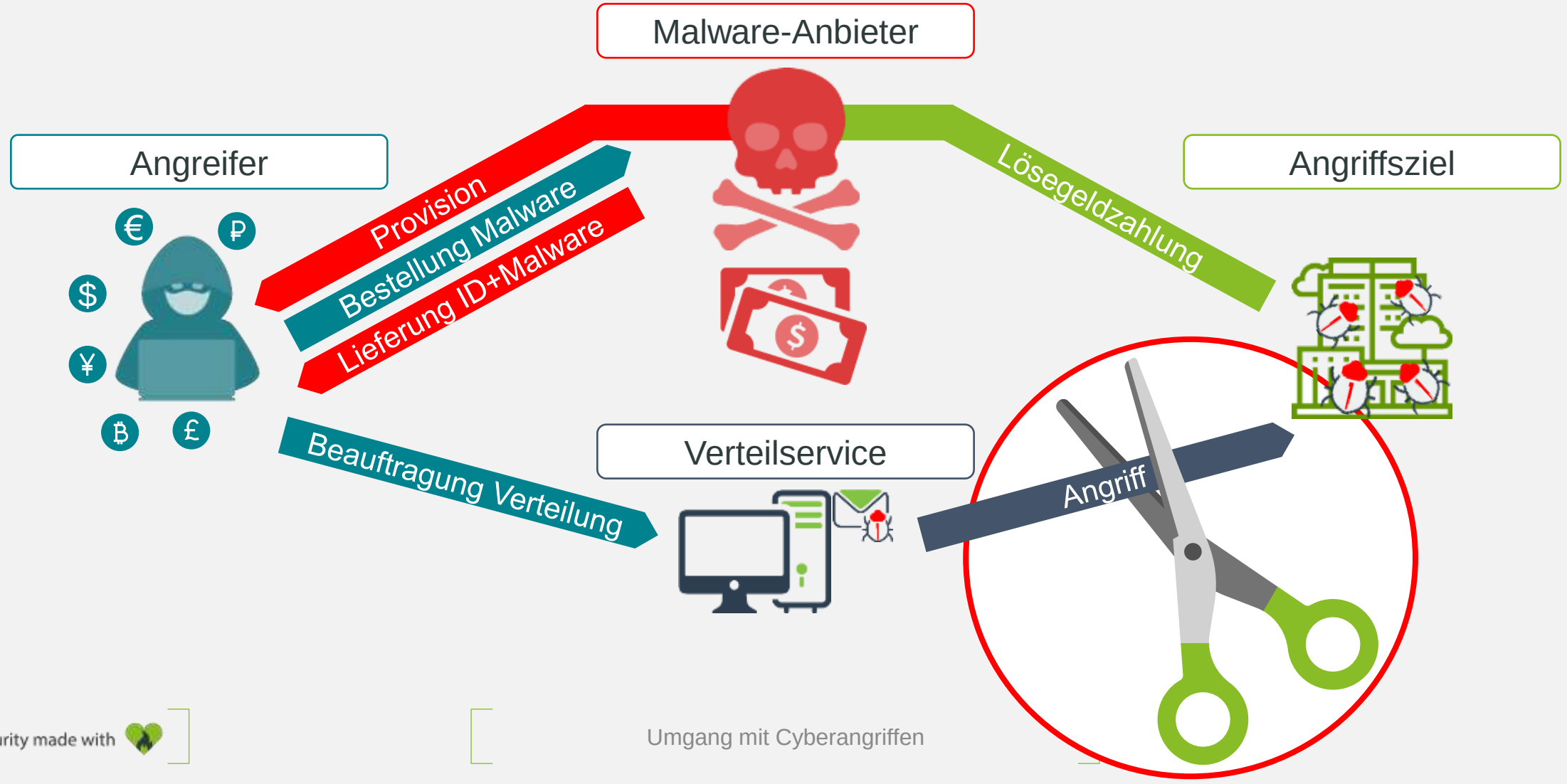
1. **Eindringen**
   a) **Malware** wird unwissentlich ausgeführt
   b) **Schwachstelle** wird ausgenutzt
2. Erweiterung der **Berechtigungen** *(Mimikatz)*
3. Schaffen von **Persistenzen**
   - Angreifer nistet sich ein und …
   - … bewegt sich im Netzwerk (*PsExec*)
4. **Exfiltration** von Daten
5. Ausführen der **Verschlüsselung**

Ø 180 Tage (!)

Vorbereitung auf Incidents

WO ANSETZEN BEIM SCHUTZ VOR CYBERATTACKEN?

KONZENTRATION AUF DAS WESENTLICHE



LOG-QUELLEN NUTZEN, AUSWERTEN UND VERSTEHEN

SECURITY OPERATION CENTER AS A SERVICE

Wer?

- SOC Analysten
- Security Consultant
- Forensiker
- SOC Admin

Was?

- Endpoint Monitoring
- Authentication Monitoring
- Network Monitoring
- Vulnerability Scanning

Incident Response Management

Basis Ihrer Cybersecurity Strategie

IT-Security made with

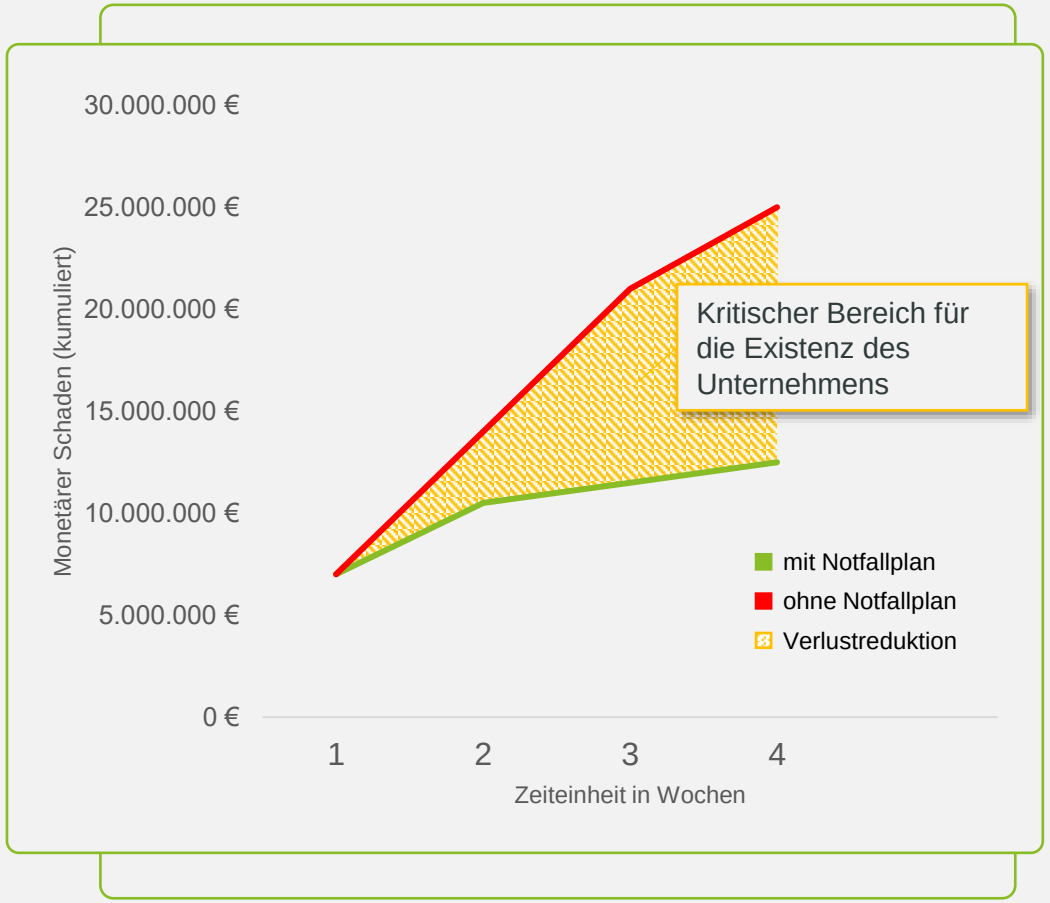
SICHERHEITSVORFALL IST EIN WETTLAUF GEGEN DIE ZEIT

INCIDENT RESPONSE MANAGEMENT

Sind sie bereit für das Rennen?

Benchmark-Werte – ohne gute Prävention:

- Dauer bis zum Notbetrieb:
  2 bis 4 Wochen
- Dauer bis zum erweiterten Notbetrieb:
  4 bis 8 Wochen
- Dauer bis zum Normalbetrieb:
  6 bis 12 Monate



Worum geht es?

DATEN

GELD

UMSATZ

REPUTATION

WELCHE RESSOURCEN SIND NÖTIG

IRM: VORBEREITENDE MAßNAHMENN

Interne & externe Security-Experten → SMEs, IT-Forensiker, Incident Manager und Verantwortlichkeiten bestimmen

Notfallbudget → Externe Berater, Hard- und Software, Pizza

Wiederherstellungsplan → Wiederherstellung eines Notfallbetriebs (Kernprozesse eines Unternehmens)

WIE BEREITEN SIE SICH RICHTIG VOR?

INCIDENT RESPONSE PREPARATION

BESTANDTEILE DES IRMP

INCIDENT MANAGMENT RESPONS PLAN (IRMP)

INCIDENT KLASSI-FIZIERUNG

INCIDENT ERKENUNG

INCIDENT MELDUNG

INCIDENT ERFASSUNG

INCIDENT BEWERTUNG

INCIDENT ESKALATION

INCIDENT REAKTION

Verantwortlichkeiten / Klare Definitionen der Rollen

Dokumentenmanagement / Aufbewahrung und Verwaltung

Rechtliche und Regulatorische Anforderungen

Lessons Learned / Bewertungsmechanismus des IRP

[s]

sure[secure]

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60
Telefax: +49 (0) 2156 975 49 78

E-Mail: kontakt@suresecure.de
www.suresecure.de

/suresecure.gmbh

/suresecure-gmbh

/suresecuregmbh

/suresecure GmbH

/the world of it security

/suresecure_de

IT-Security made with