Hackerangriff — und jetzt?

Tipps vom CyberSecurity-Profi
Martin Braun

Avaya Academy
webcast

Die Referenten stellen sich vor

Martin Braun

Geschäftsführer
CyberSecurity manufaktur GmbH

Uwe Pranghofer

Head of
Healthcare Business

Jürgen Urbitsch

Moderator

Cyberangriffe auf Deutsche Krankenhäuser haben um 220% zugenommen.

Über 30% aller Krankenhäuser weisen Angriffspunkte auf.

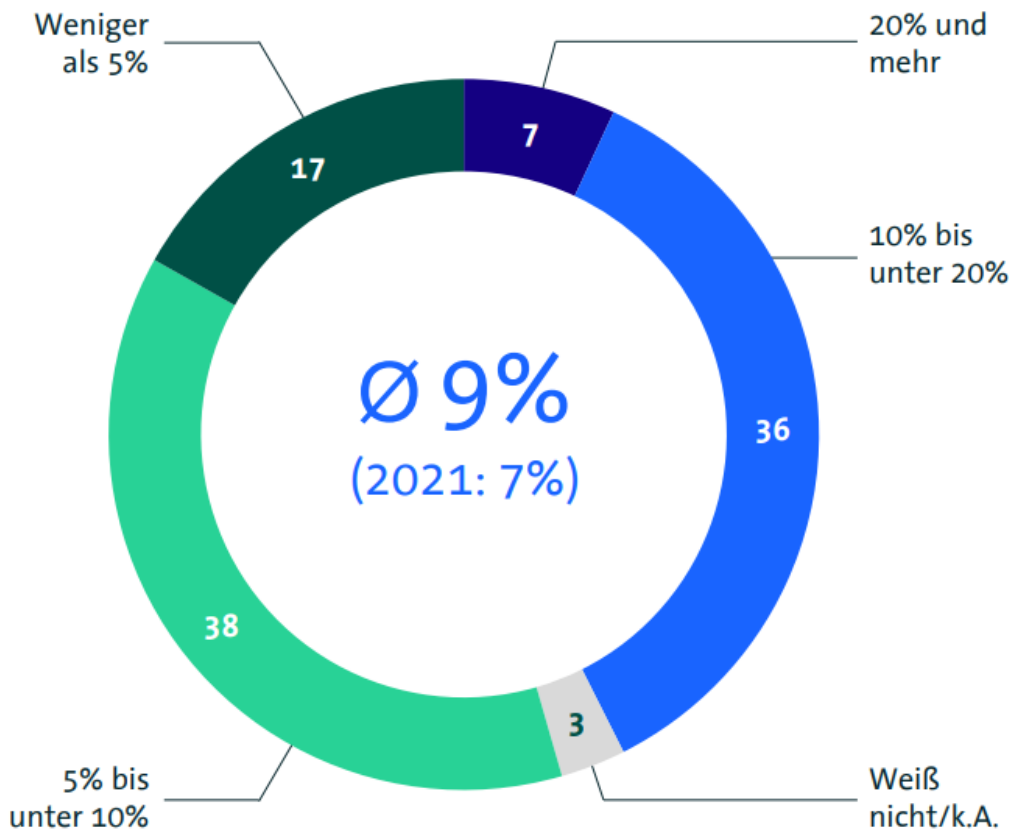
230 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen.

45% der Unternehmen bestätigen, dass Cyberangriffe die geschäftliche Existenz bedrohen.

Basis: Alle befragten Unternehmen (n=1.066) | Quelle: Bitkom Research 2022

Cybersicherheit: Anteil der Investitionen wächst – aber zu langsam

Wie hoch ist geschätzt der Anteil des Budgets für IT-Sicherheit am gesamten IT-Budget Ihres Unternehmens?



in Prozent

Basis: Alle Unternehmen (n=1.066) | Quelle: Bitkom Research 2022

bitkom

CyberSecurity manufaktur

Hackerangriff und jetzt?

Martin Braun
Geschäftsführer CyberSecurity manufaktur GmbH
Martin.braun@cybersecurity-manufaktur.de

CyberSecurity manufaktur

Unsere Agenda ?

1. Habe ich mich mit dem Thema Cyberangriff beschäftigt?
2. Wie sehen die Geschäftsmodelle der Hacker aus?
3. Wie läuft ein Hackerangriff ab (Erfahrungsbericht) ?
4. Was sind die Auswirkungen in meinem Unternehmen?
5. Kann ich einen Hackerangriff vermeiden oder nur die Auswirkungen mildern?
6. Wie muss ich mich als Unternehmen aufstellen ?

Habe ich mich mit dem Thema Cyberangriff beschäftigt?

- Wie hoch ist unser aktuelles Cyber-Risiko?
- Wie sind wir für Cyber-Attacken / Cyber-Risiken aufgestellt?
- Wie sieht der Incident-Response- und Desaster-Recovery-Plan aus?
- Wie sind unsere Daten und wie unsere Prozesse geschützt?
- Was kostet uns ein erfolgreicher Cyber-Angriff?

Unternehmen und ihre Organisationen – Opfer der unsichtbaren Angreifer

Kennen Sie die aktuellen Bedrohungen und die Angriffstechniken?

Kennen Sie die aktuellen Geschäftsmodelle der Angreifer

Kennen Sie Ihre Kronjuwelen?

Wissen Sie was sie schützen müssen?

Angriffsziel Mittelstand in Deutschland

Aktuelle Fakten – Quelle: BITKOM

War Ihr Unternehmen innerhalb der letzten 2 Jahre von Datendiebstahl, Industriespionage oder Sabotage betroffen oder vermutlich betroffen?

Nein:
12%

Ja:
88%

- **40%** Digitales Social Engineering
- **41%** Diebstahl von sensiblen digitalen Daten bzw. Informationen
- **42%** Digitale Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen
- **43%** Ausspähen von digitaler Kommunikation

Quelle: https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-100-Milliarden-Euro-Schaden-pro-Jahr

CyberSecurity manufaktur

Wie sehen die Geschäftsmodelle der Hacker aus?

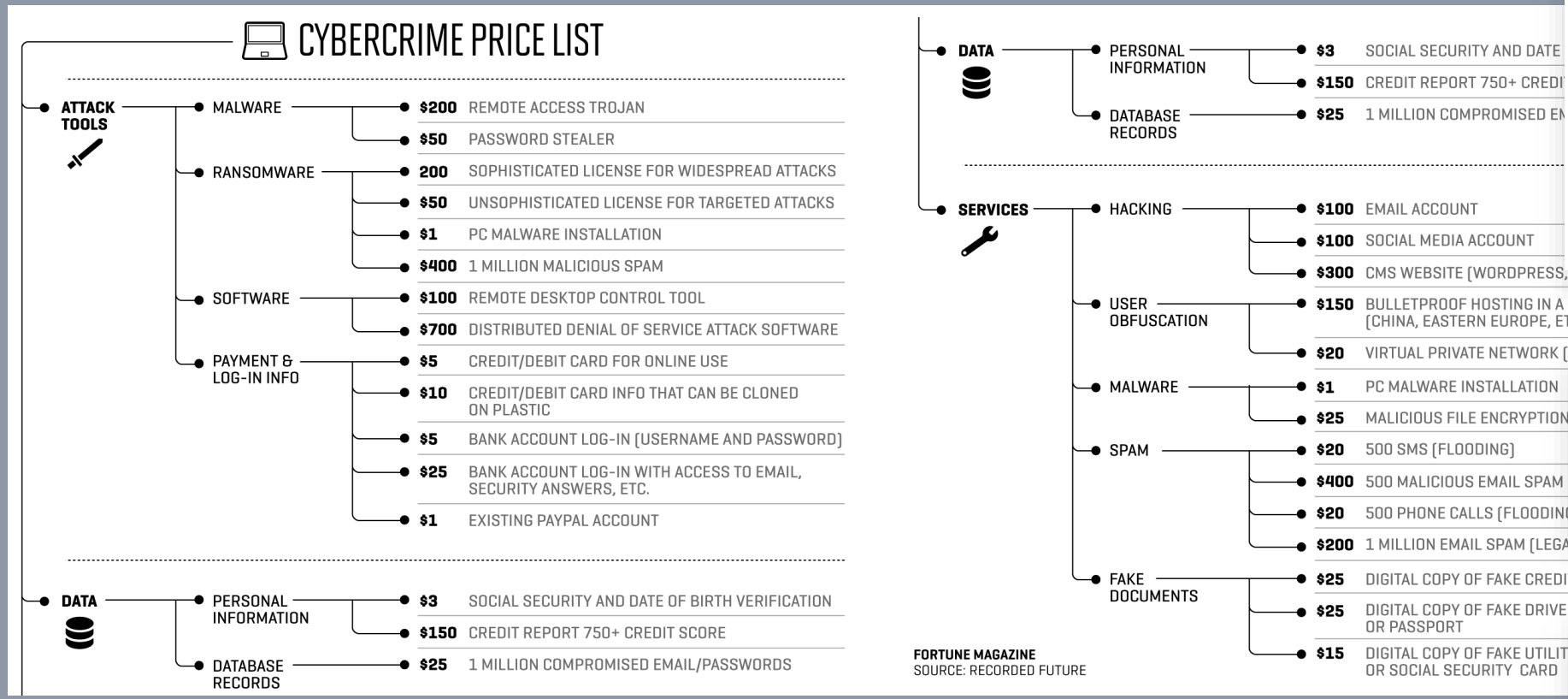
Angriffsmotivation, Vorgehensweise und Folgen

Motivation	Vorgehensweise	Auswirkung	Folgen
Produktpiraterie Verdrängung	Stiller Angreifer; Cyber-Kill-Chain: Initiale Infektion, Reconnaissance, Lateral Movement bis Data Exfiltration, gewinnorientierte, professionelle Vorgehenswesie	Datenverlust von Forschungsergebnissen, Kalkulationen, Kundendaten, Produktionsverfahren, Rezepturen	Verlust von Aufträgen, Rückgang von Marktanteilen, Verlust des Innovationsvorsprungs
Sabotage	1) Kollateralschaden: Kein zielgerichteter Angriff, Unternehmen wird Opfer eines „allgemeinen Angriffs“ 2) Zielgerichteter Angriff mit individuell zugeschnittener Malware, Exploits, Social Engineering etc.	Ausfall/Störung von unternehmenskritischen Prozessen (Produktion / Logistik / e-Commerce)	Großer unmittelbarer Schaden Weitere mittelbare Schaden: Rufverlust, Kundenabwanderung zu Marktbegleitern, etc.
Phishing & CEO-Fraud	Zielgerichtete (oder allgemeine) Phishing-Attacke CEO-Fraud: Zielgerichtete Kampagne mit Social-Engineering-Komponenten, Infiltration, etc.	Überweisung ins Nirwana Verlust von Passwörtern, Unternehmensdaten, Installation von Malware, etc.	Direkter Verlust Rufschaden erster Schritt einer anderen Attacke
Erpressung / Ransomware	Massenhafte Verschlüsselung von Servern, Clients und anderen Systemen	Produktionsstillstand Große Produktivitätseinbußen	Großer betriebswirtschaftlicher Schaden, Rufschädigung

Wie sehen die Geschäftsmodelle der Hacker aus?

Cybercrime as a Service – Cyber Crime Price List

Einkaufspreise Ihrer Gegner



Offering	Price per 1,000 Downloads
Australia (AU)	US$300-550
Great Britain (UK)	US$220-300
Italy (IT)	US$200-350
New Zealand (NZ)	US$200-250
Spain (ES), Germany (DE), or France (FR)	US$170-250
United States (US)	US$100-150
Global mix	US$12-15
European mix	US$80
Russia (RU)	US$100

Offering	Price
Basic statistical crypter	US$10-30
Stub crypter with various add-ons	US$30-80
Polymorphic crypter	US$100+
Joiner	US$10-30

Offering	Price
1-day DDoS service	US$30-70
1-hour DDoS service	US$10
1-week DDoS service	US$150
1-month DDoS service	US$1,200

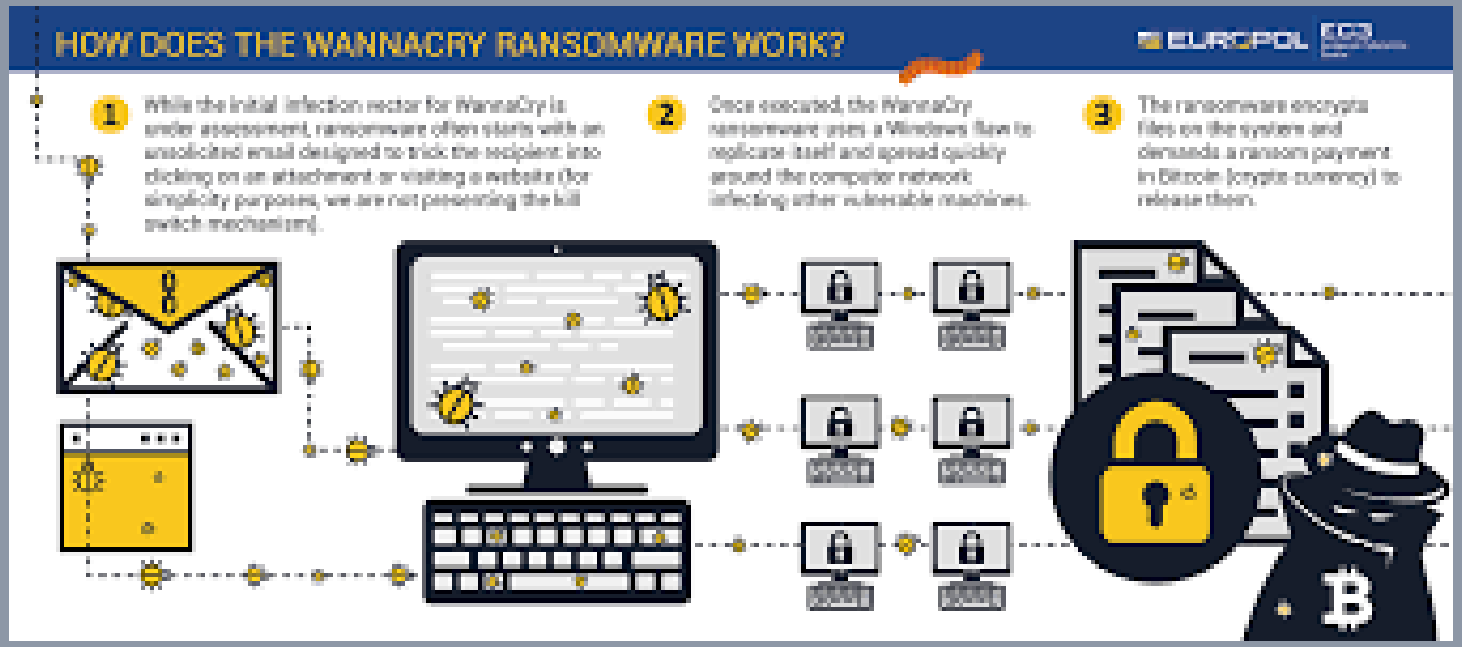
Quellen:
https://resources.infosecinstitute.com/cybercrime-and-the-underground-market/#gref
https://fortune.com/2017/10/25/cybercrime-spyware-marketplace/

CyberSecurity manufaktur

Wie läuft ein Hackerangriff ab (Erfahrungsbericht)

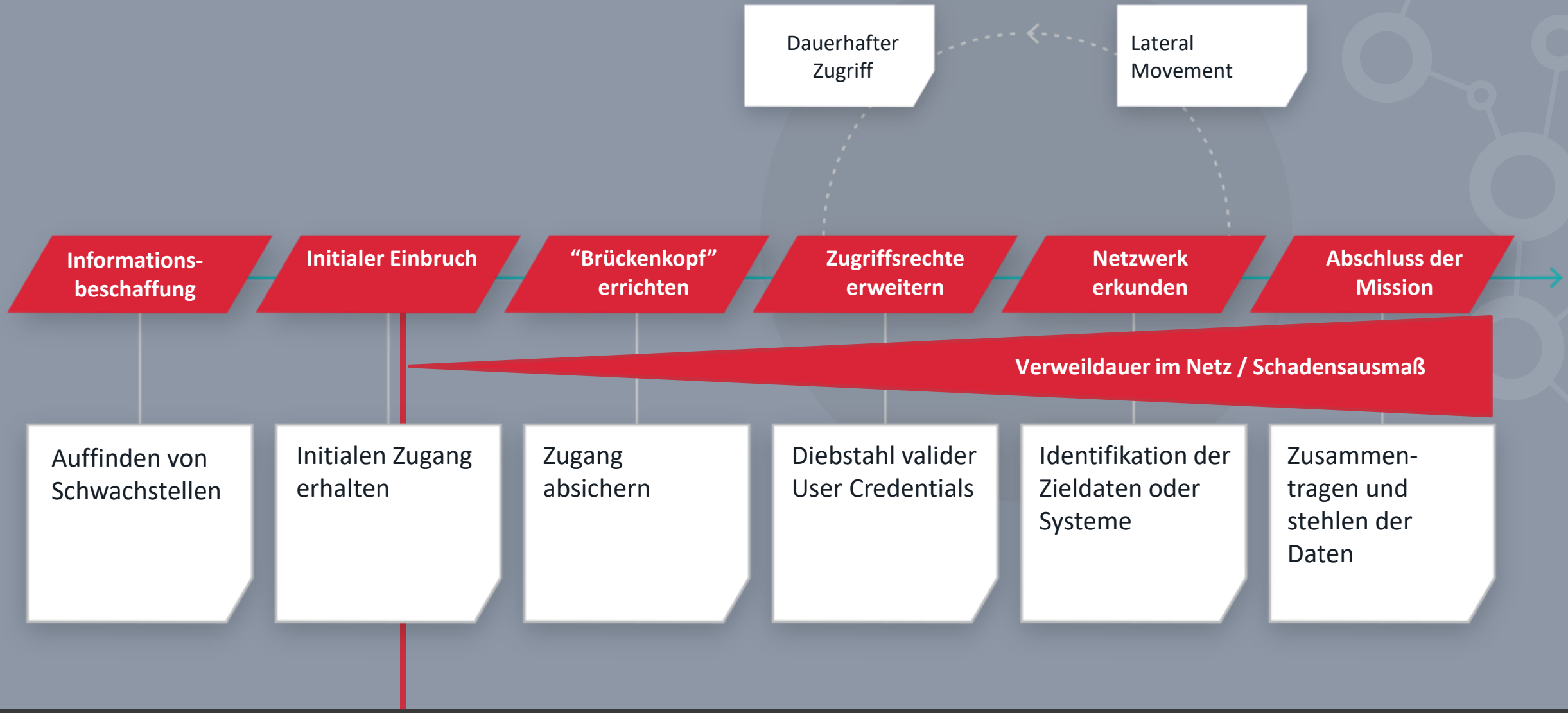
Erfahrungen aus den letzten Angriffen:

Ein Hackerangriff oder ein Virenbefall ist nicht planbar, die Verbreitungswege sind nicht vorhersehbar und vor allem darf man sich niemals in Sicherheit wägen.



CyberSecurity manufaktur

Typischer Verlauf eines Cyber-Angriffs



CyberSecurity manufaktur

Wie läuft ein Hackerangriff ab (Erfahrungsbericht)

Namhafte Unternehmen werden Opfer von Hackerangriffen wie zum Beispiel Petya und WannaCry oder anderen Schadcode Varianten

z.B. Hafen von Rotterdamm

z.B. Milka Lörrach

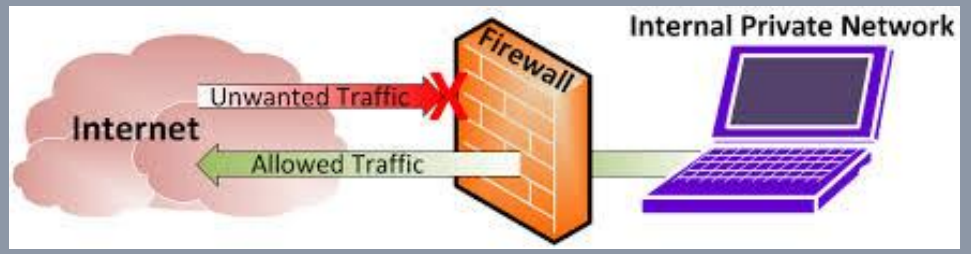
z.B. Continental

……

Gemeinsamkeiten !!!!!! mehrwöchige / monatelanger Unternehmensstillstand

Wie läuft ein Hackerangriff ab (Erfahrungsbericht)

Herausforderungen an die Organisation und die Technik



Menschen + Organisation + Technik

Diese 3 Komponenten sind die Erfolgsfaktoren für eine erfolgreiche Cyberattacke

Wie läuft ein Hackerangriff ab (Erfahrungsbericht)

Welche Wege nutzen Angreifer?

WELCHE WEGE NUTZTE ZUM BEISPIEL PETYA?

- Ungepatchte Windows Systeme (SMB Schwachstelle)
- Nutzung von Systemtools
- Ausspähung von Adminaccounts und Verbreitung mittels eines „Golden Tickets“
- Trusted WAN-Connections
- Systeme

Erfahrungen bei einem Cyberangriff?

IT-Systeme wurden innerhalb von Minuten verschlüsselt

- 365 Server in 12 Minuten während der Mittagspause
- Verschlüsselung der Storagesysteme
- Verschlüsselung Produktionssysteme
- Verschlüsselung von Backupsystemen
- Verschlüsselung von Security Systemen
- Kompromittierung des Aktive Direktory mit einem Golden Ticket
- Löschung von Backupdaten

Was sind die Auswirkungen in meine Unternehmen?

- Kein Zugriff auf Daten möglich
- Internetkommunikation über Wochen und Monate nicht möglich bis die Lokalisierung des Schadcodes und die Infektionsanalyse abgeschlossen ist. (Ist der Schadcode im gesamten Netzwerk eliminiert)
- Standorte und Fachbereiche sind nicht mehr funktionsfähig. (Keine Produktion, keine Logsitik, Standorte sind nicht mehr erreichbar)
- Chaotische Zustände im Support, hunderte Supportanfragen sofern noch möglich.

Was sind die Auswirkungen in meine Unternehmen?

Technische Auswirkungen

Es sind Systeme befallen womit Sie nie gerechnet haben!!!!

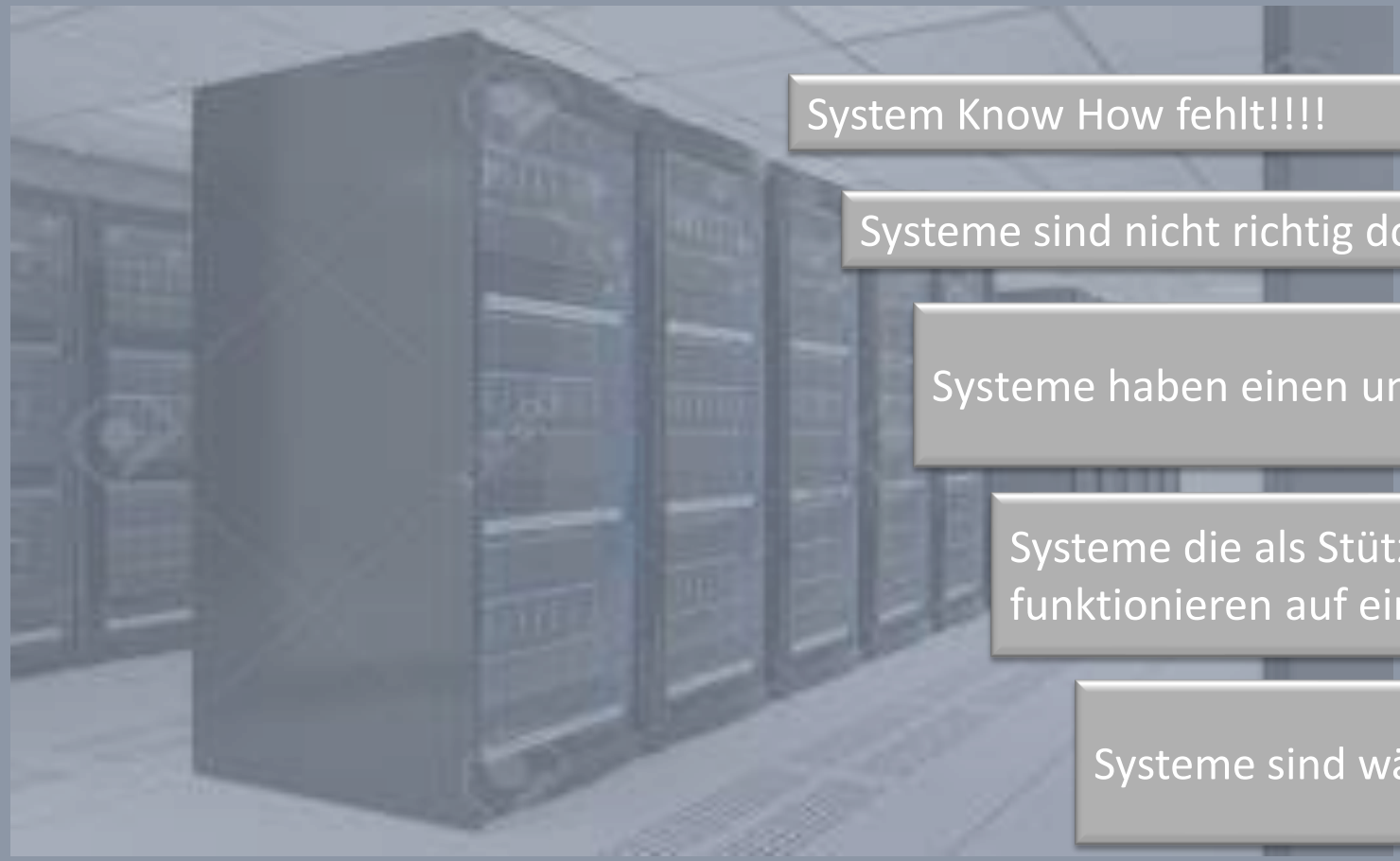
Keine funktionierende AD Services!

Keine funktionierende DNS / DHCP Services!

- Backup – Sind wir überhaupt in der Lage die verschlüsselten Daten zu restoren?
- Sind die Daten verschlüsselt? Thema Backup2Disk
- Was ist mit meinem Cloudbackup?

Was sind die Auswirkungen in meine Unternehmen?

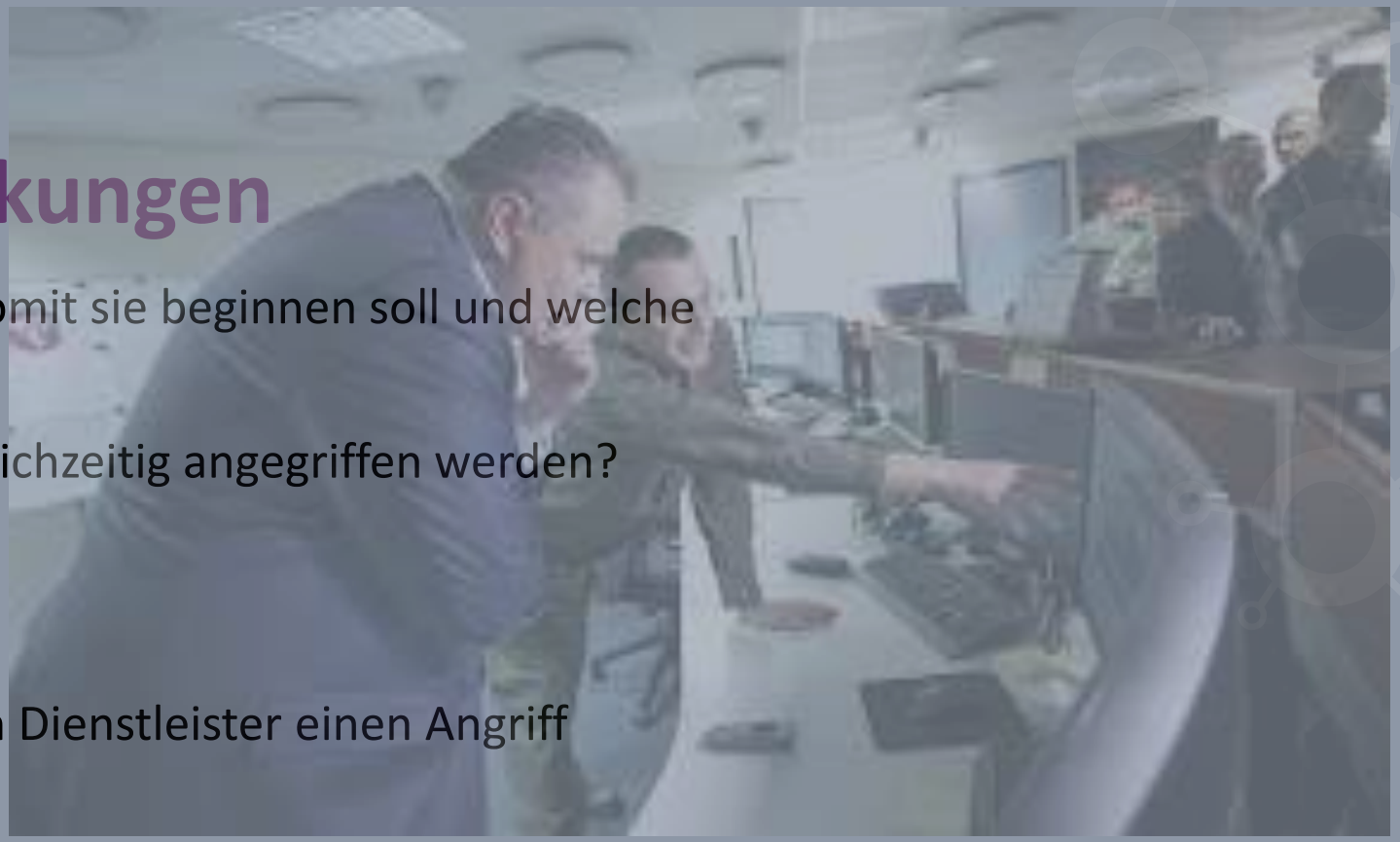
Prozessuale Auswirkungen



- System Know How fehlt!!!!
- Systeme sind nicht richtig dokumentiert!
- Systeme haben einen undefinierbaren Zustand
- Systeme die als Stütze ihres Wideranlaufprozesses dienen funktionieren auf einmal nicht mehr!
- Systeme sind während der Migration in neue Technologien!

Kundenerfahrung

Organisatorische Auswirkungen



Die IT-Abteilung weiß im Angriffsfall nicht, womit sie beginnen soll und welche Schritte als erstes NOTWENDIG sind.

1. Was tun Sie wenn 350 Serversysteme gleichzeitig angegriffen werden?
2. Haben sie einen Plan?
3. Was schützen sie zuerst?
4. Wie verhalten Sie sich, wenn Sie oder ein Dienstleister einen Angriff erkennen?

Kundenerfahrung

Organisatorische Auswirkungen

Achtung Geschäftsleitung

Fehlende Managementvorgaben erschweren die strukturierten Maßnahmen für den Wiederanlauf.

IT-Risiko – und Notfallmanagement

Im Cyberangriffsfall werden die fehlenden Entscheidungen und organisationsschwächen des Unternehmens im Krisenfall sichtbar.

Fragen während eines Cyberangriffs?

Welche Prozesse und Systeme sind betroffen?

I. **Wo fange ich an**
II. **Wer entscheidet was**
III. **Was schalte ich ab**
IV. **Welche Verbindungen muss ich trennen**
V. **Welche Systeme müssen als erstes wiederhergestellt werden**

KENNEN SIE DIE RISIKEN IHRER GESCHÄFTSPROZESSE - WAS HABEN GESCHÄFTSPROZESSE MIT SICHERHEIT ZU TUN?

BEWERTUNGENSSCHEMA

Kundenerfahrung

Organisatorische Regelungen

- Welche Geschäftsprozesse müssen als erste wieder laufen?
- Welche IT-Services sind notwendig?
- Welche IT-Infrastruktur ist notwendig?
- Welche externe und interne Spezialisten sind notwendig?
- Sind die Spezialisten verfügbar und erreichbar?

Strategien entwickeln

- Schützen sie nur ihre wichtigen Werte!
- Schützen sie ihre Geschäftsprozesse
- Beschäftigen sie sich mit den Angreifern!
- Gelegenheit macht Diebe. Bieten sie ihren Angreifern keine Angriffsflächen!

Unsere strukturierte Vorgehensweise

CyberSecurity Lifecycle

1) Analyse der Geschäftsprozesse mit den spezifischen Cyberrisiken

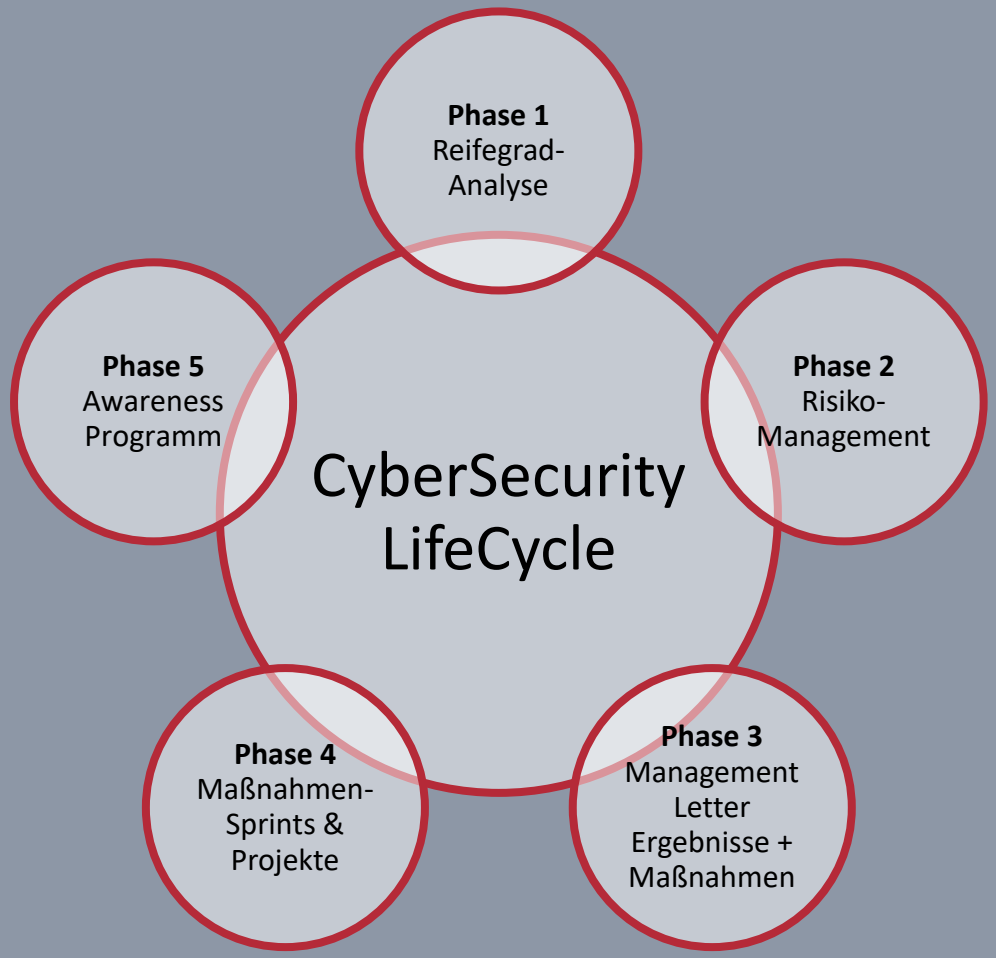
2) Analyse der aktuellen CyberSecurity-Maßnahmen und deren Wirksamkeit
   - Policies & Richtlinien
   - Technologien
   - Prozesse, insbesondere Cyber-Krisen-Prozesse

3) Priorisierte Handlungsempfehlungen für Prozesse und Technologien

4) Unterstützung bei der Umsetzung
   - Prävention: Technologien und Beratung zur Verhinderung von Cyberangriffen
   - Detektion: Technologien und Services zur Erkennung
   - Reaktion: Services zur Reaktion auf Angriffe / Krisen-Management

CyberSecurity LifeCycle

Vorsprung durch intelligente Prozesse



Schritt 1:
Erstellung einer Matrix aller bekannten Kern-Geschäftsprozesse. Ermittlung der Verfügbarkeitsanforderungen und Kritikalitätsbewertung

Schritt 2:
Ergänzung der Kritikalität - und Verfügbarkeitsanforderungen durch die Fachbereiche, sowie Ergänzung wichtiger Subprozesse.

Schritt 3:
Erstellung Dokumentation: Prozesslandkarte; Kritikalitätsmatrix; Wiederanlaufprioritätenliste, Ressourcenübersicht der kritischen Geschäftsprozesse.

Schritt 4:
Risikoanalyse – Liste aller möglichen Risiken und Ergebnisse der Risikobewertung.

Schritt 5:
Verknüpfung der Geschäftsprozesse mit den notwendigen IT-Services und IT-Systemen.

CyberSecurity manufaktur

Ihre direkten Ansprechpartner

Dipl. Betriebswirt
Martin Braun
Geschäftsführer, Gründer
martin.braun@cybersecurity-manufaktur.de
+49 151 16135560

AVAYA | Experiences That Matter

Vielen Dank für Ihre Aufmerksamkeit!

www.avaya.com