# INCIDENT MANAGEMENT
# für die Optimierung der Cybersicherheit

# Inhaltsverzeichnis

Alen Avdic

- Alen Avdic
- Gründer und CEO von Tectag
- Beginn 2015
- Leitung der Sparten Cybersecurity & Software Development

# Nationale Standorte


- Dortmund (Headquarter)
- Frankfurt am Main
- Stuttgart

# Internationale Standorte


- Deutschland
- Marokko
- Vereinigtes Königreich

# Einleitung

## Was ist Cyber Security Incident Management?

Cybersecurity Incident Management bezieht sich auf den Prozess der effektiven Handhabung und Reaktion auf Cybersicherheitsvorfälle innerhalb einer Organisation. Es umfasst den systematischen Ansatz zur Identifizierung, Analyse, Eindämmung, Ausrottung und Wiederherstellung von Sicherheitsvorfällen, um deren Auswirkungen auf die Systeme, Daten und den Betrieb der Organisation zu minimieren.

# Einleitung

## Zielsetzung der Präsentation

- Anregungen für eigenes IM
- Tools für Aufbau eines IM
- Cyber Security Awareness
- Sensibilität für Risiken steigern

# Einleitung

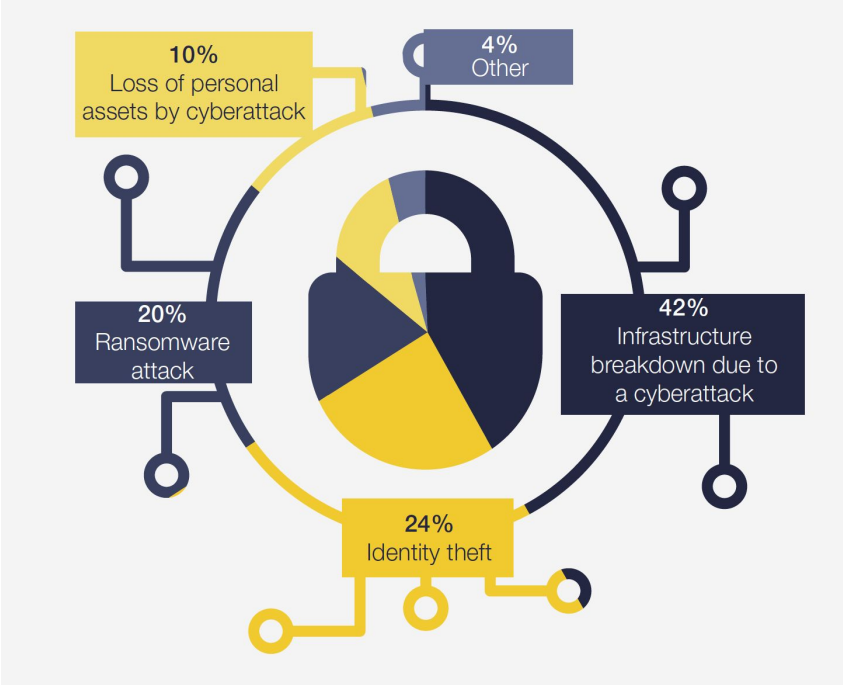
## Bedeutung der Cybersicherheit für Organisationen

*“Es gibt zwei Arten von Unternehmen: Solche, die schon gehackt wurden, und solche, die es noch werden.”*

*- Robert Mueller, 2012, ehem. Direktor FBI*

# Einleitung

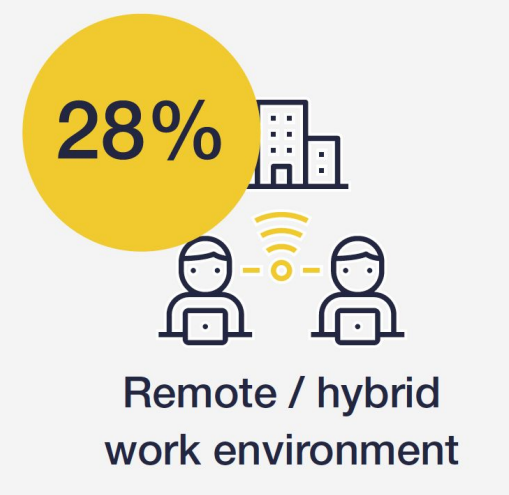
Was sind die persönlichen Cybersicherheitsbedenken von Führungskräften?

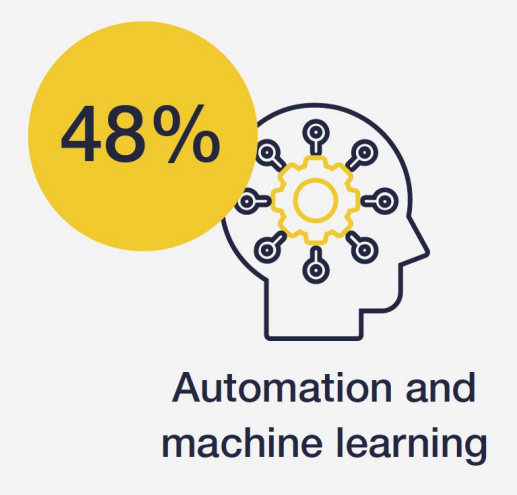



Source: World Economic Forum, Global Security Outlook 2022

# Einleitung

Was dürfte in den nächsten zwei Jahren den größten Einfluss auf die Transformation der Cybersicherheit haben?




Source: World Economic Forum, Global Security Outlook 2022

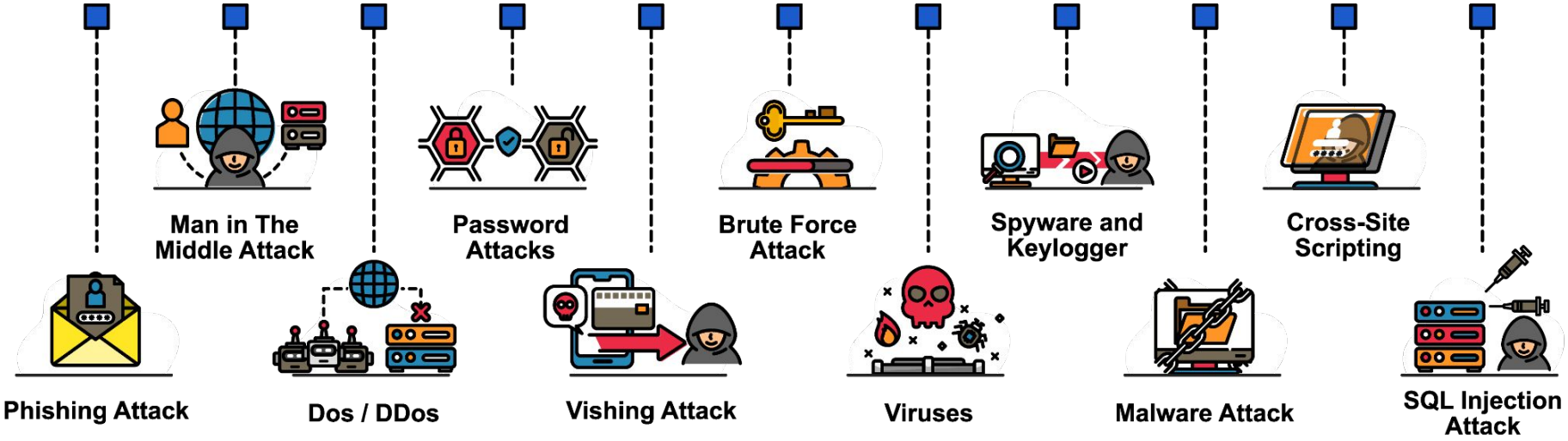
# Einleitung

## Daten und Fakten

- Die weltweiten Kosten durch Cyberkriminalität werden 2023 auf ca. 8,15 Billionen US Dollar geschätzt, 2025 auf 10,29 Billionen US-Dollar (1)
- Unternehmen benötigen im Schnitt 2-4 Wochen für das Erkennen eines Angriffs. (2)

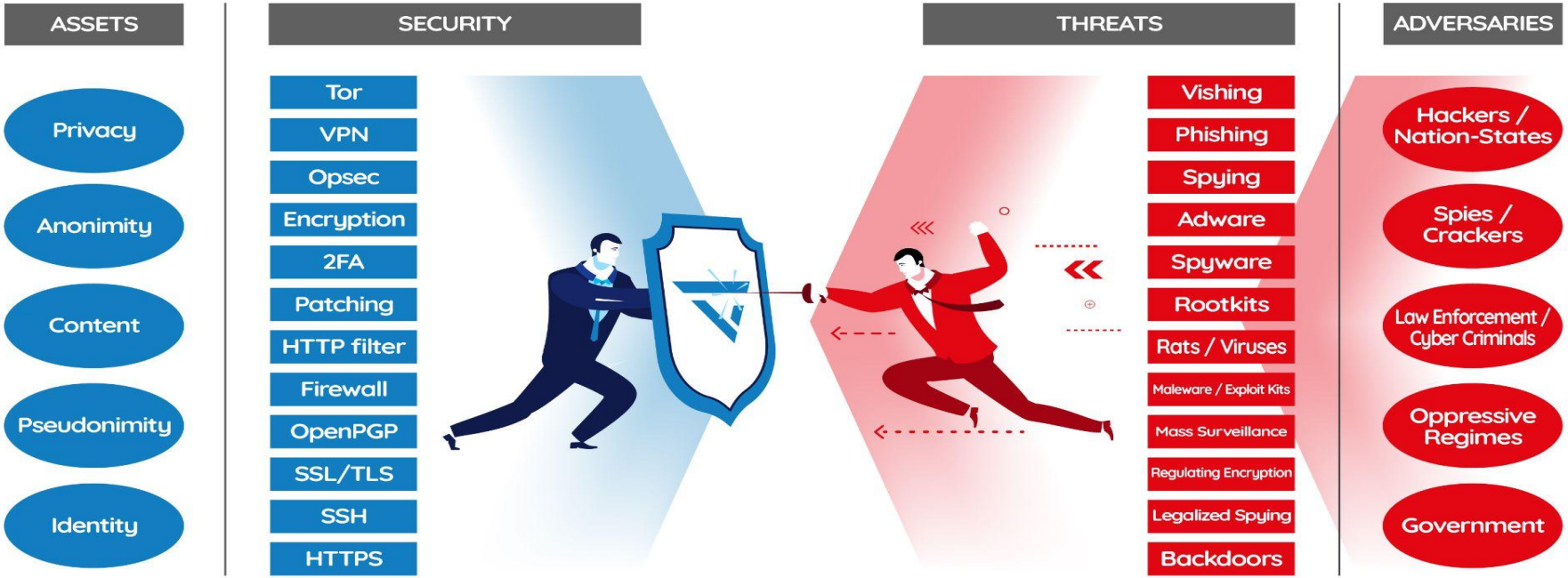
1) https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
2) IBM Security Incident Responder Study, 2022, IBM.

# Überblick: Cyberbedrohungen



# Assets-Security-Threats-Adversaries

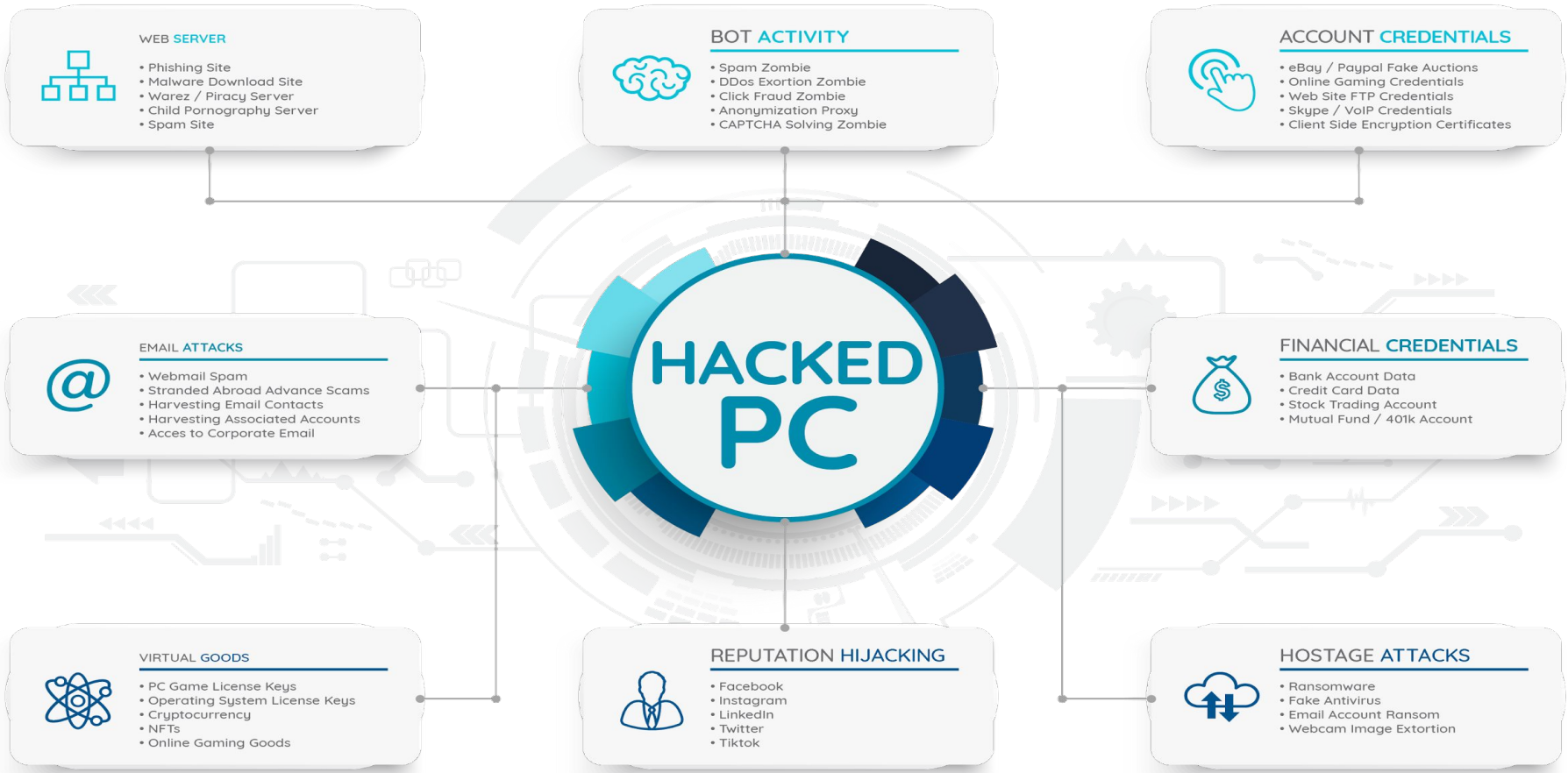
tectag



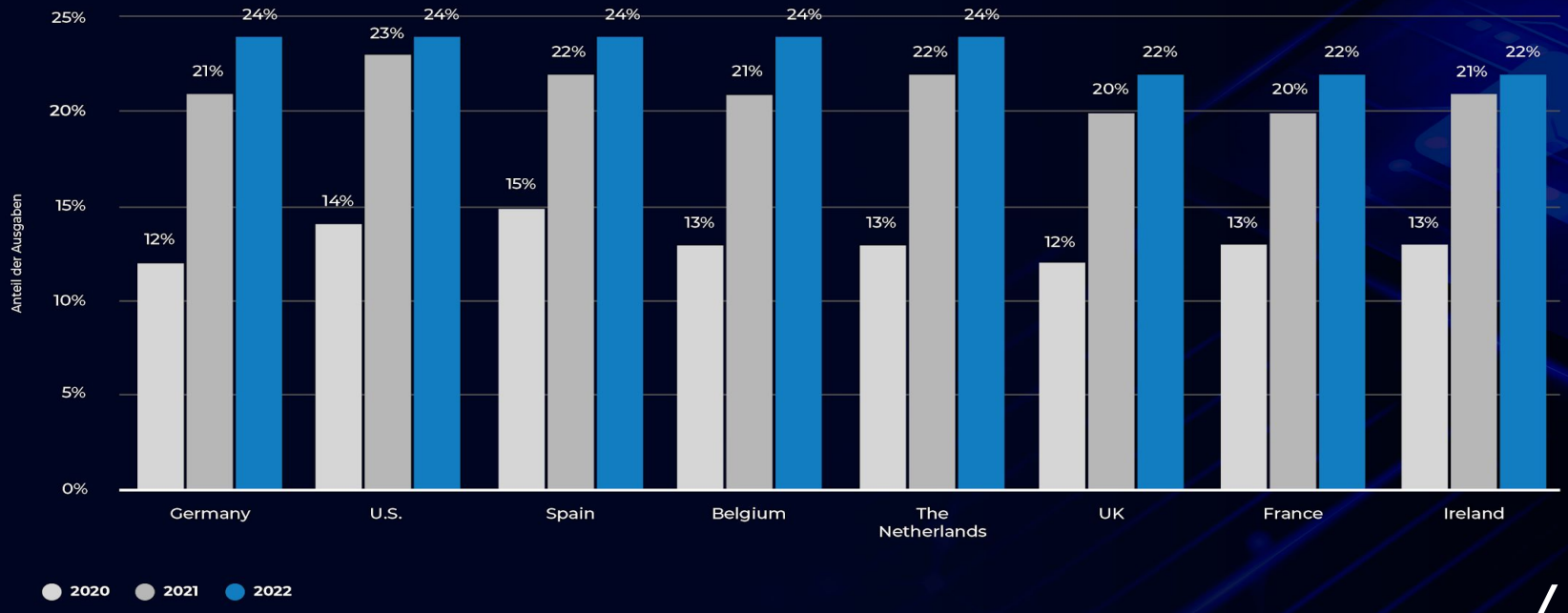
# Value of a hacked Email

tectag

# Value of a hacked PC



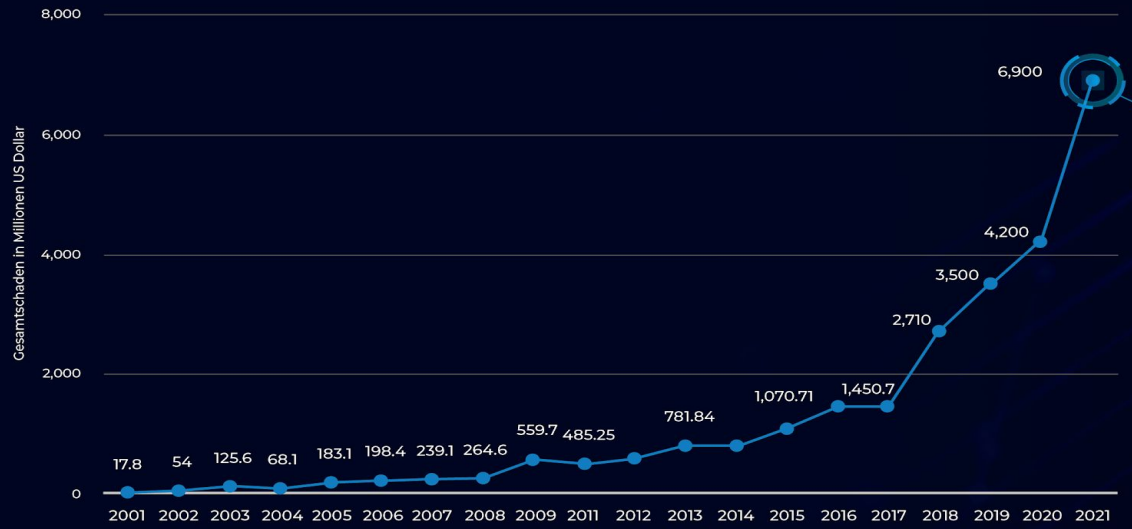
## Cybersicherheit als Prozentsatz der IT-Ausgaben in den USA und europäischen Unternehmen von 2020 bis 2022, nach Ländern



# Zahlen, die Unternehmen schaden

**Höhe des finanziellen Schadens, der von 2001 bis 2021 durch gemeldete Cyberkriminalität beim IC3 verursacht wurde**

Kosten in Millionen US Dollar




Dieses Diagramm zeigt wie **teuer Cybersecurity Attacken sind** und dass die Zahlen weiter steigen

# Incidents aus der Praxis

## Beispiel: Aluminium-Produzent

### Daten

- Mehrere Standorte
- International
- Über 2000 Mitarbeiter
- Produziert und veredelt Aluminium

### Vorfall

- Server lahmgelegt
- Website offline
- Interne Tools offline
- Datenbanken beschädigt

### Ursache

- Mitarbeiter lädt infizierte Datei herunter
- Netzwerke nicht separiert
- Benutzer mit der Rolle “Super-Admin” haben Zugriff auf alles

# Incidents aus der Praxis

## Lösung

- Segmentierung des Netzwerks
- Firewall neu eingerichtet und konfiguriert
- Sandbox implementiert
- Datenbank-Bindungen neu gesetzt und Daten gesichert
- Training der Mitarbeiter (Security Awareness)

# Incidents aus der Praxis

## Beispiel: Autohaus

### Daten

- Lokales Autohaus in Dortmund
- Handelt mit Neu- und Gebrauchtwagen verschiedener Hersteller
- Eigener Server vorhanden

### Vorfall

- Rechnungen wurden manipuliert
- Geld wurde an ein falsches Konto überwiesen
- 70.000 € Schaden

### Ursache

- PDF-Rechnungen wurden auf eigenem Server unverschlüsselt gespeichert
- Server war schlecht gesichert
- Besucher-Wifi läuft rund um die Uhr

# Incidents aus der Praxis

## Lösung

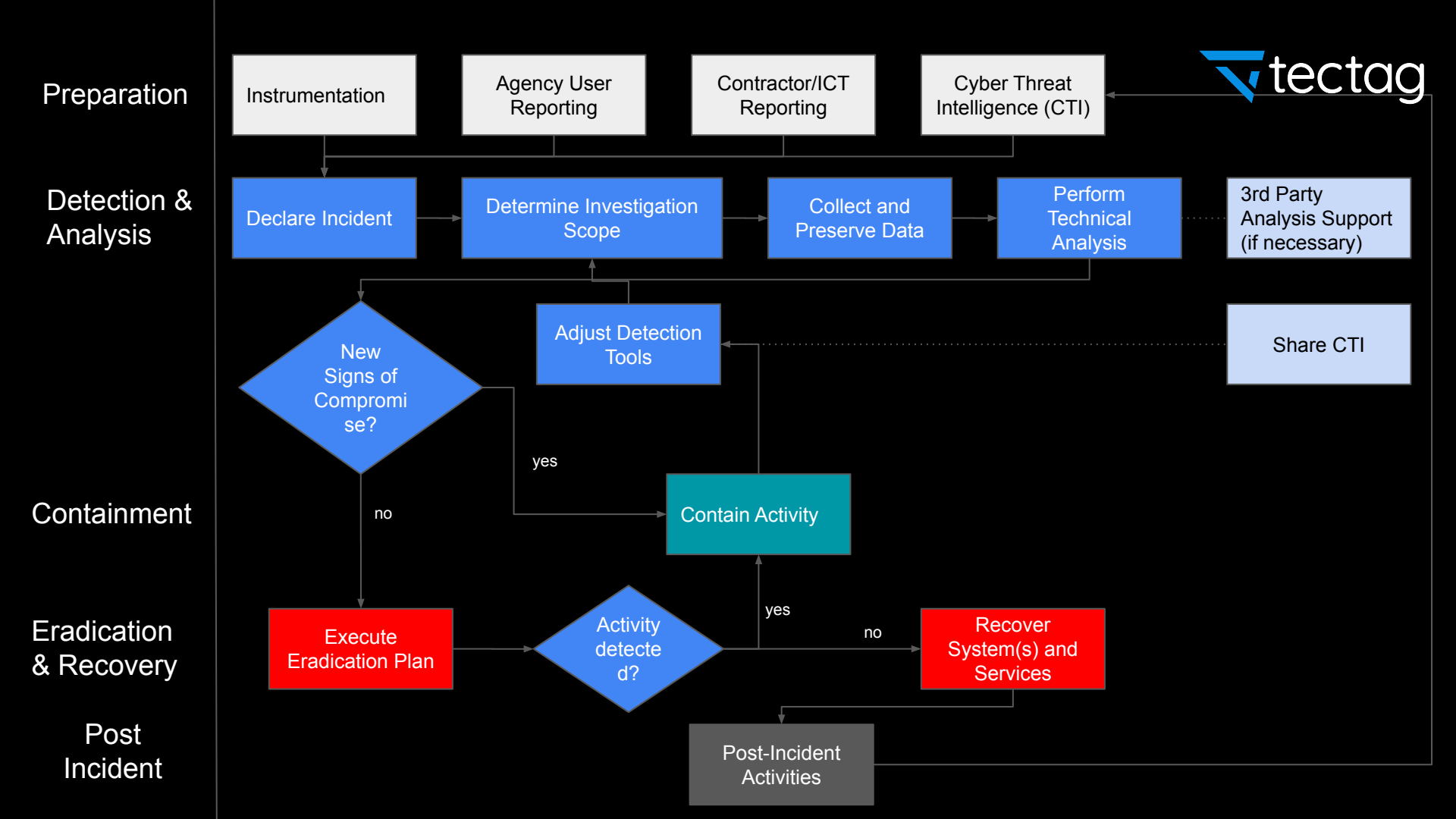
- Alle Rechnungen geprüft und mit Lieferanten abgeglichen
- Rechnungsbearbeitung in die Cloud ausgelagert, aufgrund fehlender Kapazitäten zur Selbst-Administration
- Wifi nur zu Besuchszeiten aktiviert

# Incident Management

*“Companies are not judged by whether they were hit by a cyberattack, but by the character of their response.”*

*(Unternehmen werden nicht danach beurteilt, ob sie von einem Cyberangriff getroffen wurden, sondern nach der Art ihrer Reaktion)*

*- Robert Silvers, 2021, US Department of Homeland Security*


Preparation
Detection & Analysis
Containment
Eradication & Recovery
Post Incident
Instrumentation
Agency User Reporting
Contractor/ICT Reporting
Cyber Threat Intelligence (CTI)
tectag
Declare Incident
Determine Investigation Scope
Collect and Preserve Data
Perform Technical Analysis
3rd Party Analysis Support (if necessary)
New Signs of Compromise?
Adjust Detection Tools
Share CTI
yes
no
Contain Activity
Execute Eradication Plan
Activity detected?
yes
no
Recover System(s) and Services
Post-Incident Activities

# Incident Management

## Wie baue ich ein IM auf?

Auf den folgenden Seiten werden alle Anforderungen für ein grundlegendes Security Incident Management aufgeführt.

# Incident Management

## Preparation - Ziele

1. Ausrüstung, Tools, etc. bereithalten und updaten
2. Dokumentation bereithalten mit Angaben zu Prozessen, Richtlinien und involvierten Personen sowie Lieferanten
3. Regelmäßiges Training des involvierten Personals

# Incident Management

## Preparation - Richtlinien & Prozesse

1. Hierarchie im Unternehmen & Team
2. Eskalation und interdisziplinäres Reporting
3. Notfallpläne bereithalten
4. Zusätzliche Personalreserven für Notfälle aus eigenem Unternehmen oder von Lieferanten
5. Berichterstattung und Interaktion an und mit Behörden sowie evt. Strafverfolgung klären

# Incident Management

## Preparation - Infrastructure Auditing

1. Aktuelle Datenbanken der eigenen Infrastruktur pflegen (inkl. alle Endpunkte, Netzwerke, Cloud-Netzwerke, sonst. Drittanbieter-Ressourcen)
2. Alle Netzwerkressourcen überwachen (Antivirus, Firewall, etc.)
3. Anforderungen an Logging implementieren (Wo wird gespeichert? Was wird gespeichert? Wer hat Zugriff?)

# Incident Management

## Preparation - Cyber Threat Intelligence

1. Informations-Feeds konstant auf News & Bedrohungen überwachen (Internetportale, Wettbewerb, Behörden, eigene Intelligence, etc.)
2. Aggregierung von Daten, auch aus anderen Unternehmen
3. Forensic Solutions einbinden

# Incident Management

## Preparation - Geschultes Personal

1. Sicherstellung, dass das Personal einen ausreichenden Wissensstand in der Kette hat
2. Regelmäßige Tests der Prozesse auf menschliche Schwachstellen
3. “Security Awareness Trainings”

# Incident Management

## Preparation - Daten teilen

1. Security Intelligence mit allen zugehörigen Unternehmen, Abteilungen, Shareholdern, etc. teilen
2. Koordinierung und Berichterstattung an BSI
3. Sicherheitsfreigaben beim Informationsaustausch beachten

# Incident Management

## Detection & Analysis - Vorfall erklären und Umfang klären

1. Notwendige Personen und Behörden sowie Unternehmen informieren, gemäß Reporting-Prozessen
2. Umfang der nötigen Untersuchung bestimmen

# Incident Management

## Detection & Analysis - Daten sammeln & schützen

1. Überprüfung, Kategorisierung, Priorisierung, Schadensbegrenzung, Berichterstattung und Zuordnung von Vorfällen
2. Daten aus allen Quellen sammeln
3. Daten forensisch sichern (Sowohl Festplatten, Cloud-Speicher als auch Arbeitsspeicher)
4. Alle Daten den Incident Response Team zur Verfügung stellen

# Incident Management

## Detection & Analysis - Technische Analyse durchführen

1. Den Vorfall verstehen (Vergleich mit Normalzustand, Anomalien erkennen)
2. Ursachen erkennen
3. Mögliche Angriffe beobachten, erkennen, vergleichen, etc.
4. Konstante Überwachung des Analyseprozesses

# Incident Management

## Containment

Ziel in diesem Schritt ist, weiteren Schaden zu verhindern und den oder die Angreifer am weiteren Voranschreiten zu hindern. In dieser Phase muss der angegriffene Bereich auch vom Rest des Netzwerks abgeschottet werden.

# Incident Management

## Containment - Grundlegende Überlegungen

1. Hier sollte innerhalb des Unternehmens kommuniziert werden, wie lange die Abschottung des infizierten / attackierten Bereichs dauern wird
2. Bedenke: Die Eindämmung könnte die Sicherung von Daten verhindern oder verlangsamen
3. Falls möglich: Eindämmung, ohne dass der Angreifer hiervon erfährt

# Incident Management

## Containment - Maßnahmen

1. Betroffene Bereich und Netzwerksegmente vom Rest des Netzwerks trennen
2. Forensische Datenträgerabbildungen (Images) sichern
3. Alle Zugangsdaten von Nutzern ändern
4. Alle Secret Keys sowie API-Schlüssel ändern
5. Unbefugten Zugriff verhindern
6. Evtl. Sandbox nutzen

# Incident Management

## Detection & Analysis - Analyse-Werkzeuge anpassen

1. Während der gesamten Analyse müssen die genutzten Tools stets angepasst werden, um weitere Verbreitung im Netzwerk zu unterbinden
2. Evt. Tools austauschen, je nach Bedarf

# Incident Management

## Eradication

1. In dieser Phase wichtig: Geduld
2. Alles genau beobachten um Rückstände des Angriffs komplett zu entfernen
3. Backups und Images neu installieren, falls möglich
4. Komprimierte Dateien mit sauberen Versionen ersetzen
5. Passwörter von kompromittierten Accounts zurücksetzen

# Incident Management

## Recovery

1. Sicherstellung, dass alle vorherigen Maßnahmen erfolgreich waren
2. Netzwerke wieder einschalten, verbinden und eingedämmte Sektoren wieder verknüpfen
3. Sicherheitsmaßnahmen verstärken
4. Alle neuen Systeme und Maßnahmen testen

Ziel: Der Wiederherstellungsplan wurde erfolgreich durchgeführt und alle Rückstände des Angriffs sollten entfernt sein!

# Incident Management

## Post-Incident Activities

Ziel in diesem Schritt ist, den Vorfall zu dokumentieren, Behörden und sonstige interessierte Parteien zu informieren, um ähnliche Vorfälle in Zukunft zu vermeiden.

# Incident Management

## Post-Incident Activities - Maßnahmen

1. Penetrationstests durchführen
2. Die zuvor attackierten Netzwerksegmente weiterhin beobachten
3. Evtl. Fehler korrigieren
4. Retrospektive durchführen & Mitarbeiter schulen
5. Lücken schließen im Incident Response Plan
6. Tools, Prozesse, Richtlinien verbessern.

# Defense in Depth


## PREVENT

### Measures against known Threats

- Blacklist
- Reputation systems
- Threat intelligence
- Signature based network and endpoint methods
- Intrusion Prevention Systems (IPS)
- Virtual keyboards
- URL-blockers
- Content filtering
- Host based firewalls
- Parental controls
- File and disk encryption

### Measures against unknown Threats

- Exploit prevention
- Sandboxes
- Isolation & compartmentalitation
- Application white listing
- Application control Konown good
- Host based firewalls
- File and disk encryption
- Secure deletion
- Access Control List (ACL)
- User Access Control (UAC)
- Software Restriction Policies (SRP)

## DETECT

### Measures against known Threats

- Anti-Virus
- Intrusion DetectionSystems (IDS)
- Web Application Firewall (WAF)
- OSquery
- Credit monitoring
- Vulnerability scanning
- Traffic monitoring
- Anti-spam
- EDR technology

### Measures against unknown Threats

- Behavioral analysis
- Anomaly detection
- Binary Analysis
- Machine learning
- Heuristic detection
- OSquery
- EDR Technology
- CabaryPi
- Canary Tokens

## RECOVER

### Possible measures

- Anti-virus
- Automated response & remediation
- Backup
- Snapshot
- Re-imaging
- Roll back
- EDR technology

# Hilfreiche Ressourcen

- Cyber Security Incident & Vulnerability Response Playbooks, CISA, November 2021
- Computer Security Incident Handling Guide, NIST 800-61 rev2, August 2012
- https://attack.mitre.org/ (Auflistung von möglichen Angriffen)
- https://www.tectag.group


# Vielen Dank für Ihre Aufmerksamkeit!

www.tectag.group