CYBER SECURITY

Stephan Halder

Hamburg, 21. November 2018

1. CYBER FACTS

GOVERNANCE SURVEY CYBERSECURITY

3 von 4 Board Mitgliedern halten Ihre Cybersecurity für anfällig

72 Prozent bestätigen dass das Board im letzten Jahr wesentlich stärker involviert wurde

Über die Hälfte empfindet dass Produkte nicht cyber secure entwickelt werden

Nur 1 von 3 entwickelt oder implementiert Intelligence für Threats

Fast 3 von 4 nehmen externe Unterstützung in Anspruch um Cyber Risk Anforderungen zu erfüllen

Nur 1 von 4 geht von einer guten Cybersecurity der Zulieferer aus

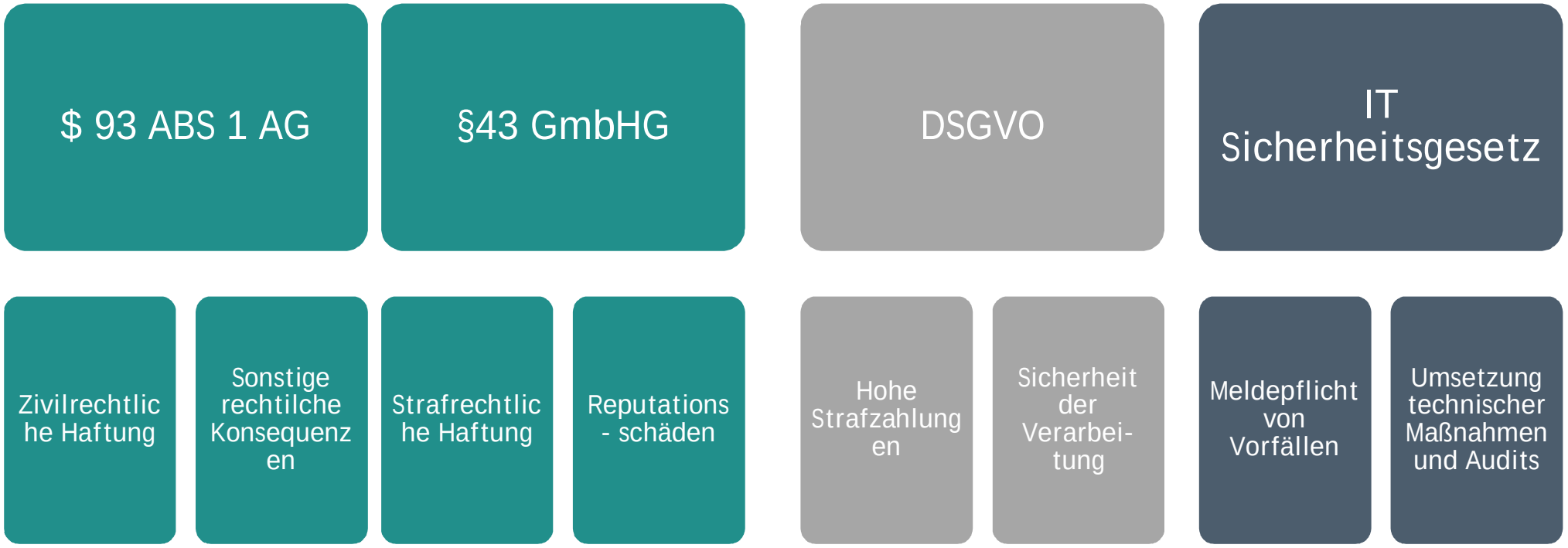
Fast 3 von 4 bestätigen dass im letzten Jahr das Cybersecurity Investment erhöht wurde

Nur 30% planen eine einheitliche Cybersecurity Strategy über deren Ecosystem

32 Prozent werden mindestens einmal im Quartal über Cyberthemen informiert

8 von 10 Unternehmen haben einen Incident Response Plan um möglichen Cyber Risks zu entsprechen

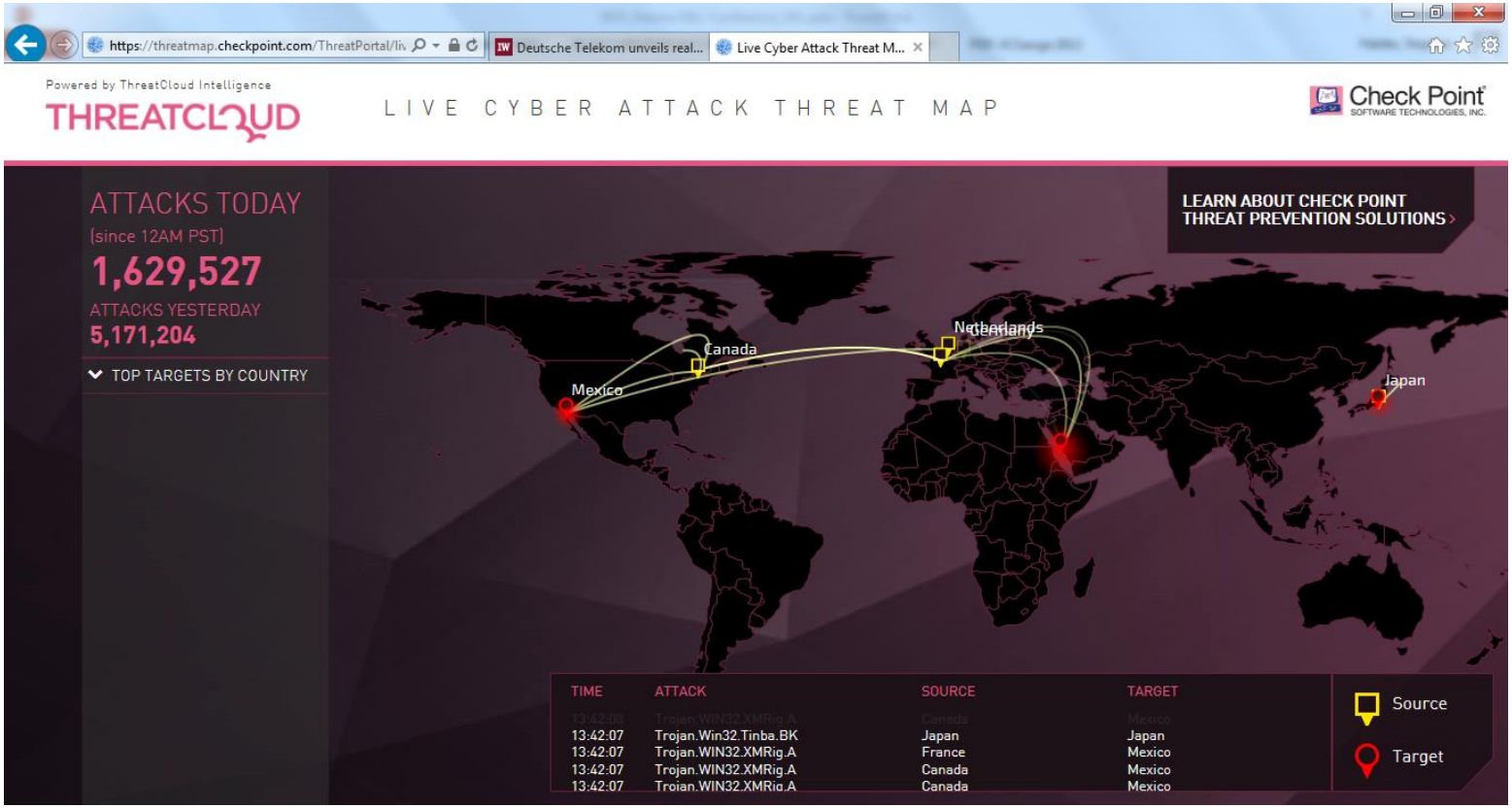
RECHTLICHER RAHMEN



ANGRIFFSVEKTOREN FÜR CYBERCRIME

Vektor	Beschreibung
Fake President	Auch bekannt als CEO Fraud. Über sog. Spear Phishing wird versucht gezielt Mitarbeiter zu täuschen und zur Transaktion von Geld zu bewegen
Ransomware	Verschlüsselung von Unternehmensdaten
Phishing	Über bspw. gefälschte Internetseiten oder Emails wird versucht Zugangsdaten der Targets zu erbeuten
DDoS	Internetservices der Targets werden mit Anfragen überfrachtet und gehen offline
Watering Hole	Targets werden auf manipulierte Internetseite gelockt und mit Malware infiziert
Supply Chain Exploit	Angriff von Lieferanten um über deren Produkte deren Kunden anzugreifen
Cryptocurrency Heists	Diebstahl von Crypto Coins von exchange markets oder ICO
Cryptojacking	Mailicious Crypto Mining durch Stehlen von Rechenpower

LIVE-MONITORING FÜR CYBER ATTACKS



2. MANAGING CYBER RISK

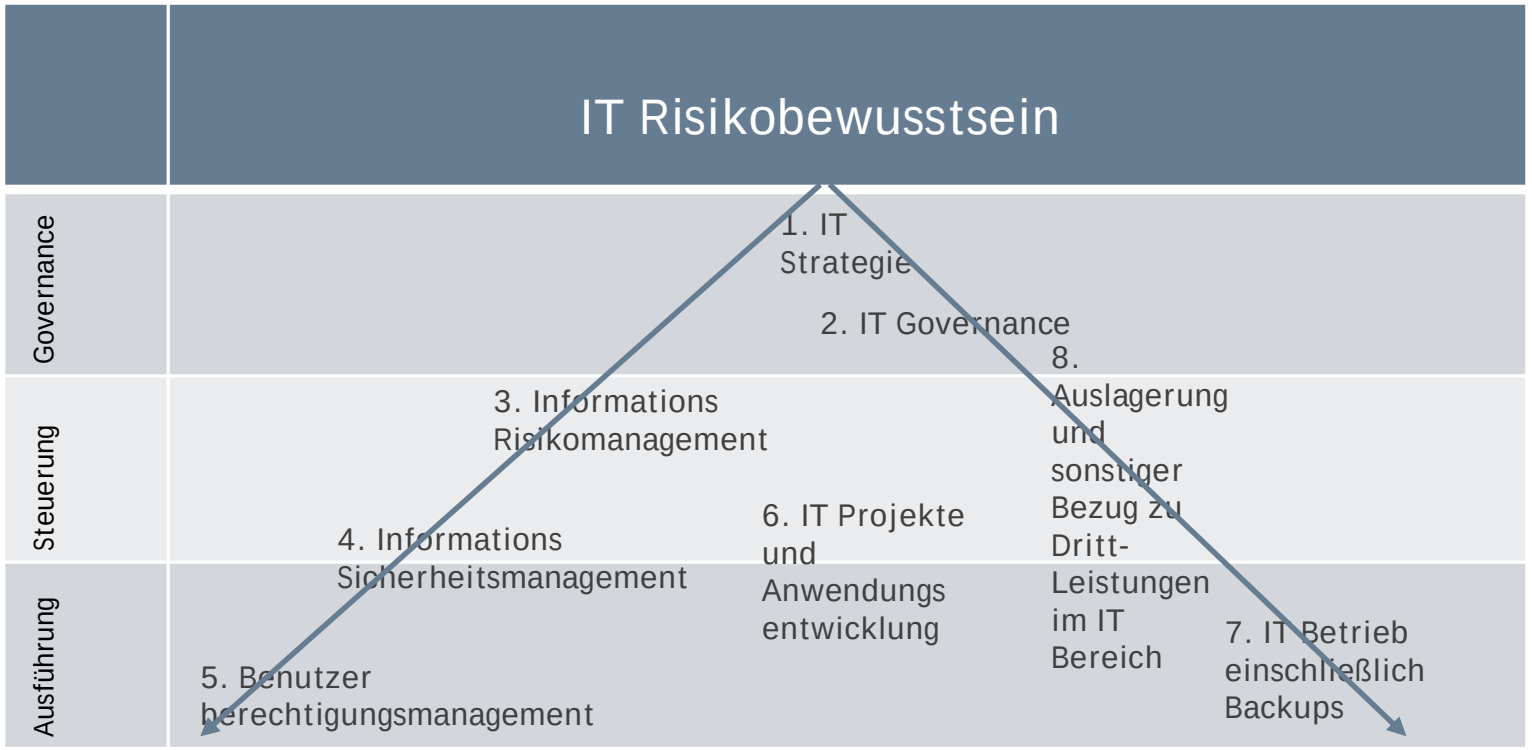
WIE SIEHT IHR RISK APPETITE AUS?

THEFT OR COMPROMISE OF SENSITIVE INFORMATION?

UNAVAILABLE SYSTEMS?

MANIPULATION OF SENSITIVE DATA?

RISK AWARENESS



SECURITY STRATEGY

Beschreibt die Abhängigkeiten zwischen Geschäftsmodell und der unterstützenden Cyber Security:

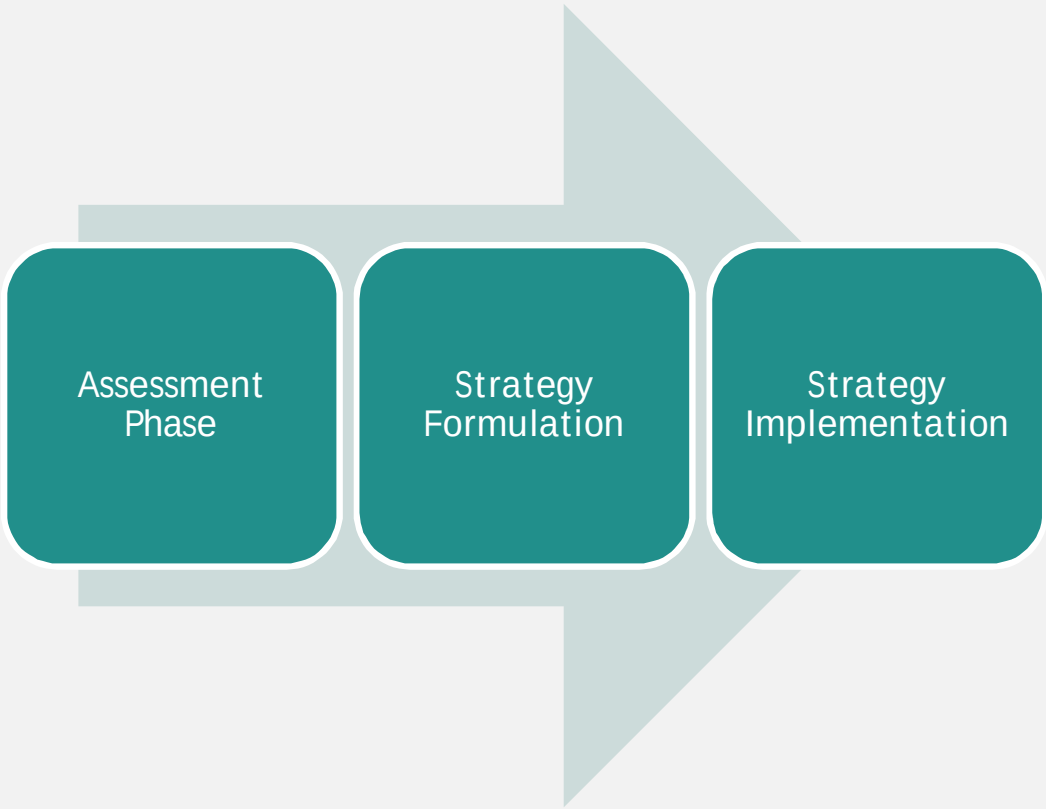
- Möglichkeiten Geschäftsziele zu erreichen
- Dynamische Anpassung

Definition der High-Level Security Principles vor dem Hintergrund der Geschäftsziele

Definiert die vorhandenen Sicherheitseinrichtungen aus technologischer, prozessualer oder governance Perspektive und deren unterstützenden Elemente wie HR und Finance.

Schützenswerte Unternehmenswerte

CYBERSECURITY MANAGEMENT FRAMEWORK CORE



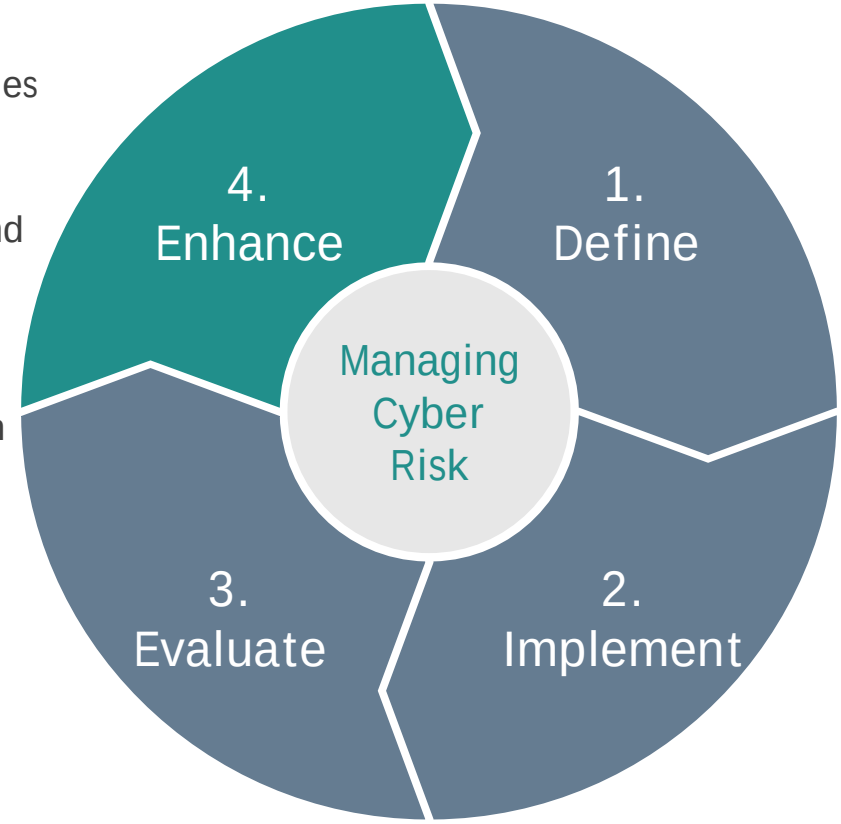
MANAGING CYBER RISK

Enhance

- Enhance Controls und Activities wo:
  - Neue Anforderungen bestehen (Risk, Policy and Implementation)
  - Neue Geschäftsprozesse bestehen
  - Bedrohungen sich ändern

Evaluate

- Assess Effectivity of:
  - implemented controls
  - Regulatory Requirments
  - Risk Level



Define

- Tone from the top
- Commitment zu:
  - Security Governance
  - Assess Risk Appetite
  - Align Security Strategy
  - Set Information Security Policies

Implement

- Implement Policy
- Assess Risk
- Apply Controls with Risk Appetite

3. CYBER SECURITY INCIDENT HANDLING

BEISPIELE FÜR CYBERSECURITY

Financial assets

Personal data

R&D

Contract negotiations

Sensitive transactions

Know-how

Classified information

Detailed information about buildings

Information about critical infrastructure

Business relations

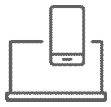
Information about political processes

Risk assessments and emergency plans

Marked strategies

Sensitive info about clients

Websites



PCs and mobile devices

E-mail

Operations

Ticketing system

Customer databases

SCADA

INFORMATIONSBASIS

Welche Daten benötigen besonderen Schutz …?

Wie oft werden Ihre Systeme angegriffen …?
Wie werden Ihre Systeme angegriffen …?

Wie lange dauert es bis Schwachstellen ausgenutzt werden …?

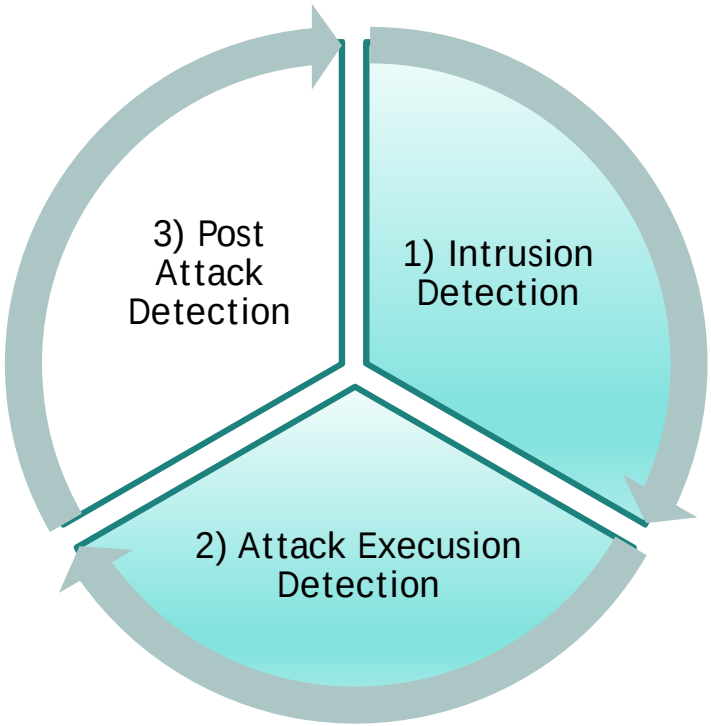
Welche Software ist whitegelistet …?
Welche wird aktiv bei Ihnen eingesetzt …?

Wie groß ist Ihr Risk Appetite …?
Welche Angriffsvektoren gibt es …?

Verfügen Sie über eine Threat Intelligence und kennen aktuelle Angriffsvektoren …?

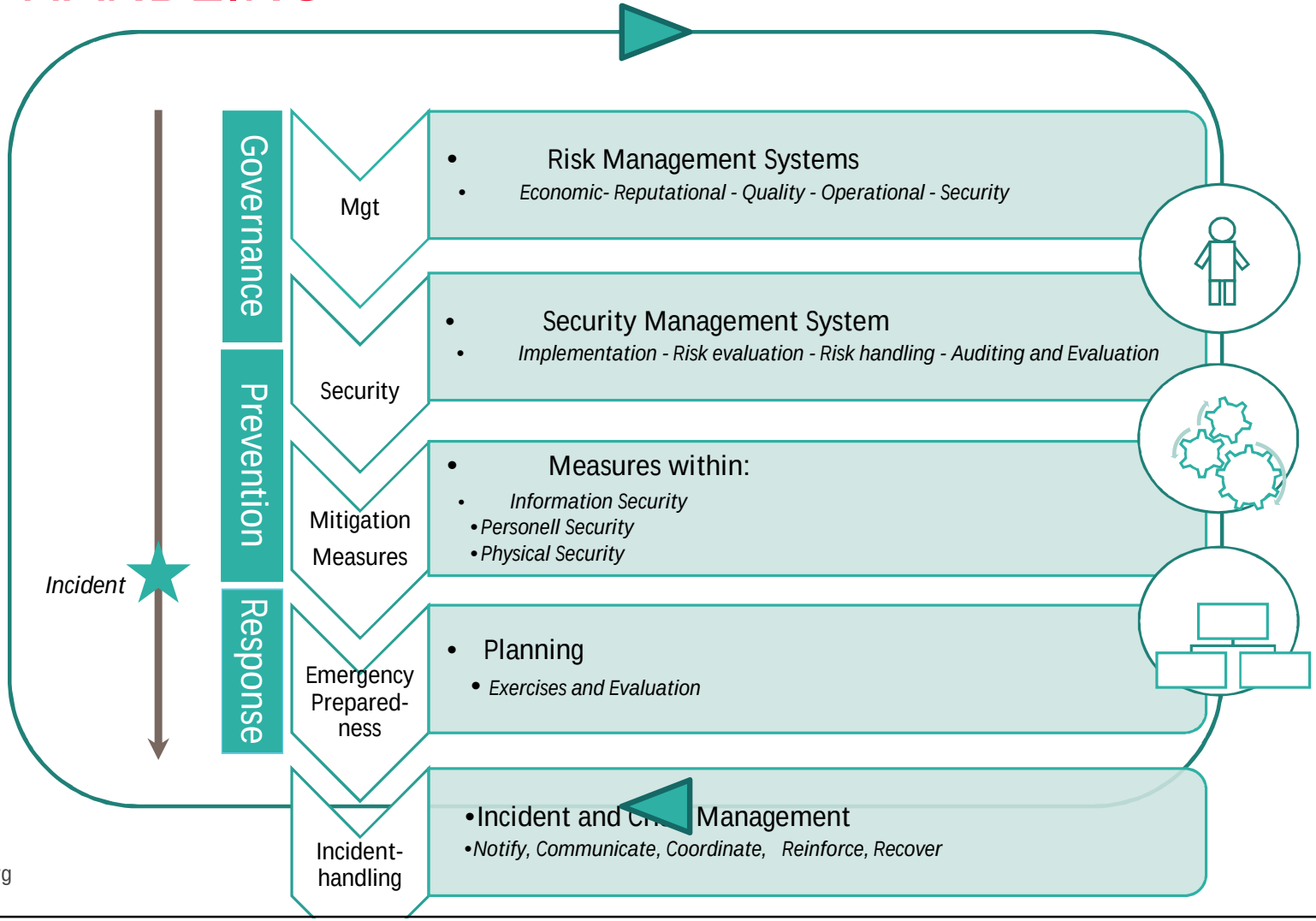
Wie ausgereift sind Ihre Prozesse und Systeme zur Cybersicherheit …?
Wie ausgereift ist die Cyber Sicherheit Ihrer Geschäftspartner …?

INCIDENT DETECTION PHASEN

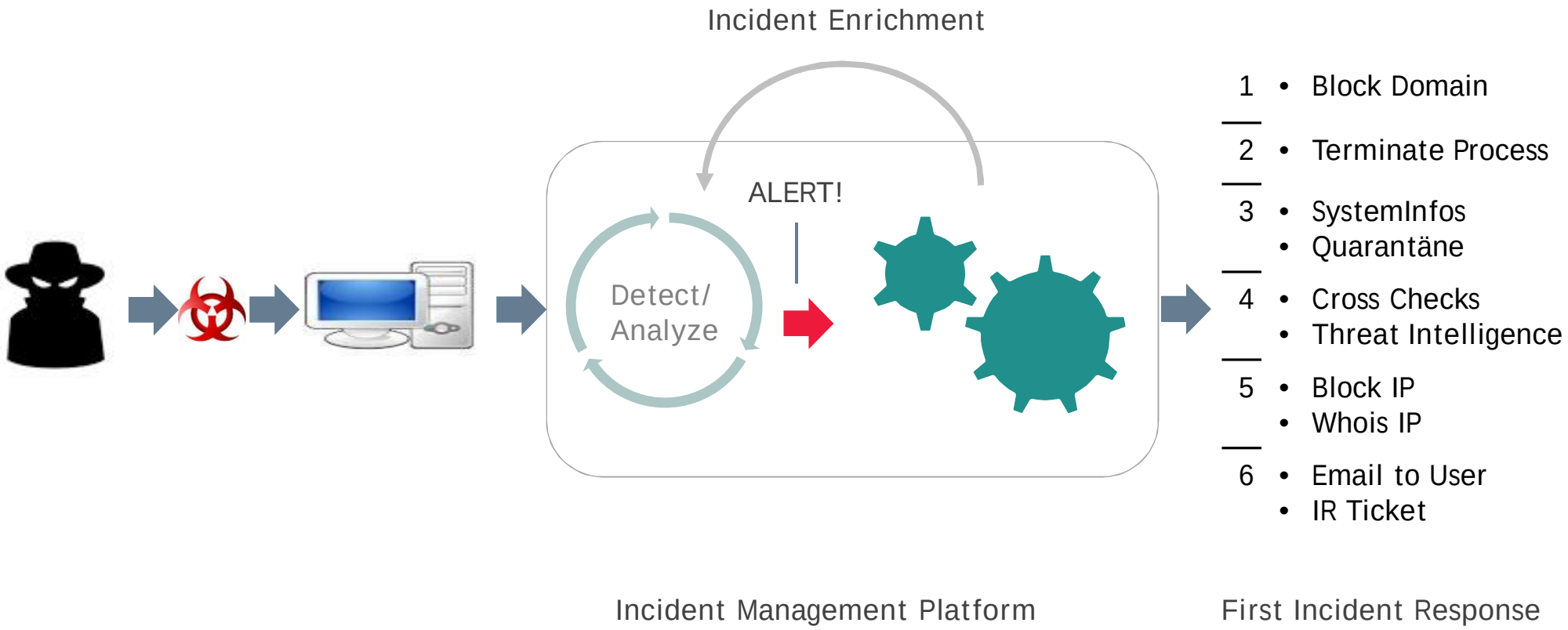


1	• Aufklärungs- und ExploitPhase eines Angriffs
2	• Privilegien-Eskalation (lateral Movement) • Konsolidierung gehackter Systeme • Umsetzung des Angriffsziels
3	• Suche nach Angriffsspuren auch außerhalb des Firmennetzes

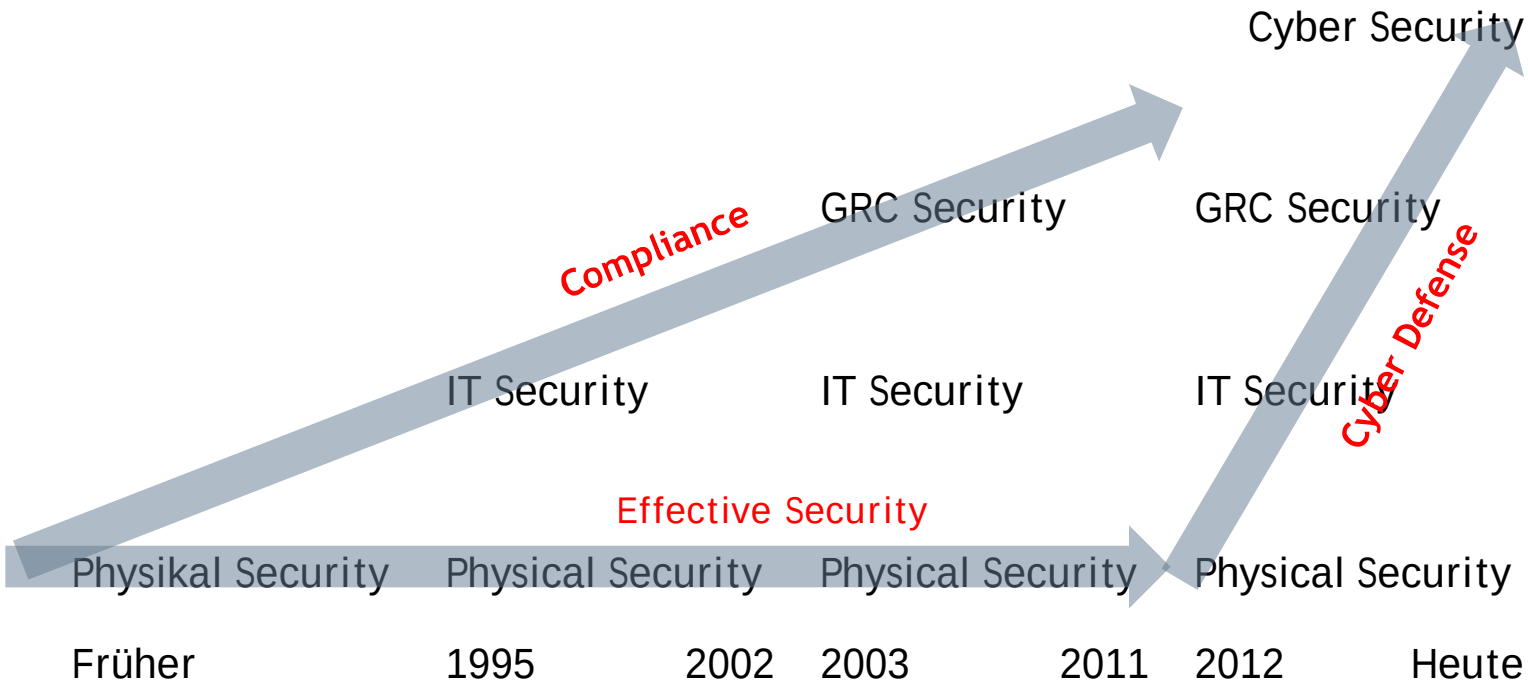
INCIDENT HANDLING



INCIDENT PROCESSING

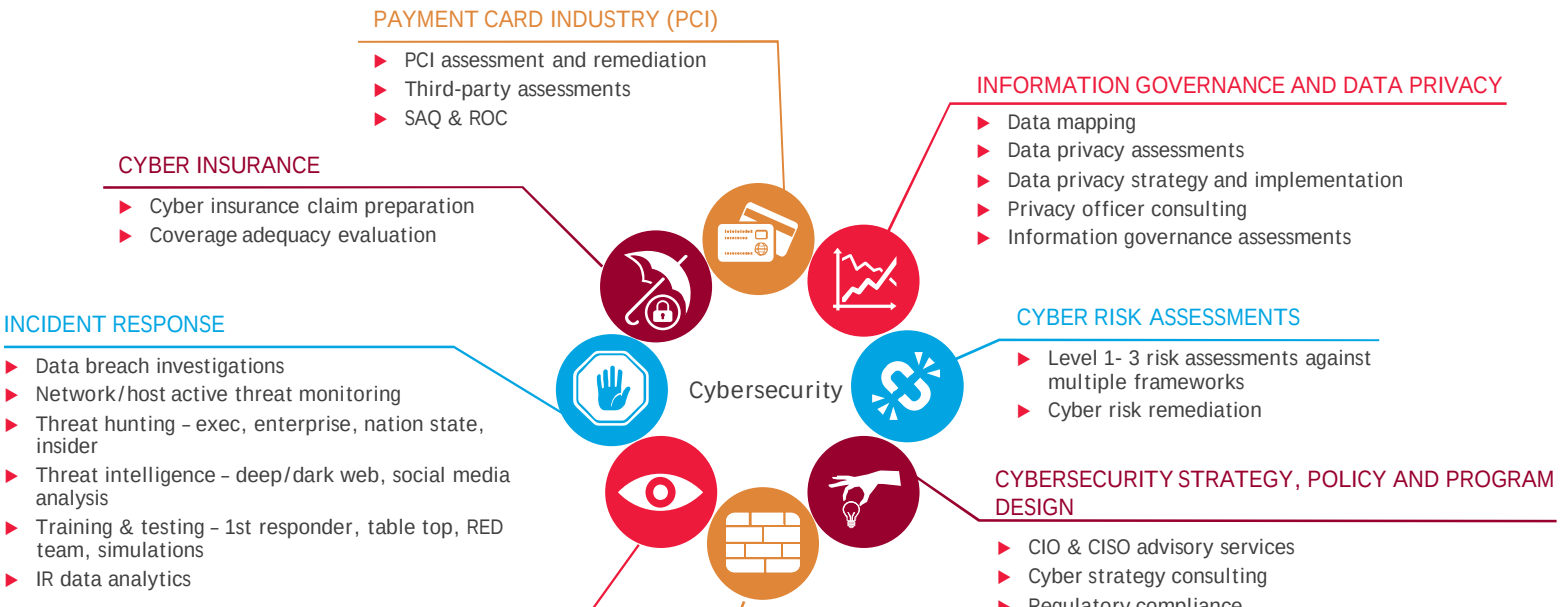


EVOLUTION OF CYBER SECURITY



4. CYBERSECURITY SERVICES

ÜBERSICHT CYBERSECURITY PRODUKTE UND SERVICES



PAYMENT CARD INDUSTRY (PCI)

- PCI assessment and remediation
- Third-party assessments
- SAQ & ROC

CYBER INSURANCE

- Cyber insurance claim preparation
- Coverage adequacy evaluation

INCIDENT RESPONSE

- Data breach investigations
- Network/host active threat monitoring
- Threat hunting – exec, enterprise, nation state, insider
- Threat intelligence – deep/dark web, social media analysis
- Training & testing – 1st responder, table top, RED team, simulations
- IR data analytics

CYBER THREAT INTELLIGENCE

- Dark web recon - flat rate low cost
- Dark web analysis
- Social media

INFORMATION GOVERNANCE AND DATA PRIVACY

- Data mapping
- Data privacy assessments
- Data privacy strategy and implementation
- Privacy officer consulting
- Information governance assessments

CYBER RISK ASSESSMENTS

- Level 1- 3 risk assessments against multiple frameworks
- Cyber risk remediation

CYBERSECURITY STRATEGY, POLICY AND PROGRAM DESIGN

- CIO & CISO advisory services
- Cyber strategy consulting
- Regulatory compliance
- Government relations consulting

INFORMATION MANAGEMENT & SECURITY-MANAGED SERVICES

- Network Operations Center (NOC)
- Security Operations Center (SOC)
- Penetration testing
- Vulnerability assessments
- Cybersecurity education, training, & simulations

FRAGEN?

KONTAKT

Stephan Halder
Senior Manager
Forensic, Risk & Compliance

BDO AG
Wirtschaftsprüfungsgesellschaft
Fuhlentwiete 12
20355 Hamburg

tel.: +49 40 30293 169
email: stephan.halder@bdo.de