CYBER THREAT INSIGHTS
ERFAHRUNGEN AUS DER WELT DER CYBER SECURITY

Stephan Halder
22. November 2018

1. CYBER MARKET

ANGRIFFE VERGANGENER JAHRE

Coinrail Coincheck	2018 wurden die Crypto Börsen Coincheck und Coinrail erfolgreich von Hackern angegriffen. Coincheck verliert 534 mio US Dollar, Coinrail 30 mio. Euro. Der Bitcoin Kurs fällt daraufhin z.T. um 500 US Dollar innerhalb einer Stunde
Youbit	2017 Nach dem 2. erfolgreichen Angriff und Diebstahl von Bitcoin im Dezember gibt die Krypto Börse auf und geht in die Insolvenz
Equifax	2017 wurde bekannt, dass Hacker von Mai bis Juli Zugriff auf Sozialversicherungsnummern, Geburtsdaten, Adressen, Führerscheinnummern oder Kreditkartennummern von 143 Mio Kunden hatten
Merck, Maersk, Rosneft	2017 einen Monat nach WannaCry infiziert Ransomware Petya/NotPetya zahlreiche Unternehmen. Besonders hart wird die Ukrainische Infrastruktur getroffen
Deutsche Telekom	2016 legt eine dilettantische Attacke auf die Telekom DSL-Router lahm. 900.000 Haushalte betroffen
Sony Pictures	2014 legt Angriff das gesamte Firmennetz lahm. Erster Fall in dem eine Firma wieder zu Papier und Fax greifen musste. Veröffentlichung vertraulicher Informationen führt zum Vertrauensverlust
Target	2013 erfolgt ein Angriff auf Kassensysteme der US Supermarktkette, Kreditkarten von 100 Mio. Kunden werden erbeutet. Eine Folge war ein deutlicher Umsatzrückgang
HBGary	2011 veröffentlicht Anonymous 10-tausende vertraulicher Dokumente (FBI, NSA)

BDO CYBERSECURITY IQ QUIZ

1 Is it True or False, that global spending on cybersecurity related hardware, software, and services is projected to hit $81.7 Billion in 2018 and climb to $105 Billion in 2020?

True

BDO CYBERSECURITY IQ QUIZ

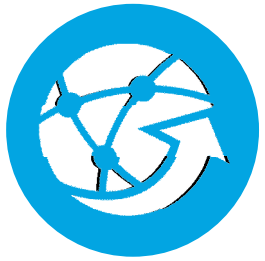
2 Is it True or False, that the average total cost of a data breach is $2 Million?

False

It is now $4.9 Million

BDO CYBERSECURITY IQ QUIZ

3 Is it True or False, that cyber liability continues to be a growing problem for all industries, especially financial services, healthcare, and energy companies?



True

BDO CYBERSECURITY IQ QUIZ

4 Is it True or False, that 15% of all multi-national companies with cyber liability coverage have experienced a data breach and submitted an insurance claim in the past two years?

False

It is actually over 30%

BDO CYBERSECURITY IQ QUIZ

5 Is it True or False, that the number of global cyber ransomware attacks have grown by over 700% in the past two years?

True

BDO CYBERSECURITY IQ QUIZ

6 Is it True or False, that the biggest cyber threats to your organization come from your current employees, former employees, and third-party suppliers?

True

BDO CYBERSECURITY IQ QUIZ

7 Is it True or False, that there is a significant increase in cyber attackers focused on spear- phishing attacks on company senior executives, based upon intelligence gathered via social media analysis?

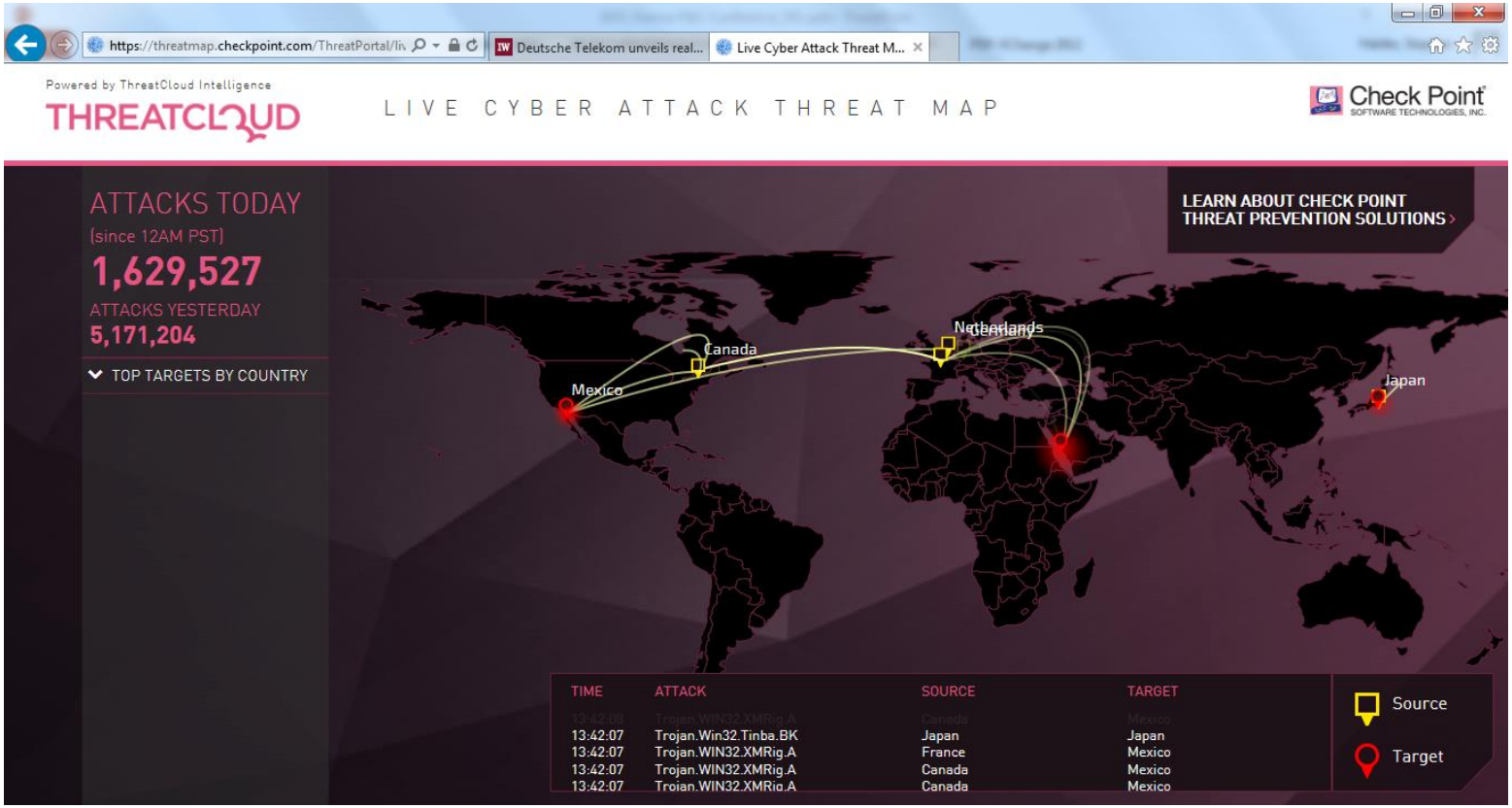
True

BDO CYBERSECURITY IQ QUIZ

8 Is it True or False, that a group of cyber attackers name Dragonfly have been targeting the global energy sector for numerous years using Trojan Horse software, ransomware, and spear phishing to gain information about energy facilities operating systems?

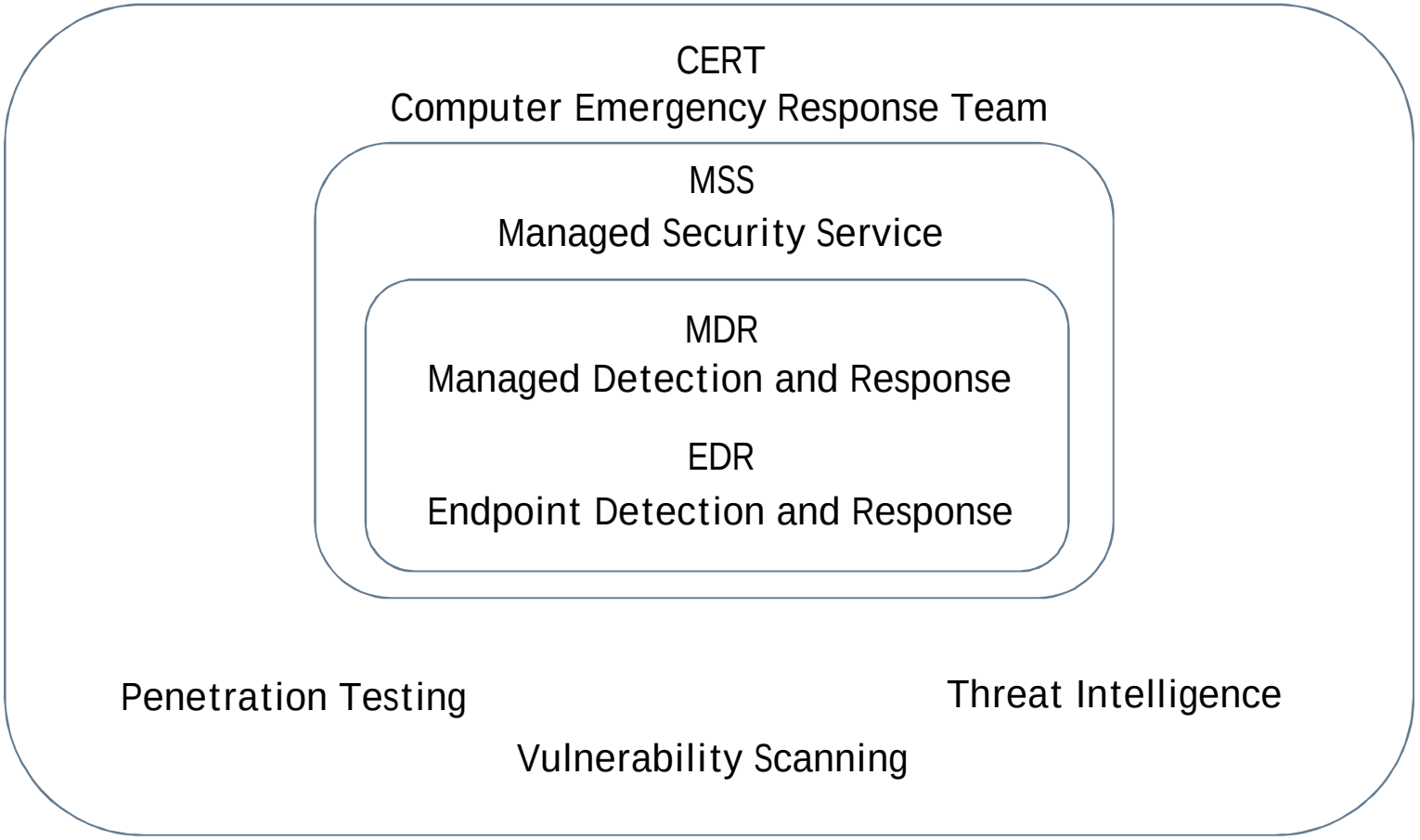
True

LIVE-MONITORING FÜR CYBER ATTACKS

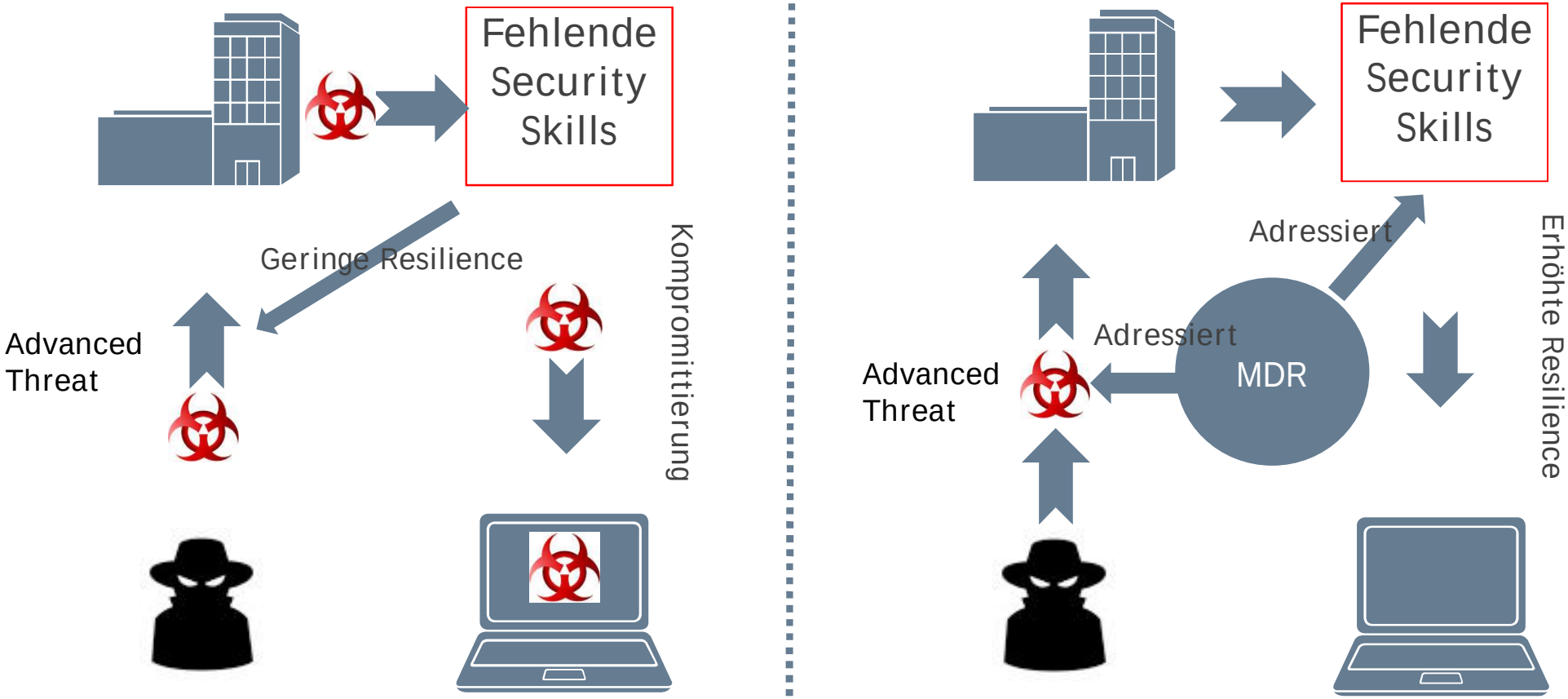


2. CYBER COUNTER MEASURES

CYBER SECURITY SERVICES



MANAGED SECURITY SERVICES



CYBERSECURITY ACTIVITIES

Identify

Protect

Detect

Respond

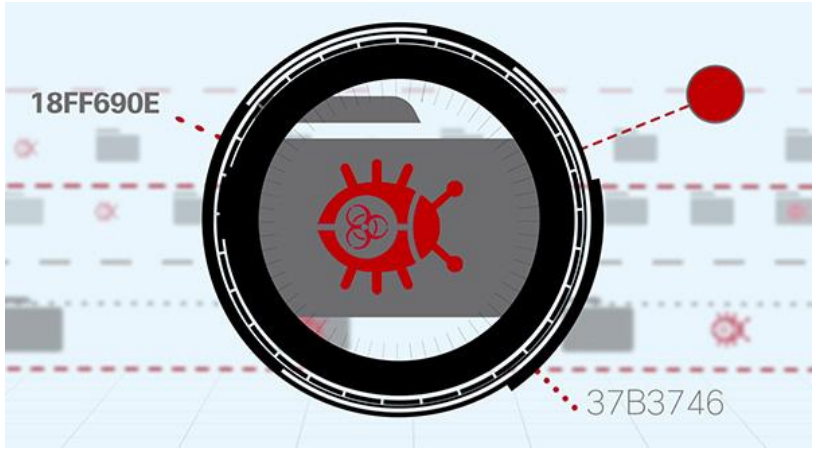
Recover

IDENTIFY

- Evaluierung und Entwicklung von Governance Security Unterlagen
- Risk Assessments mit entsprechenden Empfehlungen
- Durchführung von Sicherheits Audits
- Unterstützung bei Cyber Insurance Themen
- Evaluierung der Cyber Security unter unterschiedlichen Sicherheits Standards, Regulierungen und Management Frameworks
- Configuration Management
- Security Testing
- Vulnerability scanning
- Penetration testing
- Web Application testing

PROTECT

- Endpoint Protection
  - Block Malware
  - Quarantine Malware
- Hardening
  - Configuration Support
- Data Security
  - Encryption
  - DLP
- Awareness und Training
  - Phishing Awareness
  - Scenario-Based Training



DETECT

- Security Monitoring
  - Networks
  - Endpoints (EDR, EPP)
  - Cloud
- Threat detection
  - Events / Anomalies
- Deception
  - Honeypots / Honeytokens
- On-going Intelligence Gathering zur Unterstützung der Detection und Response Activities
- Physikalische und/oder Virtuelle Sensoren
  - Cloud und hybride Infrastrukturen
  - Einsetzbar für klassifizierte Systeme

RESPOND

- 24/7 SOC
- General alerts
  - Information about new and relevant threats and vulnerabilities as it becomes available
- Specific alerts
- Detected threats and vulnerabilities
- Incident response
  - Remote
  - On-site
- Analysis
  - Technical
  - Tactical
  - Strategic

RECOVER

- Advisory services nach einem Incident
- Follow-up of recommendations aus dem Incident Report
- Strategische Kommunikation
- BCP/DR planning als Teil der Identifikation und Post Mortem Analyse

3. CYBER ATTACK EXAMPLES

SOCIAL ENGINEERING

- Information an die zuständige Stelle
- Zuständigkeit für den Incident festlegen

- Feststellung der Ursache
- Interne Untersuchung
- Interviews

- Human Factor
- PR Risiko
- Besteht der Angriff weiter
- Welche Absicht hat der Angriff
- Bei Fraud entsprechende Untersuchung einleiten
- Welche Maßnahmen zur Wiederherstellung
- Verbesserung der Prozesse

DDOS ATTACK

- Information an die zuständige Stelle
- Zuständigkeit für den Incident festlegen

- Bestimmte Zeiten?
- Ist der Angriff zielgerichtet?
- Große files?
- Gibt es weitere Auffälligkeiten?

- Aussitzen
- Filtern nach Angriffsvektor
- Kommunikation
  - Intern
  - Extern

DATA BREACH

- Information an die zuständige Stelle
- Zuständigkeit für den Incident festlegen

- Welche Daten sind betroffen?
- Wie lange dauerte der Angriff
- APT?
- Cyber Forensics Investigation

- Legal
  - Regulatorische Policies
  - Klassifizierung der Daten
- Public Relations
  - Pressemitteilung
  - Kommunikation
    - Intern
    - Extern
- Remediation Plan

4. FUTURE OF CYBERSECURITY

FUTURE OF CYBERSECURITY

The Bad News

- Cyber Angriffe werden weiter sowohl zahlenmäßig, an Reifegrad und Schadenshöhe global zunehmen
- Die Kosten für Cyber Security werden steigen, da verbesserte Systeme benötigt werden und der Automatisierungsgrad steigen wird
- Der Mangel an erfahrenen Cyber Spezialisten wird weiter zunehmen
- Die Kosten für Cyber Versicherungen werden steigen
- Neue Technologien, Produkte und Services steigern die Cyber Angriffsfläche weiter

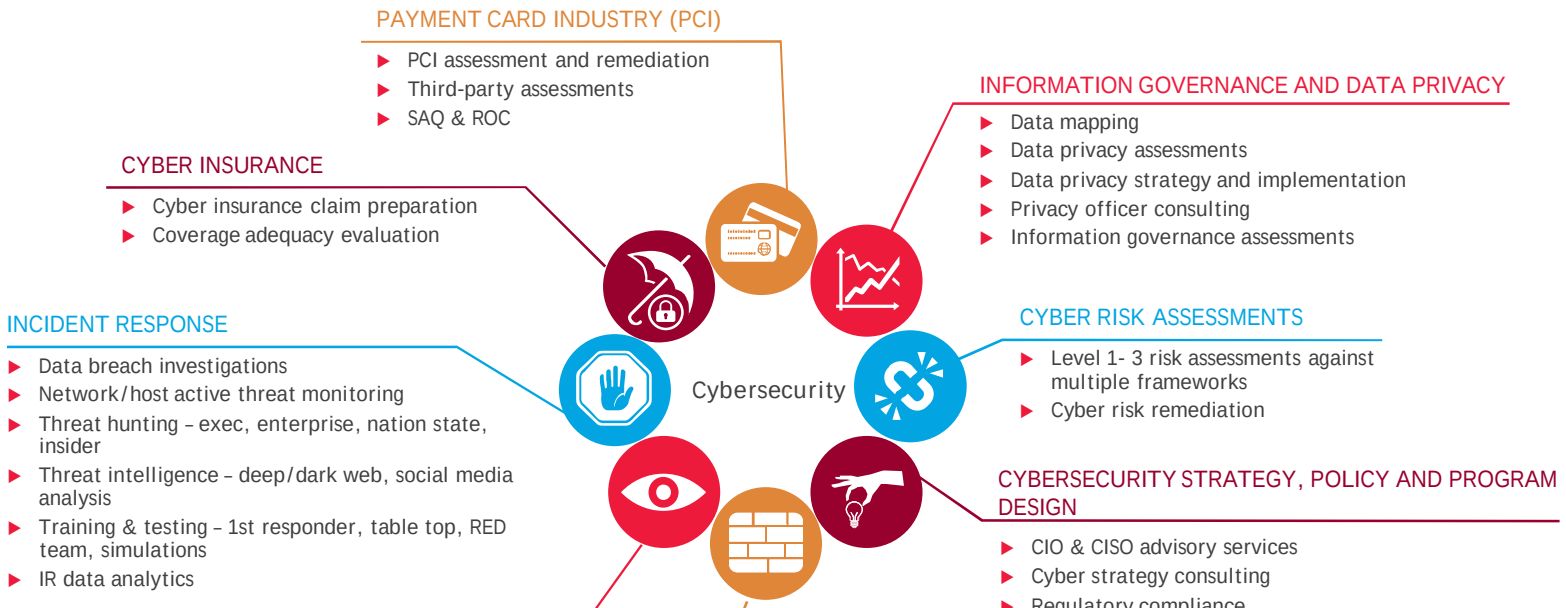
FUTURE OF CYBERSECURITY

The Good News

- Machine Learning basierend auf mathematischen Funktionen trägt dazu bei schneller Data Breaches festzustellen und entsprechend früher eine Response zu ermöglichen
- Artificial Intelligence (AI) ermöglicht es, dass Systeme sich selbst überwachen und entsprechende Maßnahmen zur Wiederherstellung einleiten
- Big Data & Threat Advanced Visualization Tools wie Splunk Data Analytics Tools, Cybersecurity Dashboards, … vereinfachen die Arbeit der Spezialisten
- Predictive Analytics Software auf User-, Applikations-, Geräte-, oder Netzwerkebene helfen Auffälligkeiten festzustellen und die Daten zu sammeln
- Enhanced Monitoring, Detection & Incident Response über Managed Security Services auf 24/7/365 Basis über global Security Operation Centers werden die Response Zeit verkürzen und die Cyber Breach Kosten deutlich reduzieren

5. 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