

# Versicherungs- und Präventionslösungen für Cyber- Risiken in sozialen Unternehmen

Andreas Braun  
Führungskonferenz  
Paritätischer Sachsen Dresden,  
26. April 2017

## Ihr Ansprechpartner:

Diplom-Ingenieur (FH)

Versicherungsfachwirt

**ANDREAS BRAUN**



### Home-Office:

Am Dammburg 18

01445 Radebeul

Telefon +49 (0) 351 8382568

Telefax + 49 (0) 351 8382570



### Niederlassung Leipzig

Brühl 65

04109 Leipzig

Telefon +49 (0) 341 41546-12

Telefax + 49 (0) 341 41546-29

E-Mail: [andreas.braun@ecclesia.de](mailto:andreas.braun@ecclesia.de)

# Agenda

1 | Cyber-Risiken im Überblick

2 | Versicherungsschutz – Spezialkonzepte der Ecclesia Gruppe

3 | Schadenprävention – Dienstleistungen der Ecclesia Gruppe

# Was ist Cyber-Kriminalität?

## Gefährdungen und Absicherungsbedarf

### Cyber-Kriminalität

- Cyber-Kriminalität ist jede vorsätzliche unerlaubte Handlung, die mittels eines Computers, Netzwerks- oder Hardware-Geräts begangen werden kann.

Cyber-Kriminalität	Klassische IT-Risiken	
Unerlaubter Zugriff/Spionage	Festplattencrash	Verschleiß
Schadsoftware (z.B. Wurm)	Fehlender EDV-Zugriff (kein DDoS)	Fehlerhafte Updates
Störung der eigenen EDV durch einen Ausfall des IT-Dienstleisters		Hardwareschäden (z.B. Brand)
Bedienungsfehler		....
Systemblockade (z.B. DDoS)		
Erpressung (Ransomware)		
Identitätsdiebstahl (z.B. Phising)		
Weitere Betrugshandlungen		

# Die Cyber-Kriminalität in Zahlen

## Fakten 2015

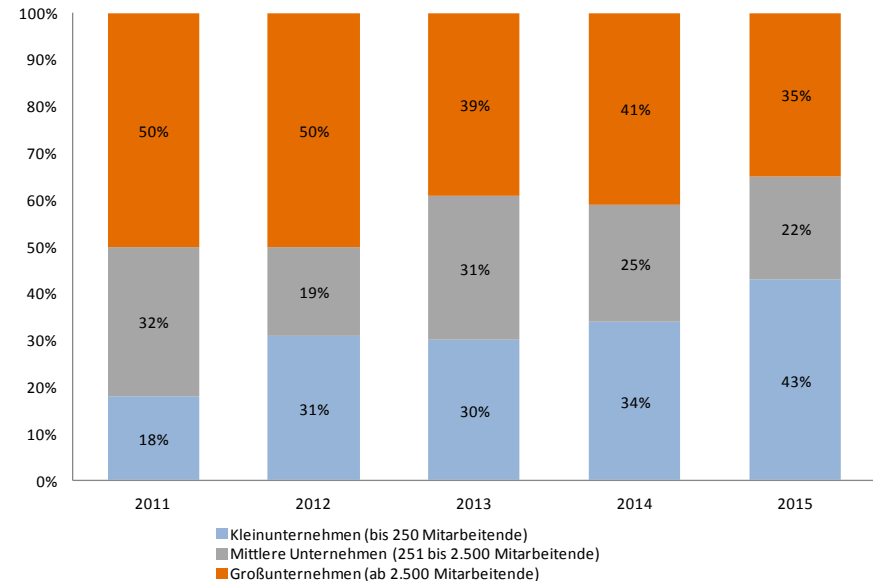
- 65% der gezielten Angriffe richten sich gegen kleine und mittlere Unternehmen.
- 431 Mio. neue Schadprogramme (1,18 Mio./Tag).
- 318 öffentlich gewordene Datendiebstähle mit 429 Mio. personenbezogenen Daten (davon rund 1/3 im Gesundheitswesen).
- 362.000 Erpressungsprogramme (Ransomware).
- Angreifer sind professionelle Hacker, Wettbewerber oder Mitarbeitende.

Neue Schadsoftware pro Jahr	
2014	2015
317 Mio.	431 Mio.
-	<b>36%</b>

Unberechtigte Zugriffe auf Daten		
2013	2014	2015
253	312	318
-	<b>23%</b>	<b>2%</b>

Erpressungssoftware (Ransomware) gesamt	
2014	2015
269.000	362.000
-	<b>35%</b>

Gezielte Angriffe (Spear-Phishing Attacks)



# Was ist Cyber-Kriminalität?

## Gefährdungen und Absicherungsbedarf

### Absicherungsbedarf

1. Mehrtägige Betriebsunterbrechung durch gesperrte oder beschädigte Daten.
2. Veranlassung eines sechststelligen Geldbetrags mittels Identitätsdiebstahl.
3. Unberechtigter Zugriff und Veröffentlichung von Gesundheitsdaten.

### Benachrichtigungskosten bei Datenschutzverletzungen

Ertragsausfall und Mehrkosten

Kosten für Rufschädigung/Krisenmanagement

Sachverständigen-/Forensikkosten

Kosten für Datenwiederherstellung

Schadenersatzansprüche

Kosten für Rechtsschutz

Kosten für Erpressung/Lösegelder

Vermögensschäden durch kriminelle Handlungen

Sachschäden

Personenschäden

Daten

## Schadenbeispiele Cyber-Risiken

### 1. Sozialeinrichtung (Geschäftsstelle)

**Hergang:** Festgestellt wurde ein Virenbefall auf mehreren Rechnern. Der Virenschanner hat diese nicht erkannt. Erst als verschiedene Anwendungen sich nicht mehr starten ließen, erfolgte ein umfangreicher Test. IT-Infrastruktur verfügt über 16 Server, 210 Arbeitsplätze und 35 Notebooks.

**Schaden ca. 68.000 Euro (Desinfektion, Vireneseitigung, Analysen über den Umfang des Befalls, Mehrarbeit eigene Mitarbeiter). Auch sind einige PC's als Schadenminderungsmaßnahme ersetzt worden, da die Vireneseitigung, etc. teurer als eine Neuanschaffung gewesen wäre.**

## Schadenbeispiele Cyber-Risiken

### 2. Pflegeeinrichtung

**Hergang:** Es wurden Probleme am Server festgestellt. Der Server konnte einige Male komplett gebootet werden, aber das System stürzte jeweils nach einigen Minuten wieder ab. Hardwarekomponenten, wie Arbeitsspeicher und CPU, wurden getauscht – jedoch auch erfolglos. Anschließend wurden Mainboard und RAID-Controller getauscht. Dadurch konnten Systemeinstellungen durchgeführt werden, Probleme waren aber weiterhin vorhanden. Daraufhin wurde ein neues System eingesetzt. Ein Backup sollte eingespielt werden. Ein Backup war fehlerhaft, sodass man auf Daten vom Vortag zurückgreifen musste. Nach umfangreichen Datensicherungs- und Rettungsmaßnahmen konnten die Daten auf das neue System übertragen werden.

Insgesamt standen die EDV-Anwendungen nicht oder nur teilweise zur Verfügung. Pflegedokumentationen mussten in dieser Zeit per Hand erfolgen. Die Daten mussten anschließend in das System übertragen werden. Eigenes Personal musste die Übertragungen durchführen, externes Personal wurde dann eingesetzt, um die eigentliche Pflege vorzunehmen. Schaden ca. 70.000 € (ohne Hardware).



## Schadenbeispiele Cyber-Risiken

### 3. Träger von Altenhilfe- und Sozialeinrichtungen

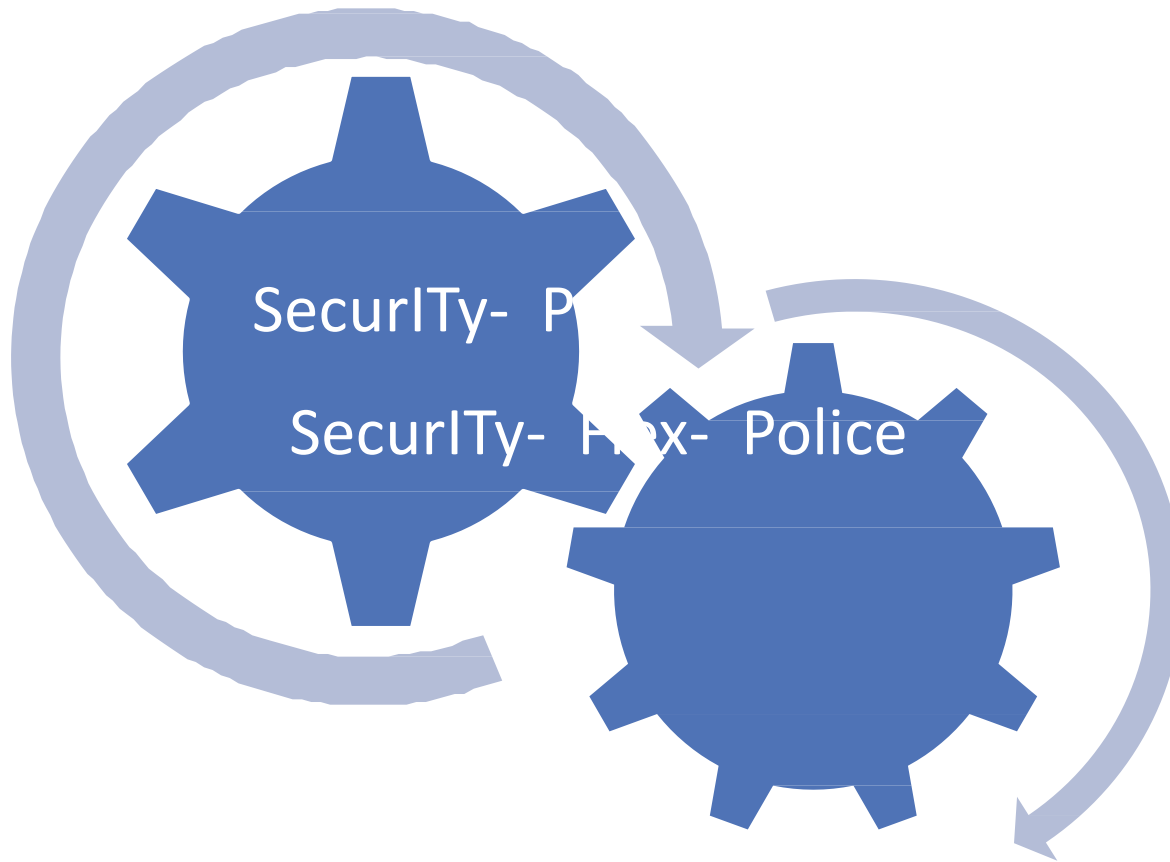
**Hergang: In der Nähe der Hauptverwaltung (Nachbargrundstück) wurde ein Stromkabel beschädigt. Im Bereich der Hauptverwaltung gab es einen kompletten Stromausfall. Mehrere Geräte wurden beschädigt, Server sind abgestürzt. Daten und Konfigurationen mussten wiederhergestellt werden. Schaden ca. 18.000 Euro für Wiederherstellungen und Mehrarbeit eigener Mitarbeiter.**

# Absicherung von Cyber-Risiken

## Spezialkonzepte der Ecclesia Gruppe

Grundschutz	A   Ertragsausfall und Mehrkosten	
	B   Sachverständigen-/Forensikkosten	
	C   Kosten für Datenwiederherstellung	
Erweiterter Versicherungsschutz	D   Kosten für Rufschädigung/Krisenmanagement	
	E   Kosten aufgrund von Datenschutzverletzungen	
	F   Vertrauensschaden (Internet-Betrug)	
	G   Erpressung	
	H   Cyber-Haftpflicht	

# Versicherungsschutz – Spezialkonzepte



# Versicherungsschutz – SecurITy-Police

- Allgefahrenversicherung bestehend aus
  - Softwareversicherung
  - Betriebsunterbrechungsversicherung
  - Mehrkostenversicherung
- Ergänzung zur Elektronik-Versicherung

# Versicherungsschutz – SecurITy-Police

- **Softwareversicherung**
  - Versicherungsschutz für Daten & Programme
- **Betriebsunterbrechungsversicherung**
  - Versicherungsschutz für unmittelbare Ertragsausfälle
- **Mehrkostenversicherung**
  - Versicherungsschutz für schadenbedingte Mehrkosten zur Fortführung des Betriebes

# Versicherungsschutz – SecurITy-Flex-Police

- **Warum überhaupt eine Cyber-Versicherung?**
  - Schäden und Risiken sind vielfältig und keiner bestehenden Versicherungssparte zuzuordnen
  - Sonstige Versicherungen bieten nur Ausschnitts-Deckungen

# Versicherungsschutz – SecurTy-Flex-Police

- **Eine Cyber-Versicherung im Baustein-Prinzip**
  - Sie entscheiden welche Module Sie absichern wollen
  
- **Vorteile:**
- Flexible Gestaltung des Versicherungsschutzes
  - Wahl der Module
  - Wahl der Versicherungssummen und Selbstbehalte
- Besonderheiten für Unternehmen aus der Sozialwirtschaft berücksichtigt (z.B. Versicherungsschutz auch für Ehrenamtliche)

# Versicherungsschutz – SecurITy-Flex-Police

A | Ertragsausfall

B | Sachverständigenkosten

C | Datenwiederherstellung

D | Rufschädigung/Krisenmanagement

E | Datenschutzverletzungen

F | Vertrauensschaden (Internet-Betrug)

G | Erpressung

H | Cyber-Haftpflicht



# Produkt „SecurTY-Flex-Police“

## Ertragsausfall

- ▶ **Ertragsausfall und Mehrkosten**, durch z.B.
  - ▶ Unvorhergesehene Beeinträchtigung des Telekommunikationsnetzes
  - ▶ Bedienungsfehler durch eigene Mitarbeiter
  - ▶ Unvorhergesehene Überlastung durch Dos-Attacken auf das EDV-System oder die Website des VN
  - ▶ Vorsätzliche Programm- oder Datenänderungen
  - ▶ Unvorhergesehener Ausfall einer vom VN mit einem Dienstleister vereinbarten IT-Dienstleistung (z.B. cloud-Ausfall)

## Sachverständigenkosten

- ▶ **Kosten für ext. Sachverständige**, z.B.
  - ▶ bei einer versicherten Betriebsunterbrechung,
  - ▶ Wirtschaftsspionage,
  - ▶ vorsätzliche Manipulation von Daten durch Mitarbeitende oder Dritte.

# Produkt „SecurTy-Flex-Police“

## Wiederherstellungskosten

- ▶ **Wiederherstellungskosten** für Daten und (betriebsfertige/funktionsfähige) Programme, um den früheren, betriebsfertigen Zustand wiederherzustellen, durch
  - ▶ Programm und Datenänderung durch Programme mit Schadenfunktion
  - ▶ Vorsätzliche Programm- oder Datenänderungen durch Dritte

## Rufschädigung

- ▶ **Kosten** zur Abwendung oder Minderung eines Reputationsschadens sowie zur Wiederherstellung des guten Rufes , durch
  - ▶ Eine versicherte Betriebsunterbrechung,
  - ▶ Wirtschaftsspionage,
  - ▶ vorsätzliche Manipulation von Daten durch Mitarbeitende oder Dritte.

# Produkt „SecurTY-Flex-Police“

## Datenschutz- verletzungen

- ▶ Aufwendungen zur gesetzlich geforderten **Information** von Behörden, Öffentlichkeit und potentiell betroffenen Personen, durch
  - ▶ Unberechtigten Zugriff auf Daten (digitale und physische Daten)
  - ▶ Verlust von Datenträgern durch Einbruch bzw. Diebstahl o. andere Gründe

## Internet-Betrug

- ▶ Hacker-Angriff über ein Telekommunikationsnetz, der unmittelbar einen **Vermögensschaden** des Versicherungsnehmers verursacht hat, durch
  - ▶ Manipulation der Webseite (einschließlich Datenbanken und Programme) und des Onlinebankings, der Zahlungssysteme oder Anwendungsprogramme;
  - ▶ Diebstahl der Identität des Versicherungsnehmers oder einer versicherten Person;
  - ▶ Unberechtigte Nutzung der Telefonanlage/des EDV-Systems.

# Produkt „SecurTy-Flex-Police“

## Erpressung

- ▶ Versichert ist das an den Erpresser gezahlte **Erpressungsgeld** und die Beratungskosten, durch
  - ▶ Zugangssperren zu Daten und Programmen oder Störung des EDV-Systems
  - ▶ Unberechtigter Zugriff auf geschützte digital gespeicherte Daten.

## Cyber-Haftpflicht

- ▶ Gesetzliche Haftpflicht privatrechtlichen Inhalts wegen Vermögensschäden und immaterieller Schäden Dritter, durch
  - ▶ Löschung, Verlust, Veränderung oder Nichtverfügbarkeit von Daten oder Programmen eines Dritten;
  - ▶ Hacker-Angriffen auf das EDV-System oder die Website;
  - ▶ Datenschutzverletzungen und
  - ▶ unberechtigter Verbreitung von Daten und Programmen.
  - ▶ **Sachlicher Umfang:** Prüfung der Haftpflichtfrage, Abwehr und Freistellung

# Versicherungsschutz – Cyber-Policen im Kontext

## SecurITy-Police

Festplattencrash

fehlender EDV-Zugriff

(kein DoS) fehlerhafte

Updates

Elementar

## SecurITy-Flex-Police

Erpressung

PR-/Krisenberater

Datenschutz

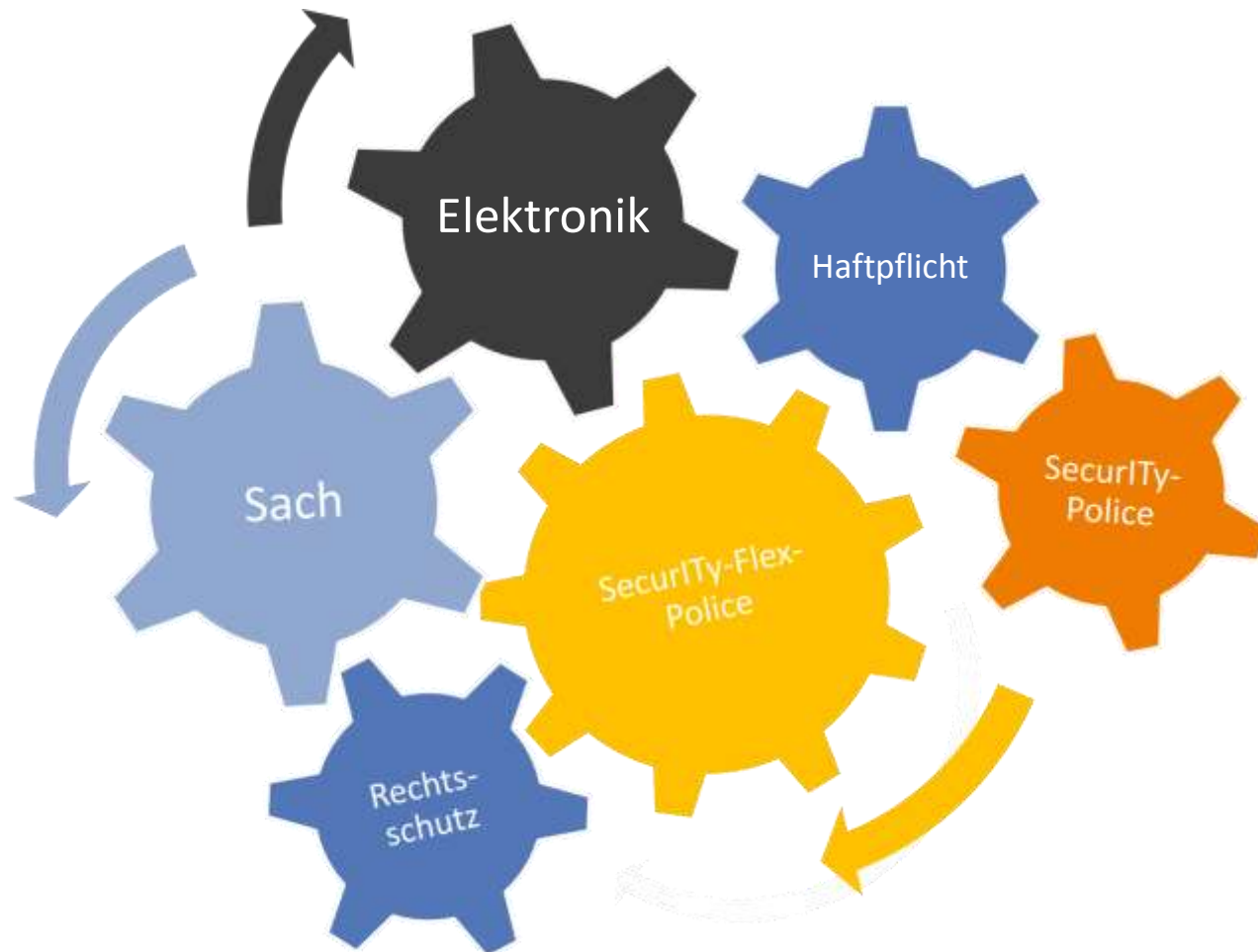
Haftpflicht

Viren  
Würmer

Trojaner

DoS-Attacke

# Versicherungsschutz



# Schadenprävention

- IT-Sicherheit – Der Brandschutz des 21. Jahrhunderts



# Schadenprävention

- Neues Dienstleistungskonzept - **CyRis**



# CyRis

Systematisches Management von Cyberrisiken



# Schadenprävention

- Neues Dienstleistungskonzept – **CyRis**
  - Spezialisierter Dienstleister: HiSolutions AG
  - Kooperationsvertrag mit Vorteilen für Kunden der Ecclesia Gruppe (z.B. Notfall-Hotline)
  - Exklusive Preise
  - Modulare Dienstleistungen

# Schadenprävention

## ■ Neues Dienstleistungskonzept – **CyRis**

- Basis-Check
- Cyber-Krisenmanagement
- IT-Notfallübungen
- IT-Sicherheitsprüfungen
- Administratorenschulungen

**Prävention**

- Cyber-Response

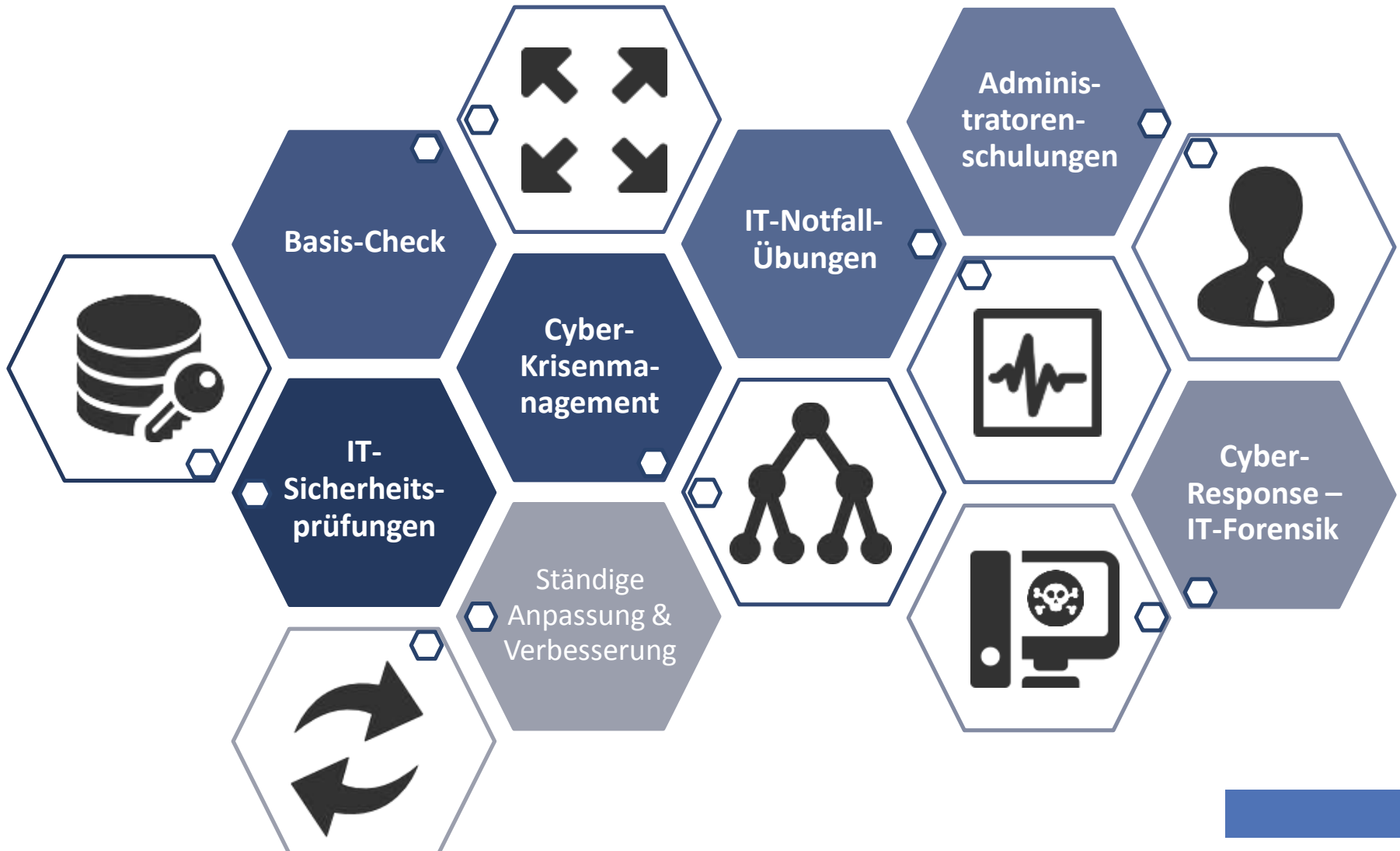
**Reaktion**

# Schadenprävention - CyRis



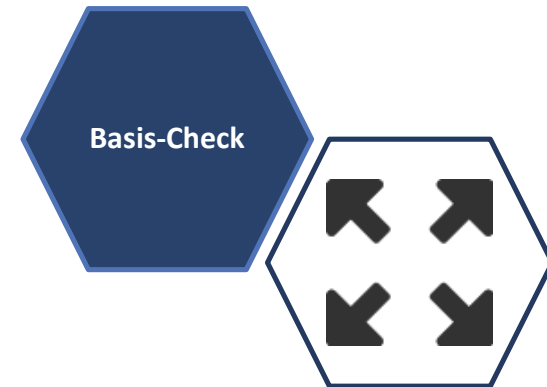
Alle Dienstleistungen können als Ausgangspunkt zur Vorbereitung auf die ISO-27001-Zertifizierung genutzt werden.

# Schadenprävention – CyRis



# CyRis – Basis-Check

- Standortbestimmung der IT-Sicherheit
  - 3 bis 4-stündigen Interview
  - Prüfung aller relevanten Bereiche
  - Organisation, ISMS, IT-Landschaft, ....
  - Erstellung eines Berichts mit Handlungsempfehlungen



## CyRis – IT-Notfallübungen

- Prüfung, der Fähigkeit in Notfallsituationen angemessen zu handeln
- Training von Fähigkeiten für schnellen Wiederanlauf des Betriebs

IT-Notfall-  
manage-  
ment



## CyRis – IT-Sicherheitsprüfungen

- Suche nach Sicherheitslücken
- Simulation von nicht autorisierten Zugriffen

IT-  
Sicherheits-  
prüfungen



## CyRis – Administratorenschulungen

Adminstra-  
toren-  
schulungen



- Vermittlung von Spezialkenntnissen zur Abwehr von Cyber-Angriffen
- Training der Reaktion auf Cyber-Angriffe
- Training von Erstmaßnahmen, Entwicklung von Strategien einschließlich Dokumentation

## CyRis – Cyber-Krisenmanagement

Cyber-  
Krisen-  
manage-  
ment



- Training von Sofortmaßnahmen zur systematischen Behandlung eines Cyber-Vorfalles

# CyRis – Cyber-Response

- Unterstützung bei der Krisenreaktion
- Gerichtsfeste Dokumentation
- Forensik

Adminstra-  
toren-  
schulungen







Fragen oder  
Anmerkungen



**Herzlichen Dank  
für Ihre Aufmerksamkeit!**

[andreas-braun@union-verdi.de](mailto:andreas-braun@union-verdi.de)