

Mehr Digitalisierung = mehr Angriffsfläche



... im Kanalnetz

Spezialisten für Wasser und Energie



Thomas Brüning, B.Eng.
john becker ingenieure
27726 Worpswede
th.bruening@wirberaten.de
+49 4792 9310-63

Spezialisten für Wasser und Energie



Dipl.-Ing. Martin Mergelmeyer
john becker ingenieure
27726 Worpswede
m.mergelmeyer@wirberaten.de
+49 4792 9310-16





Quelle: Thorben Wengert/pixelio.de

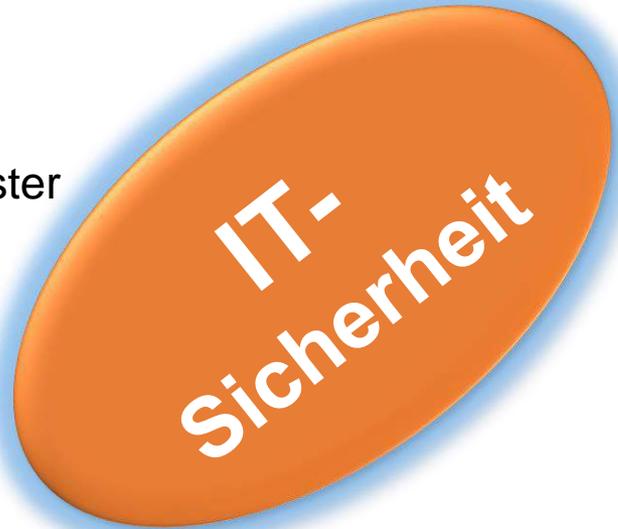
- ▶ Eingreifen/beeinflussen (schalten, Sollwertveränderung etc.)



Quelle: Fionn Große/pixelio.de

- ▶ Überwachen (Betriebszustände, Störungen, Messwerte etc.)

- Absetzen von Alarmen bei Störung der Außenstation
- Erfassung von wichtigen Betriebsdaten
- Pufferung/Zwischenverarbeitung von Daten und Meldungen
- Übertragung der Störungen und Daten zur Zentrale oder zur Bereitschaft
- flexible Kommunikationswege
- Investitionssicherheit/lange Verfügbarkeit
- Unabhängigkeit vom Hersteller und Dienstleister
- Zuverlässigkeit
- und weiteres....



IT-
Sicherheit

Systeme zum Fernwirken



SIEMENS



Automatisierungsgerät

Modem/Router



SIEMENS



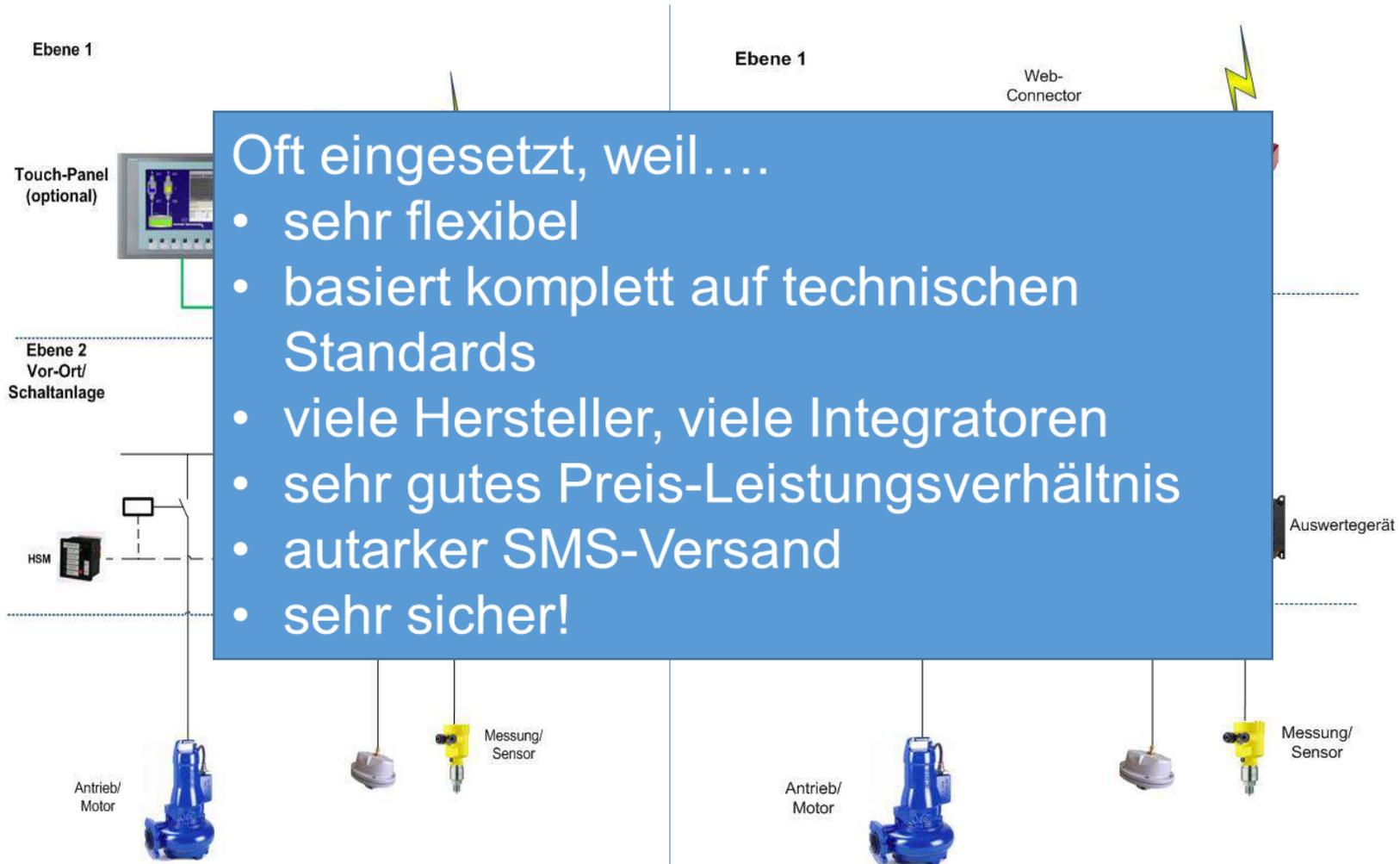
OPC



DSL (mit fester IP)

UMTS/LTE
DSL ...





• Batterie

- Batteriebetrieb
Fernwirkstationen mit autonomer Stromversorgung
- je nach Anwendung bis zu 10 Jahren
- GPRS-Datenübertragung zyklisch und eventgesteuert



• Solar

- fertige Solarsets
- praxiserprobt und optimiert ausgelegt
- Betrieb über ca. 2 Wochen ohne Sonneneinstrahlung
- schnelle Inbetriebnahme



- **sichere Datenübertragung über Mobilfunk**
- Verwendung von marktüblicher Hardware und Software (minimale Herstellerabhängigkeit) - Investitionsschutz
- Verwendung von industriellen Standardschnittstellen und Protokollen
- **Hardware im Mischbetrieb möglich**
- Kostenkontrolle der gesamten Kommunikation
- gutes Preis-Leistungsverhältnis
- autarker SMS-Versand bei Ausfall der übergeordneten Technik (2. Alarmweg)
- **ausbaufähig**
- **Datenpufferung bei Ausfall der Kommunikation**

Mehr Digitalisierung = mehr Angriffsfläche



... im Kanalnetz

DWA-Regelwerk

Merkblatt DWA-M 1060

IT-Sicherheit – Branchenstandard Wasser/Abwasser

August 2017

- IT-Schutzziele
 - Verfügbarkeit
 - Integrität
 - Authentizität
 - Vertraulichkeit

You Have
Been Hacked



Der Sicherheitstacho zeigt die weltweiten Cyberangriffe auf die Honeypotinfrastruktur der DTAG sowie ihrer Partner an.

> 1,5 Mio. Zugriffe der letzten 24

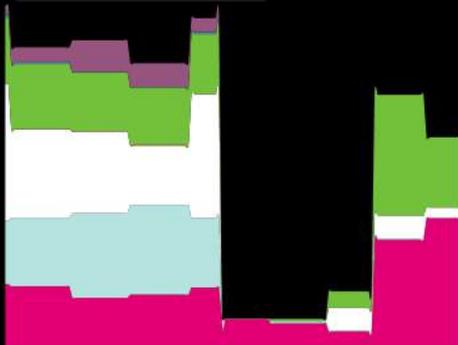
h

Attacken in der letzten Minute

88644 Attacken in den letzten 1 h

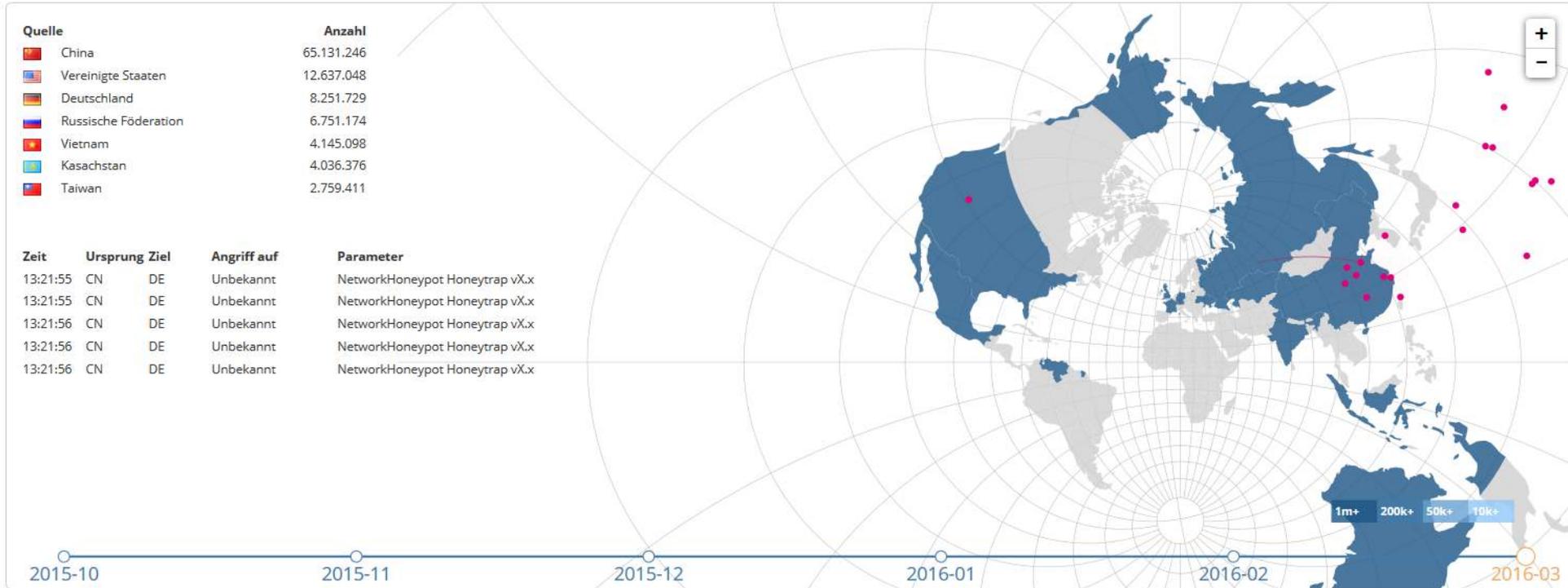
1583982 Attacken in den letzten 24 h

■ WEBPAGE
■ SSH/CONSOLE(COWRIE)
■ NETWORK(HONEYTRAP)



Cyberangriffe DTAG

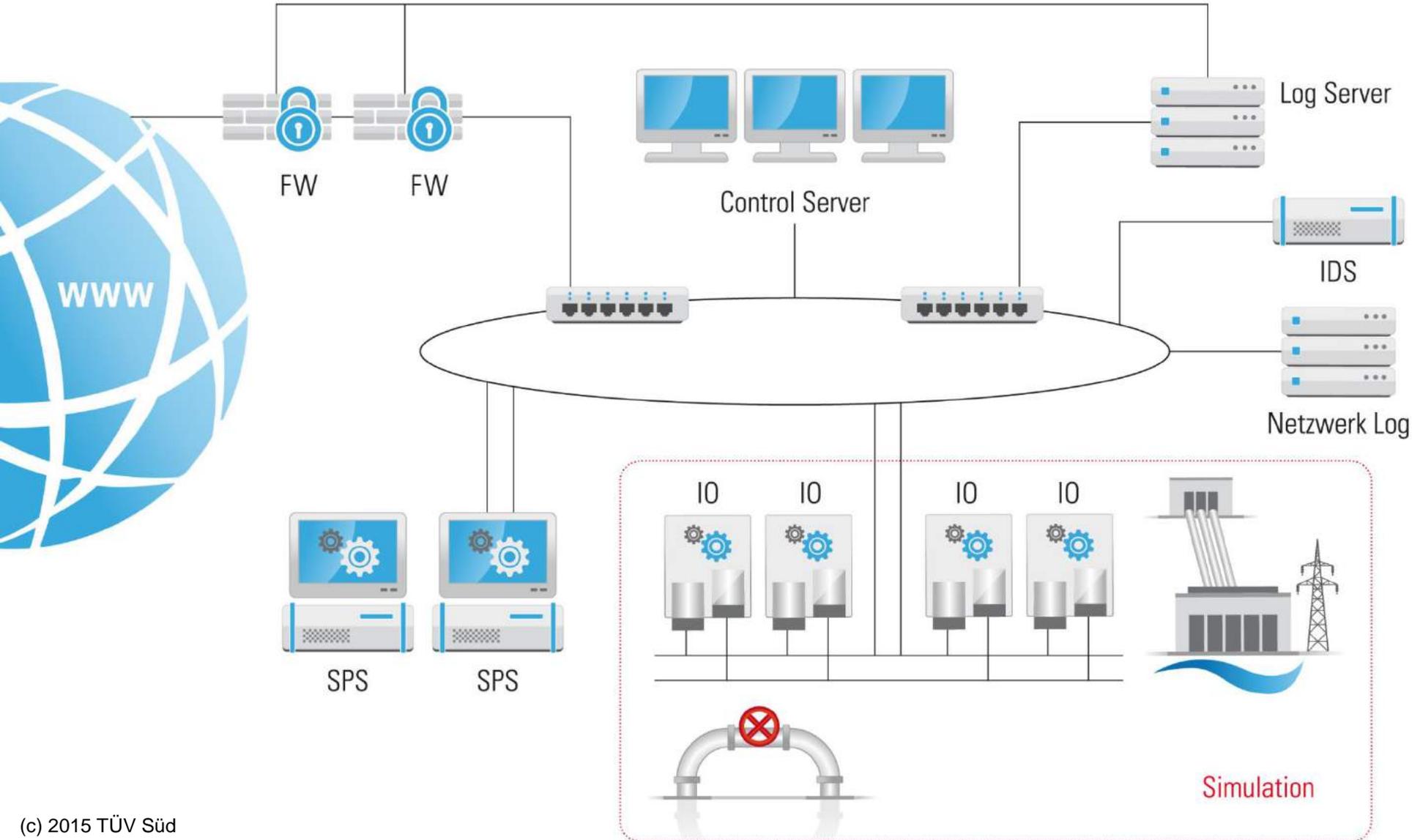
Übersicht über die aktuellen Cyberangriffe auf DTAG-Sensoren (aufgezeichnet von 180 Sensoren)



Trend Analyse

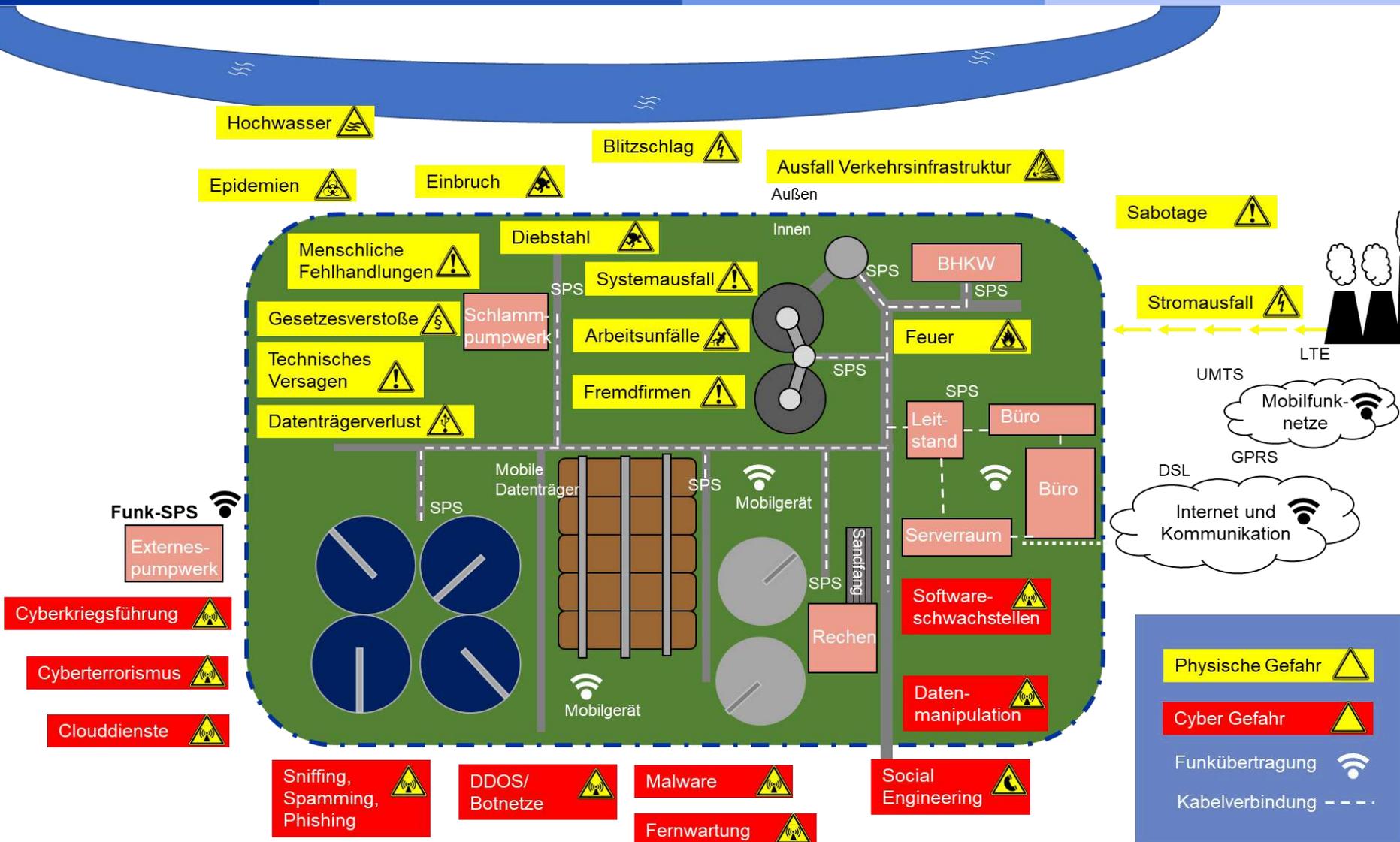


Honigtöpfe der Wasserwelt



- 8 Monate im Netz
- erster Zugriff zeitgleich mit dem Scharfschalten
- mehr als 60 000 Zugriffe aus mehr als 150 Ländern
- Zugriffe nicht nur über Büro-IT, sondern auch über Industrieprotokolle wie Modbus TCP oder S7Comm
- Lücken in der Sicherheitsarchitektur von Steuerungsanlagen

Sicherheit für KRITIS

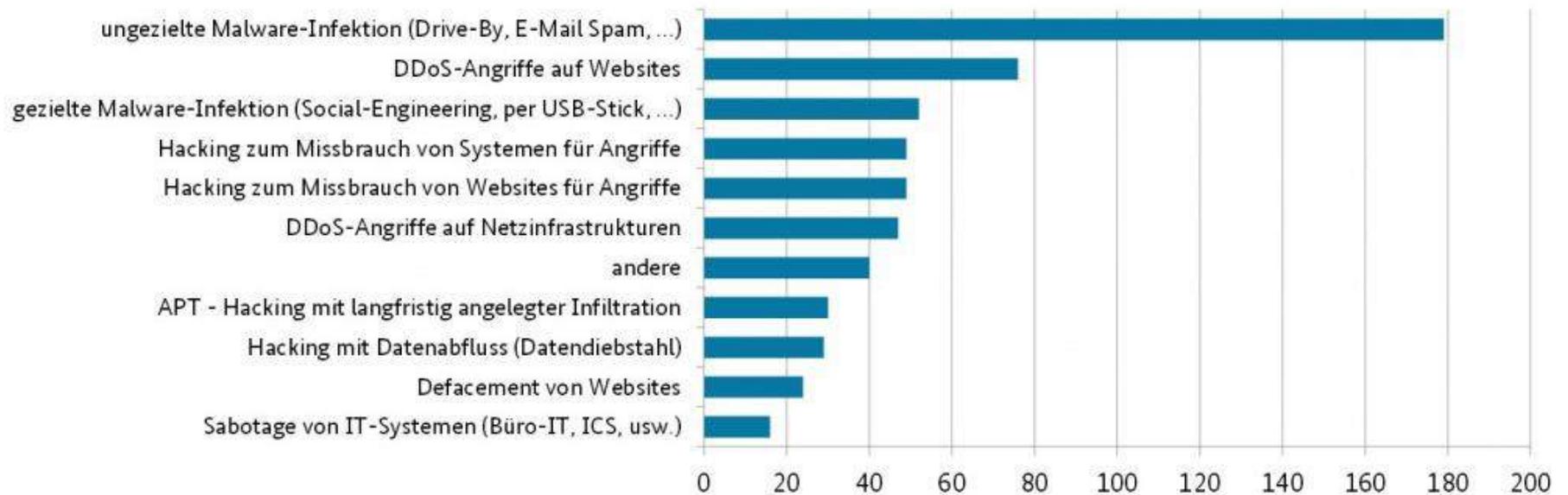


Dienstleistung	Anlagentyp	Kriterium	Schwelle
Abwasserbeseitigung	Kanalisation	Angeschlossene Einwohner	500 000
	Kläranlage	Ausbaugröße in Einwohnerwerten	500 000
	Leiteinrichtung	Ausbaugröße der gesteuerten/ überwachten Anlagen	500 000

Das BSI empfiehlt den Betreibern, ab einer Ausbaugröße von **50 000** EW bzw. **50 000** am Kanalnetz angeschlossenen Einwohnern der öffentlichen Kooperation „UP KRITIS“ beizutreten.

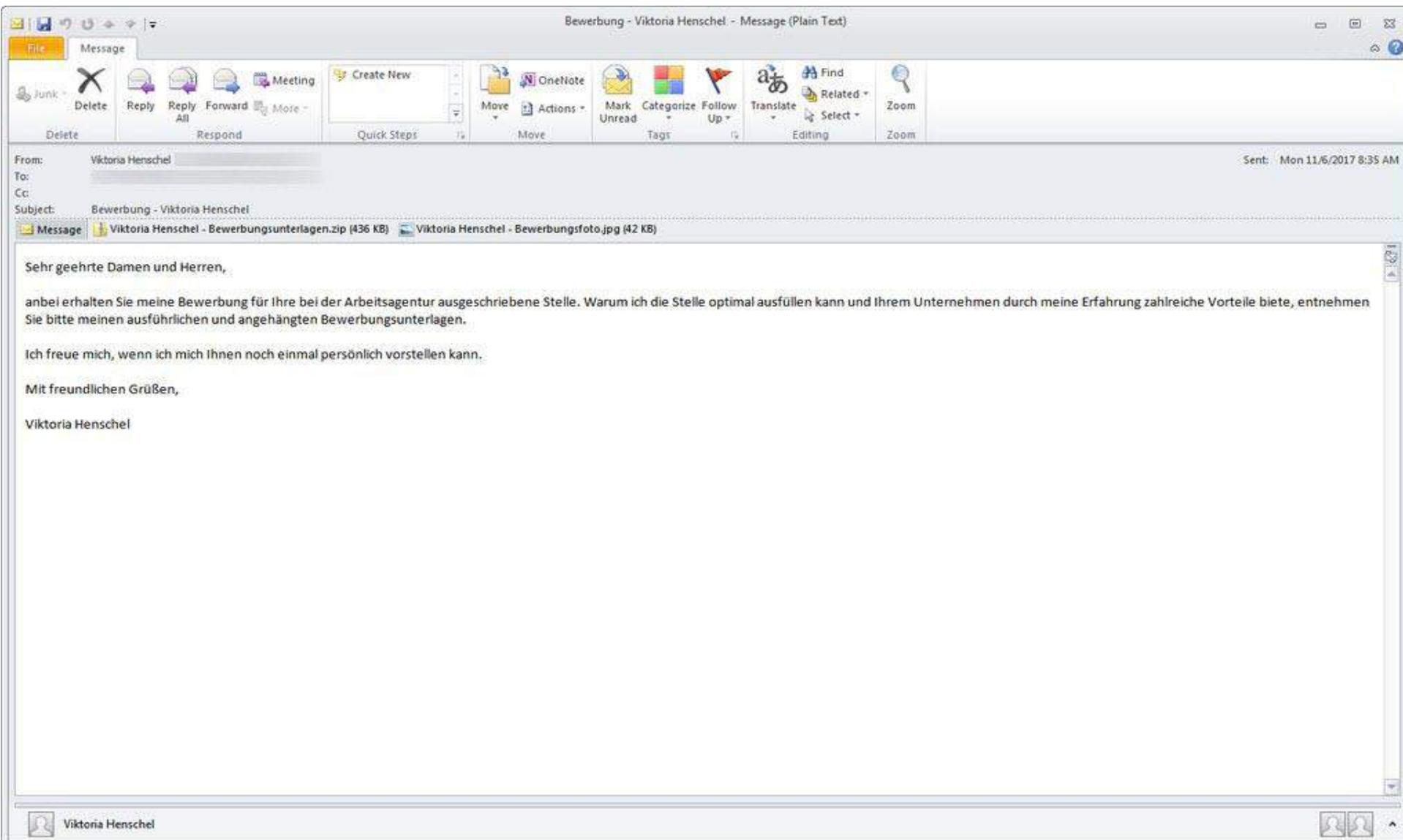
Kleineren Anlagenbetreibern wird empfohlen, der „Allianz für Cybersicherheit“ beizutreten.

Von 248 Befragten gaben ... folgende Arten von Angriffen an



Quelle: Cyber-Sicherheits-Umfrage 2015, Ergebnisse, Stand 05.10.2015

Malware



The screenshot shows an Outlook window titled "Bewerbung - Viktoria Henschel - Message (Plain Text)". The interface includes a ribbon with tabs for "File" and "Message". The "Message" tab is active, showing various actions like "Delete", "Reply", "Forward", "More", "Create New", "Move", "Actions", "Mark Unread", "Categorize", "Follow Up", "Translate", "Find", "Related", "Select", and "Zoom".

The email header shows:

- From: Viktoria Henschel
- To: [Redacted]
- Cc: [Redacted]
- Subject: Bewerbung - Viktoria Henschel
- Sent: Mon 11/6/2017 8:35 AM

The email body contains the following text:

Sehr geehrte Damen und Herren,

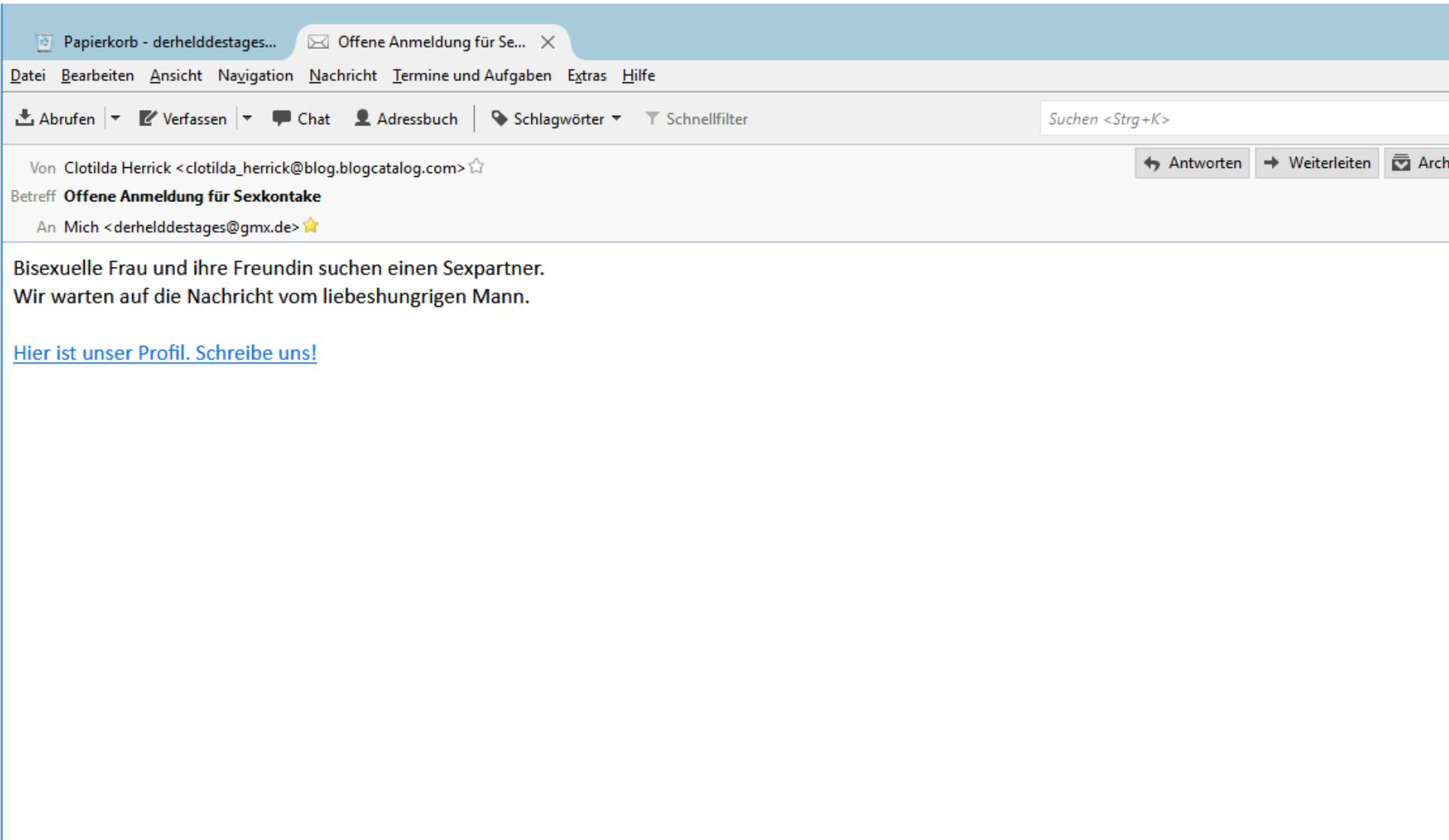
anbei erhalten Sie meine Bewerbung für Ihre bei der Arbeitsagentur ausgeschriebene Stelle. Warum ich die Stelle optimal ausfüllen kann und Ihrem Unternehmen durch meine Erfahrung zahlreiche Vorteile biete, entnehmen Sie bitte meinen ausführlichen und angehängten Bewerbungsunterlagen.

Ich freue mich, wenn ich mich Ihnen noch einmal persönlich vorstellen kann.

Mit freundlichen Grüßen,

Viktoria Henschel

The bottom of the window shows a contact card for Viktoria Henschel and a status bar with two icons.



Papierkorb - derhelddestages... Offene Anmeldung für Se... X

Datei Bearbeiten Ansicht Navigation Nachricht Termine und Aufgaben Extras Hilfe

Abrufen Verfassen Chat Adressbuch Schlagwörter Schnellfilter Suchen <Strg+K>

Von Clotilda Herrick <clotilda_herrick@blog.blogcatalog.com> ☆

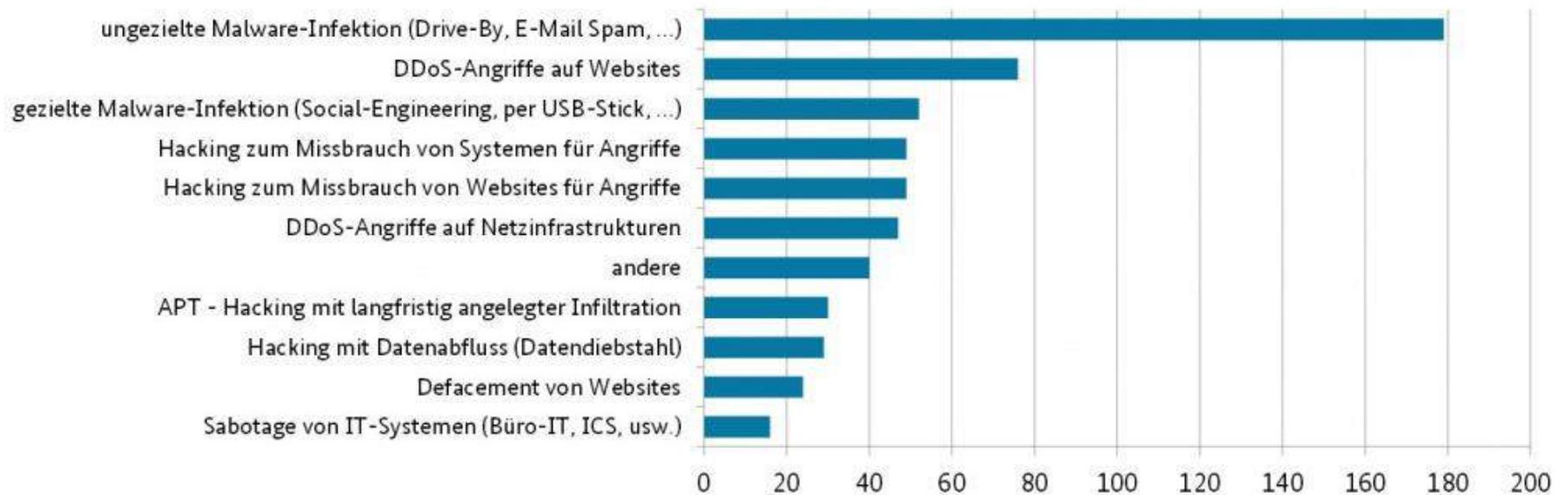
Betreff **Offene Anmeldung für Sexkontakte**

An Mich <derhelddestages@gmx.de> ☆

Bisexuelle Frau und ihre Freundin suchen einen Sexpartner.
Wir warten auf die Nachricht vom liebeshungrigen Mann.

[Hier ist unser Profil. Schreibe uns!](#)

Von 248 Befragten gaben ... folgende Arten von Angriffen an



Quelle: Cyber-Sicherheits-Umfrage 2015, Ergebnisse, Stand 05.10.2015



Mitglieder:

- Expertenkreis Cyber-Sicherheit
- Expertenkreis Internetbetreiber (ISP)
- Expertenkreis IT-Forensik



Handlungsanleitung für den **Umgang** mit sensiblen **Daten** erarbeiten.

Gefährdungslage in den Blick aller Mitarbeiter rücken.

Fremddaten.

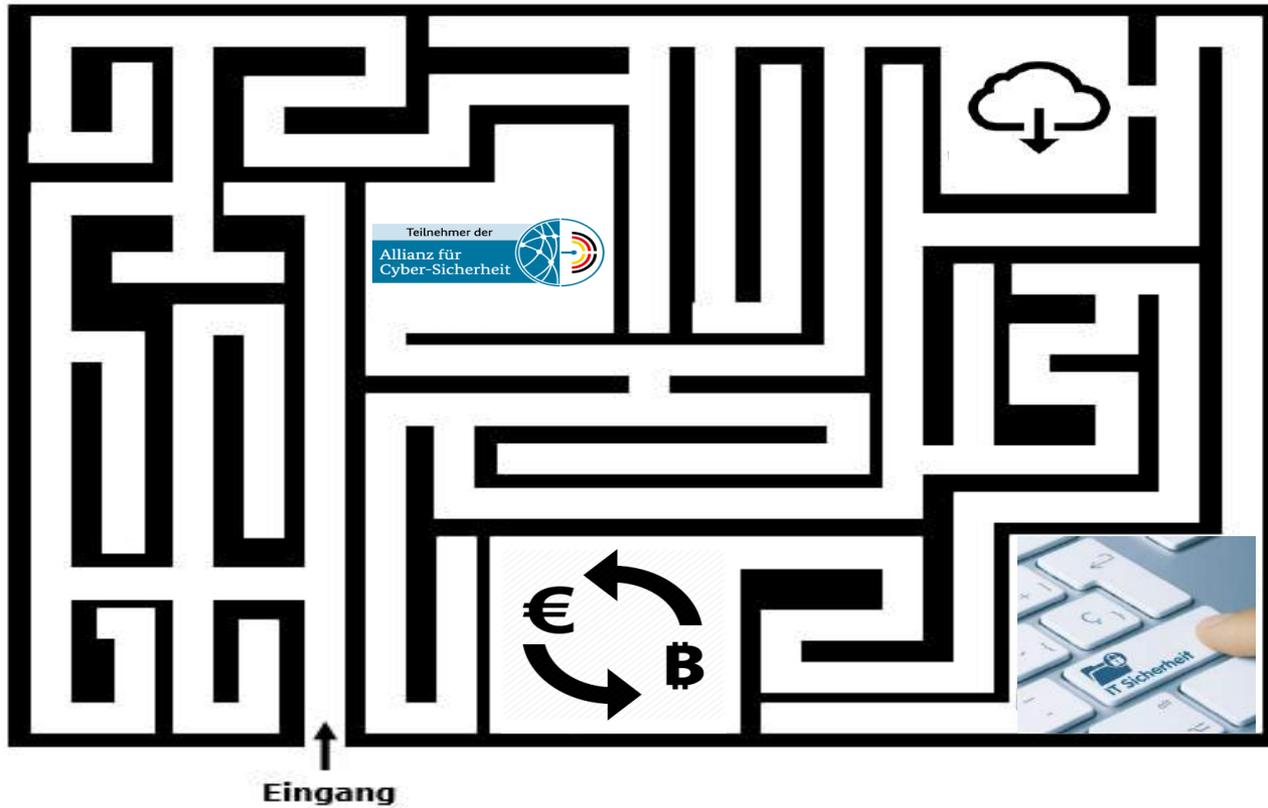
Unbefugten **Zugriff** sichern.

Fernzugänge kontrollieren.

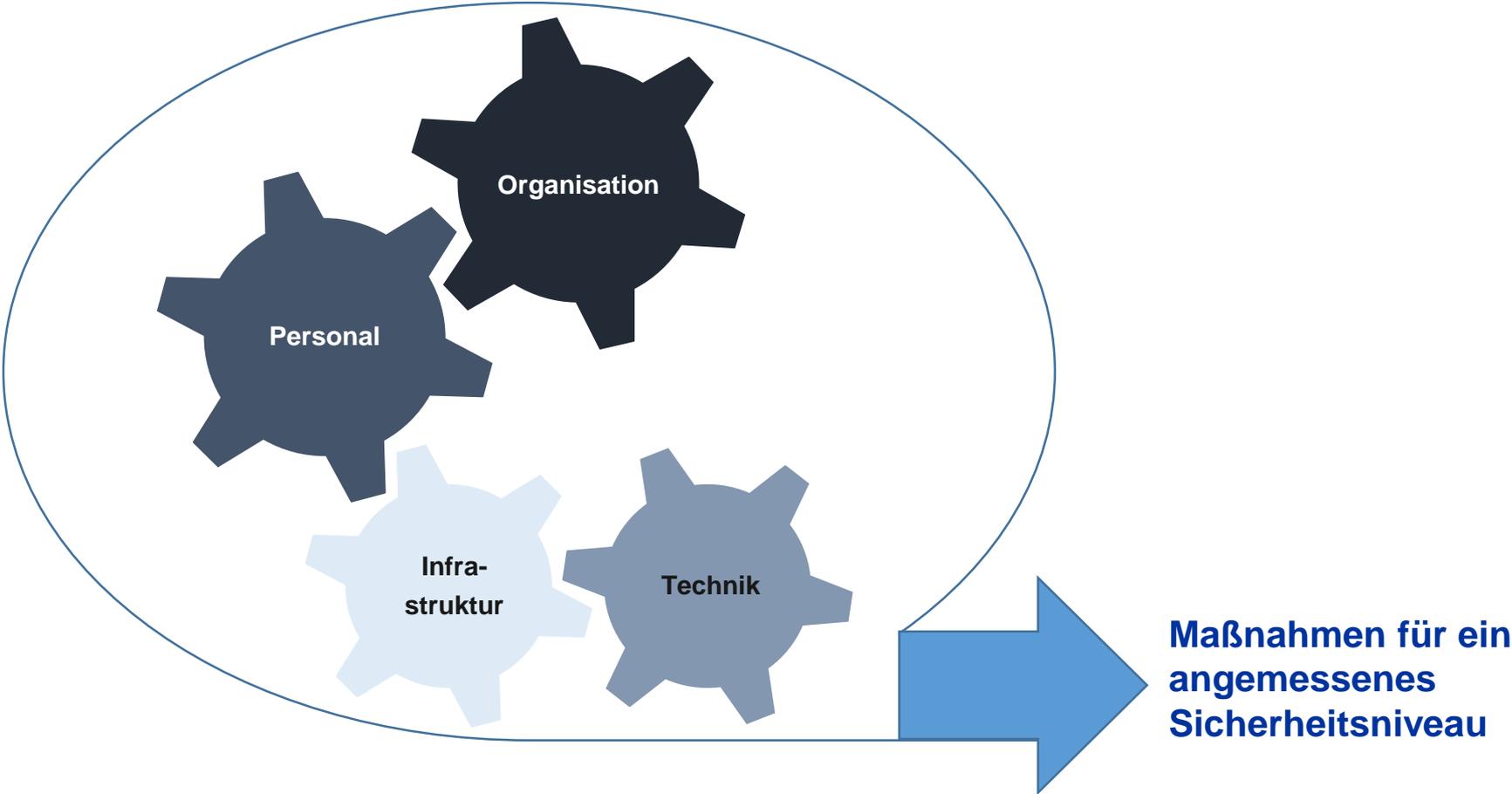
Schutzkonzept erarbeiten, **Richtlinien** dokumentieren.

Verschlüsselungsalgorithmen dem **Stand der Technik** anpassen.

Road Map



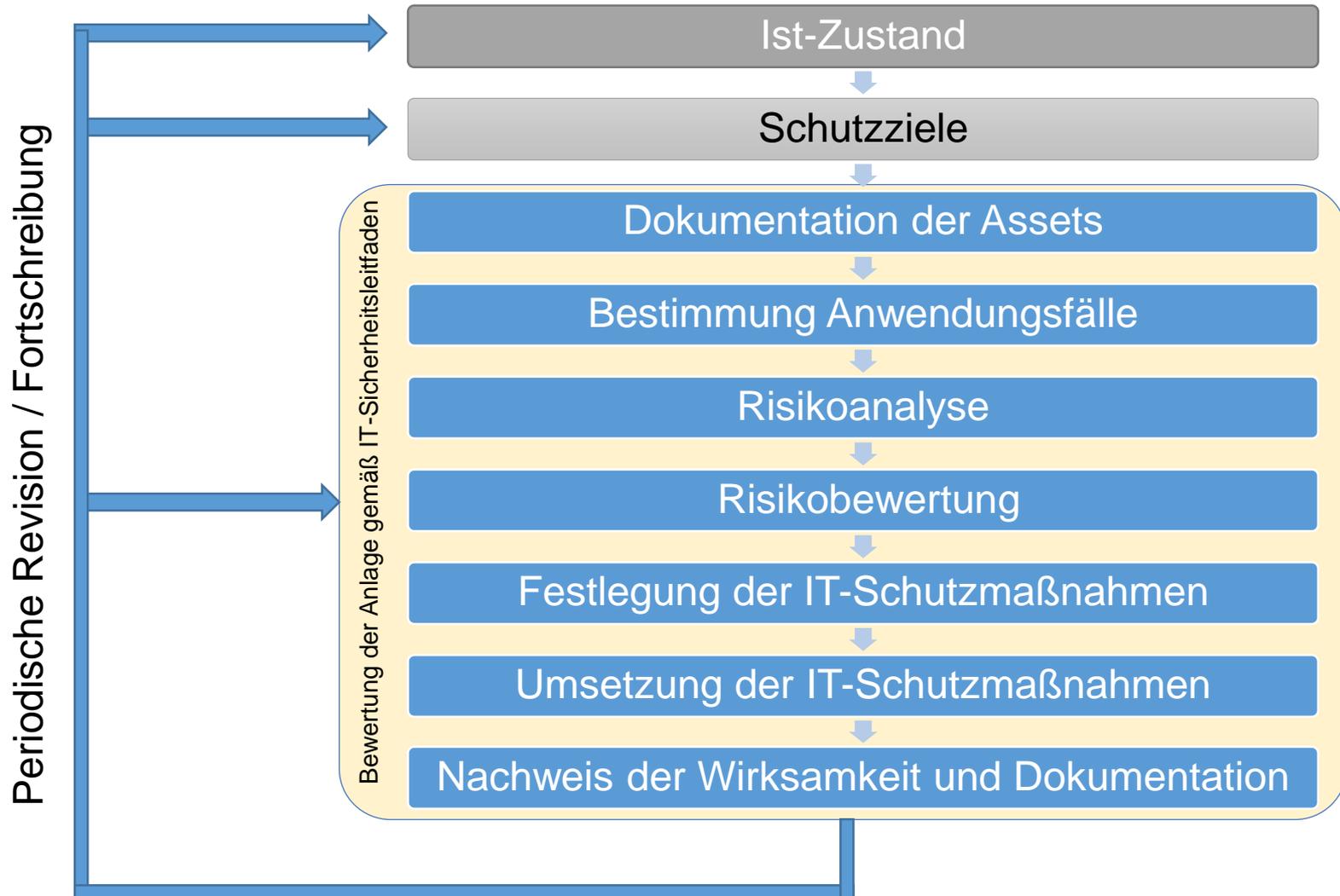
Aufgabenfelder IT Sicherheitsbetrachtung



03/2015	DIN ISO/IEC 27001
25.07.2015	IT-Sicherheitsgesetz
03.05.2016	BSI KRITIS-Verordnung
2017	DVGW-/DWA Branchenstandard DWA-M 1060

„IT-Sicherheit Branchenstandard Wasser/Abwasser“

03.05.2018	IT Grundschutz nach dem Stand der Technik
2020	Evaluierung, Prüfung der Regelungen



- Passwort richtig wählen
- wechseln



Rank	Password
1	123456
2	password
3	12345
4	12345678
5	qwerty
6	123456789
7	1234
8	baseball
9	dragon
10	football

Variante I (deaktivieren)

- ▶ Nicht benötigte Schnittstellen deaktivieren/USB-Ports blockieren (USB-Stecker mit Schloss, Heißkleber).
- ▶ Nur ein(ige) PC(s) bleiben offen, um Zugriff zu ermöglichen.

Variante II (einschränken)

- ▶ Auf den Rechnern Zusatzsoftware installieren.
- ▶ USB-Drives scannen und zertifizieren.
- ▶ Auf den Automatisierungssystemen Treiber installieren, die nur zertifizierte USB-Drives zulassen.
- ▶ Alle PC(s) bleiben offen, es können nur vorher geprüfte und freigegebene USB-Drives verwendet werden.

Ziel: automatisierte Abwehr von Angriffen

- ▶ Firewall- und Angriffserkennungssystem
- ▶ Verschlüsselungskomponenten, zum Betrieb eines Virtuellen Privaten Netzes (VPN)

**Der Weg zur IT Sicherheit:
Angriffsflächen reduzieren!**



Werden Sie kein Opfer!!

Fragen Sie die Spezialisten....



john becker ingenieure
Am Hörenberg 1
27726 Worpswede
Tel. 04792 9310-0
wirberaten.de