Bundesamt
für Sicherheit in der
Informationstechnik

Zusammenarbeit im Bedrohungsfall

Allgemein Bedrohungslage

Produktionsausfall

Phishing

Ransomware

DoS

APT

Bedrohungen

...

CEO Fraud

Schwachstellen

Hacking

Reputationsschäden

Kosten

Bundesamt
für Sicherheit in der
Informationstechnik

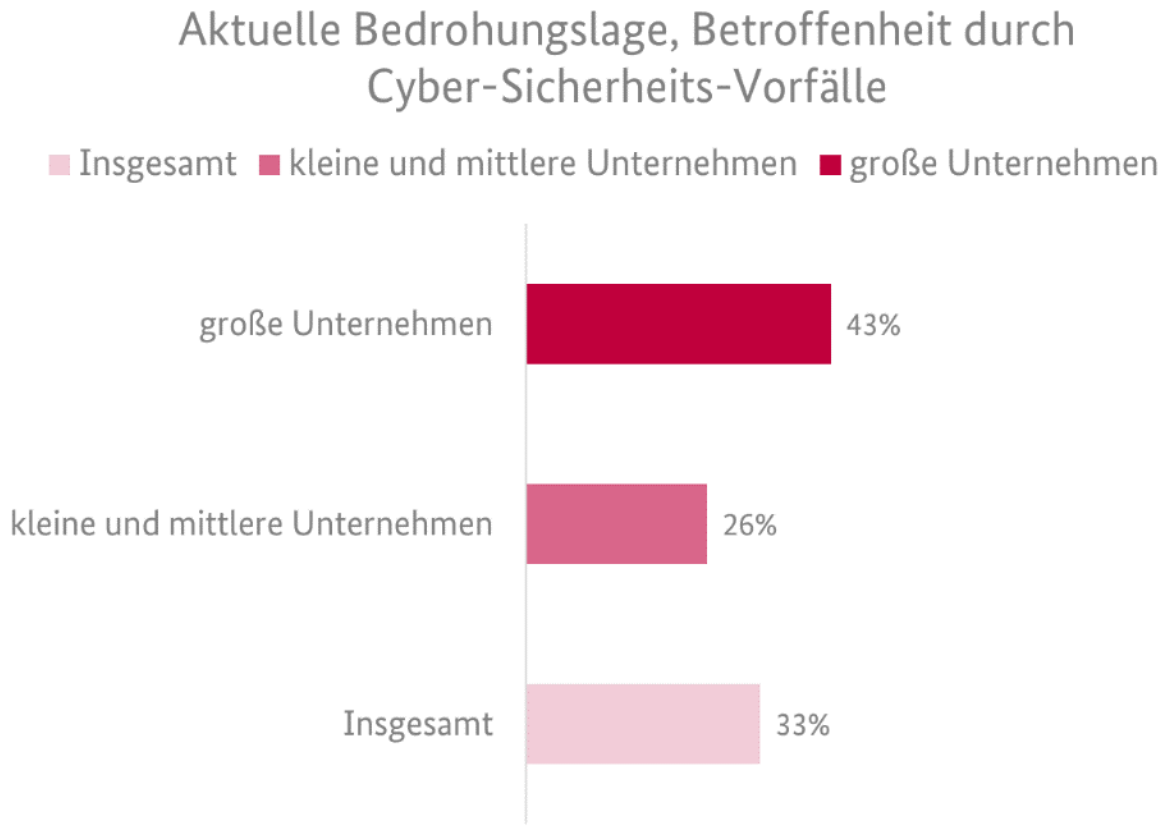
Betroffenheit durch Angriffe

Große Unternehmen am stärksten von Cyber-Sicherheits-Vorfällen betroffen

Unter den befragten Organisationen gaben 43 % der großen Unternehmen an, 2018 von Cyber-Sicherheits-Vorfällen betroffen gewesen zu sein. Bei den kleinen und mittelständischen Unternehmen lag der Wert bei 26%.

In der Hälfte der Fälle waren die Angreifer erfolgreich, d. h. sie konnten sich zum Beispiel Zugang zu IT-Systemen verschaffen, deren Funktionsweise beeinflussen oder Internet-Auftritte von Firmen manipulieren.

Hinweis: In der Regel wird nur ein Teil der Angriffe erkannt, daher sind nur detektierte Vorfälle berücksichtigt.

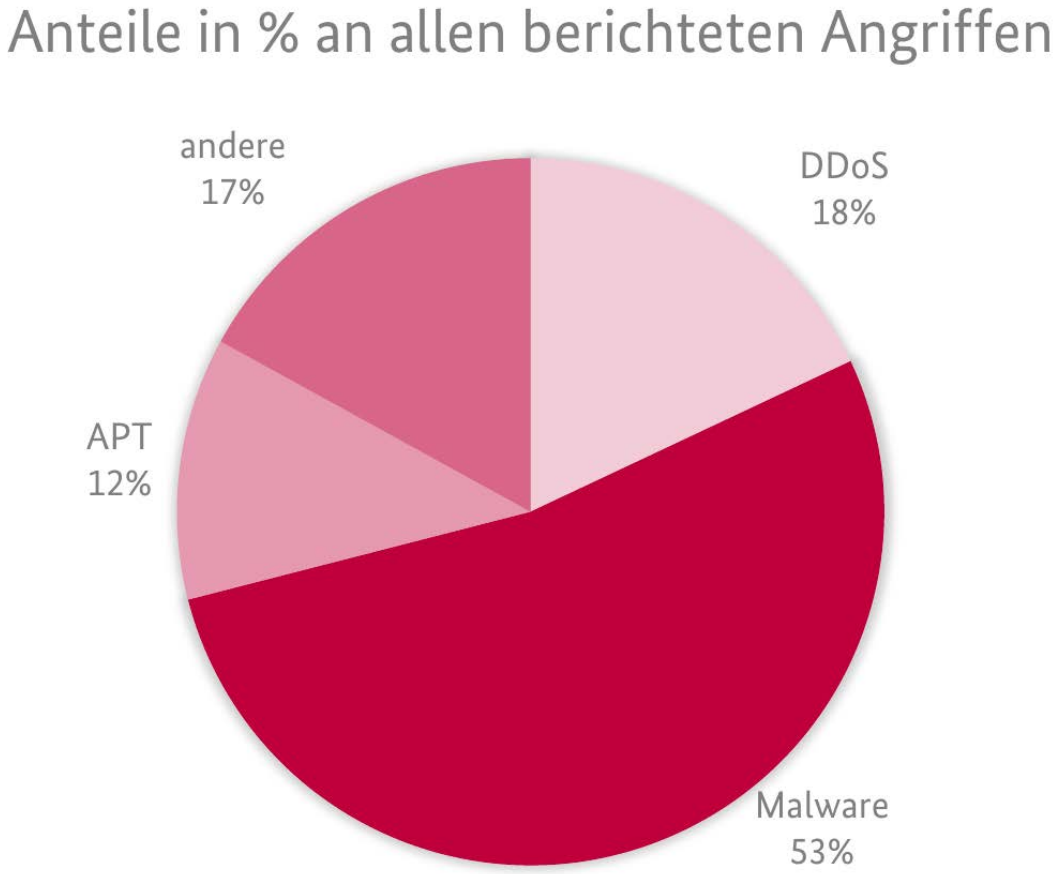


Art der Angriffe

Malware auch 2018 wieder die häufigste Angriffsart
In 53% der berichteten Angriffsfälle handelte es sich um Malware-Infektionen, bei denen Schadprogramme in betriebliche IT-Systeme eindrangen (DDoS-Attacken 18%,gezieltes Hacking 12%).

90% der Schadprogramme wurden als Anhang oder Link in einer E-Mail verteilt.

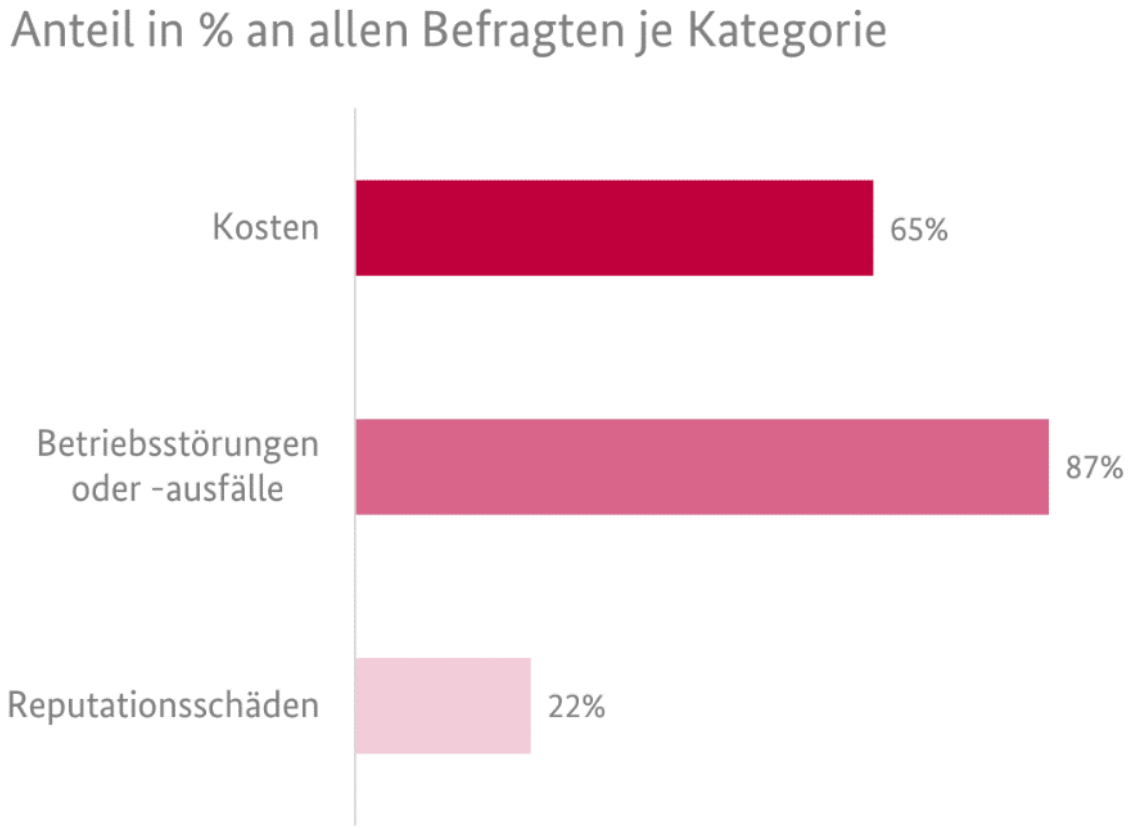
In der Hälfte der Fälle verhinderten technische Maßnahmen eine Infektion, in den übrigen Fällen war die Awareness der Beschäftigten derErfolgsfaktor.



Art der Schäden durch erfolgreiche Angriffe

Cyber-Angriffe hatten erhebliche Konsequenzen für die Betriebe
So gaben 87% der Betroffenen an, dass es 2018 zu Betriebsstörungen oder –ausfällen kam.

Hinzu kamen häufig noch Kosten für die Aufklärung der Vorfälle und die Wiederherstellung der IT-Systeme (bei 65% der Betroffenen) sowie Reputationsschäden (bei 22%der Betroffenen).



IT

Betreiber

Dienstleister

Rollen

OT

Instandhaltung

Hersteller

Integrator

Bundesamt
für Sicherheit in der
Informationstechnik

Beispiel Norsk Hydro

März 2019: Norsk Hydro - Ransomware

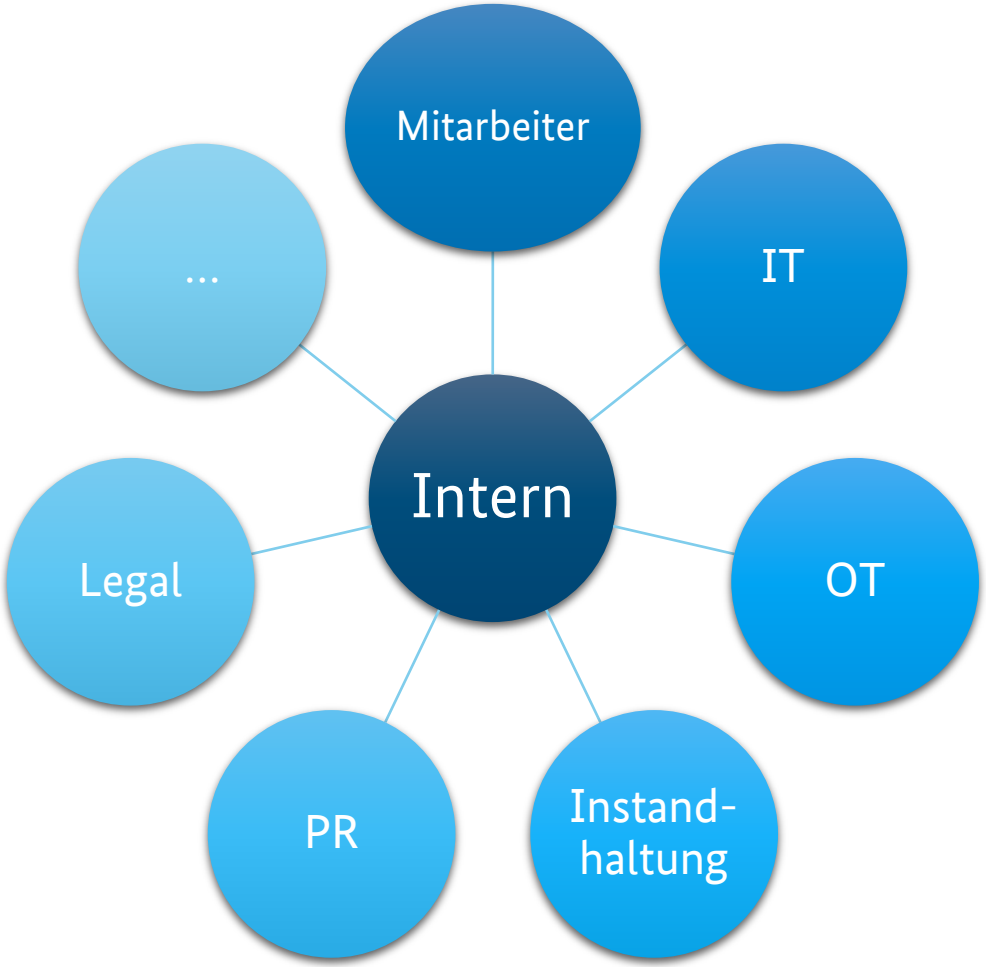
19.3.2019	Entdeckung des Angriff in den USA.
Nachts	IT Organisation koppelt Produktionsstandorte vom Firmennetzwerk ab, informiert die Anwender ihre PCs nicht einzuschalten.
8:31	Information der Finanzmärkte, Börse OSLO.
Vormittags	Temporärer Webauftritt auf Microsoft Azure mit Informationen für Investoren geschaltet.
	Norsk Hydro informiert über den Angriff auf Facebook.
14:41	Update zum Angriff mit Status zur Produktion.
15:00	Pressekonferenz, mit der norwegischen Sicherheitsbehörde.

Exzellentes Krisenmanagement verhindert Zusammenbruch der Produktion und Auswirkungen auf den Aktienkurs.

Hydro

Pressekonferenz 19.3.2019, 15:00 Uhr
Finanzvorstand Eivind Kallevik:
"Let me be clear! The situation for Hydro through this is quite severe. The entire worldwide network is down, affecting our production and our office operations. There is a lack of ability to connect to production systems, causing some production challenges and temporary stoppages at several plants.“ [1]

Beziehungen

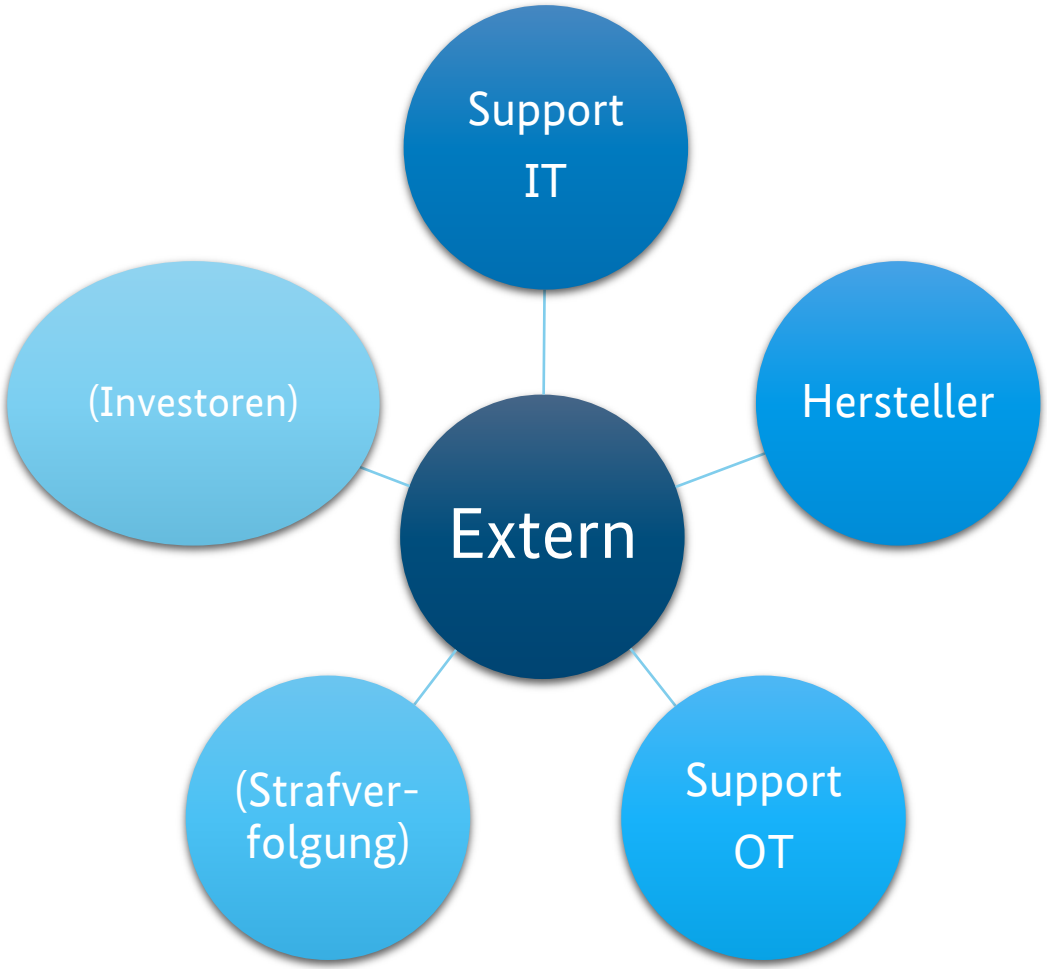


Beispiel TRITON

August 2017: Petro Rabigh
Angriff auf Sicherheitsteuerung, Triton

2014	Angreifer kompromittieren das Petro Rabigh Firmennetz[1]
Juni 2017	Schneider Electric Techniker untersuchen scheinbare Fehlfunktion in der Triconex Sicherheitssteuerung. Keine Probleme gefunden, Produktion wurde wieder angefahren.[2]
4.8.2017 7:43	Zwei Triconex SIS fahren Teile des Petro Rabigh Komplexes herunter um eine Gasexplosion zu vermeiden. Operator im Kontrollraum bemerken nichts vom Shutdown! [2]
14.8.2017	Pressemitteilung: Kurzer Ausfall im Petro Rabigh Komplex beendet. [2]

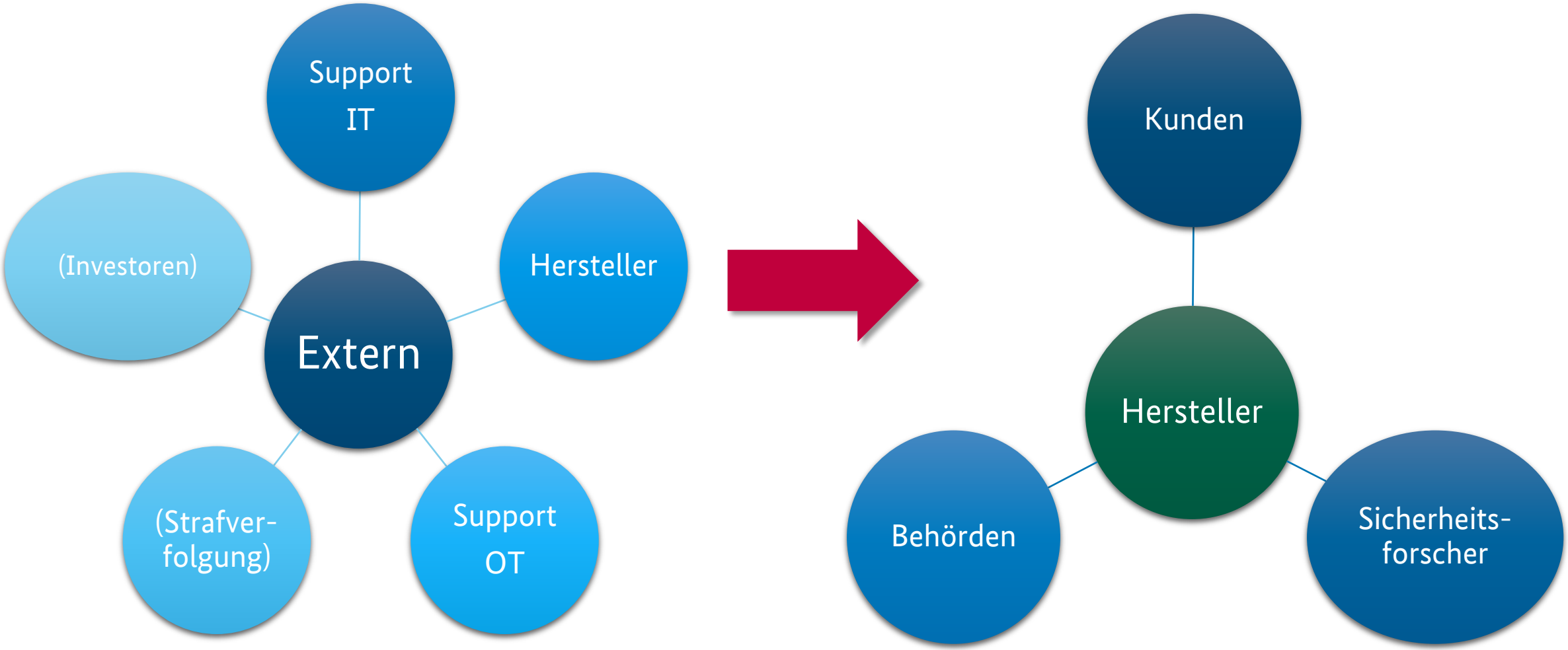
Beziehungen



August 2017: Petro Rabigh
Angriff auf Sicherheitsteuerung, Triton

2014	Angreifer kompromittieren das Petro Rabigh Firmennetz[1]
Juni 2017	Schneider Electric Techniker untersuchen scheinbare Fehlfunktion in der Triconex Sicherheitssteuerung. Keine Probleme gefunden, Produktion wurde wieder angefahren.[2]
4.8.2017 7:43	Zwei Triconex SIS fahren Teile des Petro Rabigh Komplexes herunter um eine Gasexplosion zu vermeiden. Operator im Kontrollraum bemerken nichts vom Shutdown! [2]
14.8.2017	Pressemitteilung: Kurzer Ausfall im Petro Rabigh Komplex beendet. [2]
14.12.2017	Fireeye/Dragos veröffentlichen erste Analyse.[3]
4.5.2018	Schneider Electric veröffentlicht Schwachstellen CVE-2018-7522[4] und CVE-2018-8872[5].

Beziehungen



August 2017: Petro Rabigh - Folgen

Lokal

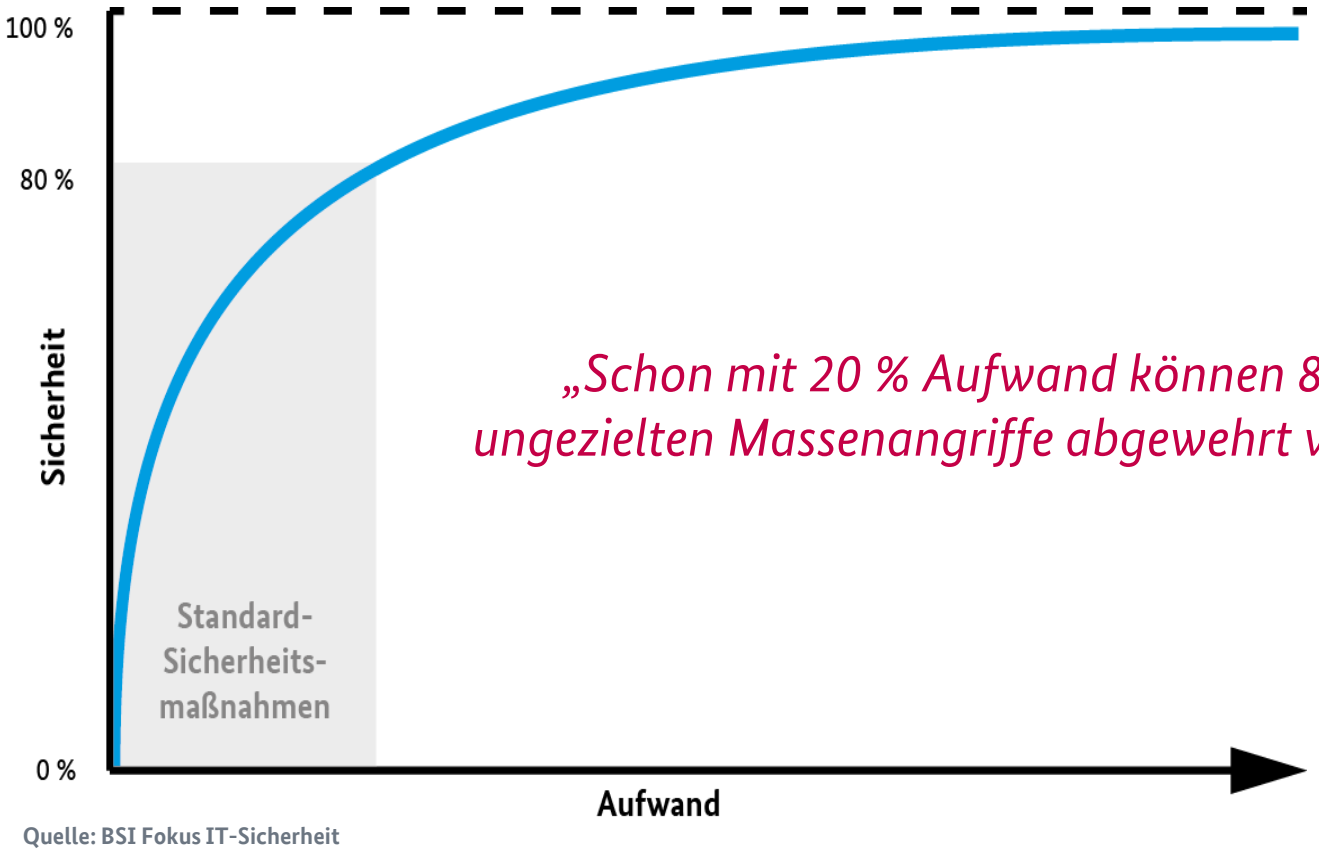
- Keine nennenswerten finanziellen Einbußen.
- Keine Pressemitteilungen zur ungeplanten Abschaltung.
- Knappe Mitteilung zum Wiederanfahren des Anlagenkomplexes am 14. August 2017.

Weltweit

- Untersuchung der betroffenen Schneider Electric Sicherheitssteuerungen.
- Umsetzen von Sofortmaßnahmen.
- Patchen der Sicherheitssteuerungen.
- Untersuchung der Produktionsnetzwerke.

Kernpunkte

Vorbereitung



Quelle: BSI Fokus IT-Sicherheit

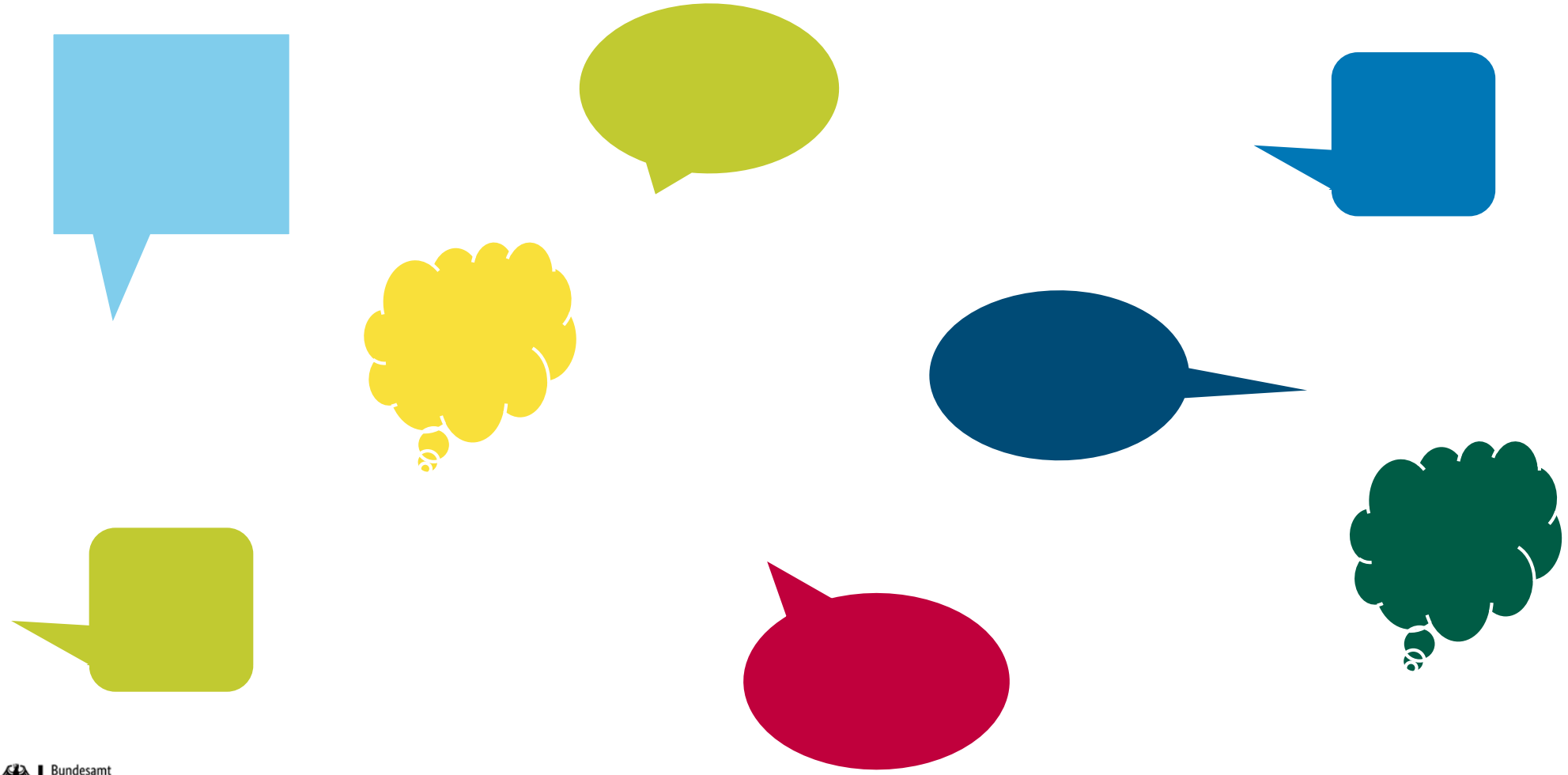
„Schon mit 20 % Aufwand können 80 % der ungezielten Massenangriffe abgewehrt werden“

Hundertprozentige Sicherheit ist auch mit noch so hohem Aufwand nicht zu erreichen.

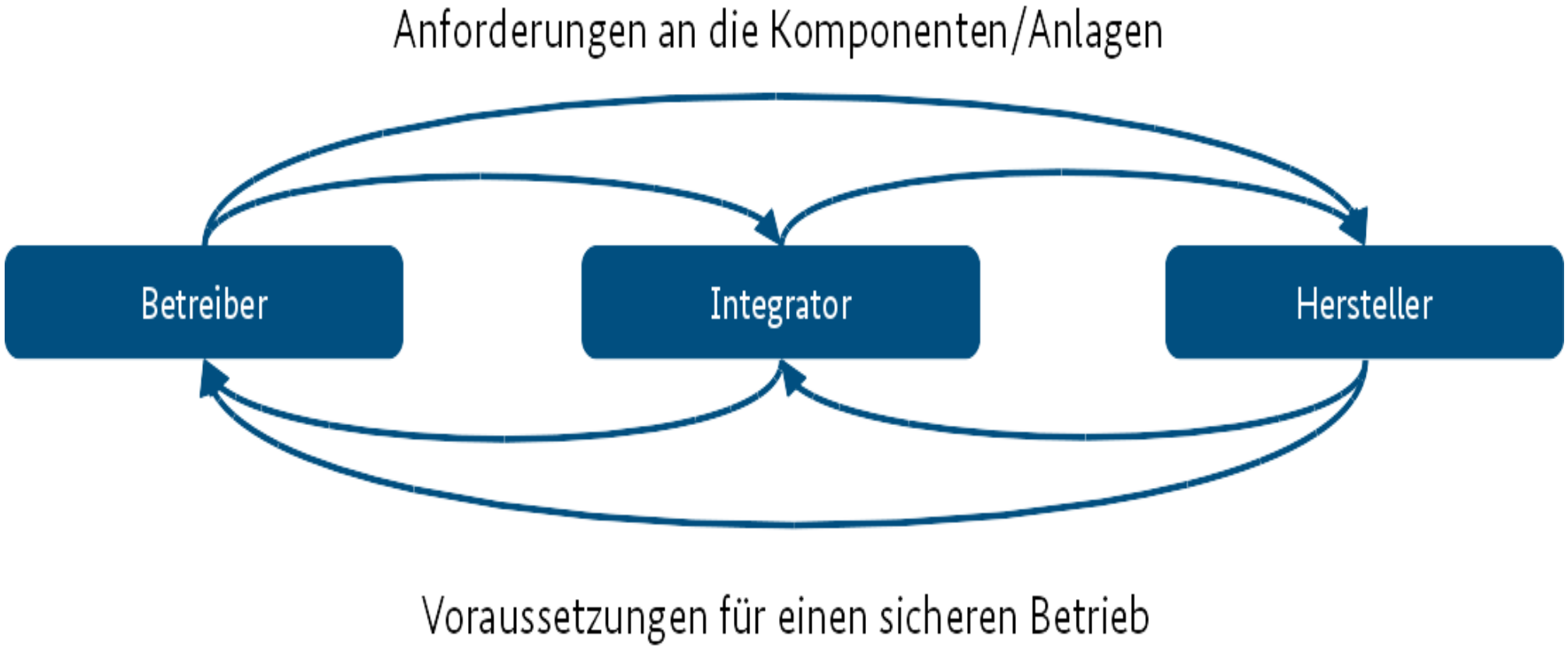
Mit überschaubarem Aufwand kann jedoch ein Großteil der Angriffe abgewehrt werden.

Lediglich ein niedriger Prozentsatz der Angriffe – u.a. die besonders ausgeklügelten und individualisierten APT – erfordern darüber hinausgehende maßgeschneiderte Maßnahmen

Kommunikationswege und –partner festlegen



Zusammenarbeit



Verantwortung in Wertschöpfungsnetzwerken

Hersteller
- Entwicklung und Angebot
- von sicheren Komponenten

Integratoren/Maschinenbauer
- Auswahl von sicheren Komponenten
- Nutzung von IT-Sicherheitsmechanismen
- sichere Konzeption & Services

Betreiber
- Sensibilität & Meldung von Vorfällen
- Einfordern von IT-Sicherheit bei der Beschaffung

Fazit

Start
- Quick Wins / Cyber Hygiene
- Grundlagen schaffen

Der Weg
- Größere Maßnahmen in Angriff nehmen
- Vorbereitung für ISMS

Ziel
- ISMS aufbauen, betreiben
- Auf Grundlage von ISO 27001, IEC 62443, BSI IT-Grundschutz

Prämisse

- !! Schlanke und verständliche Prozesse.
- !! Sinnvolle Dokumentation.

Vielen Dank für die Aufmerksamkeit!

Kontakt

Bundesamt für Sicherheit in der Informationstechnik
Referat TK 15 Industrielle Automations- und Steuerungstechnik
Godesberger Allee 185-189
53175 Bonn

Ansprechpartner
Hr. Jens Mehrfeld
jens.mehrfeld@bsi.bund.de
www.bsi.bund.de
Tel. +49 228 99 9582 5936
Fax +49 228 9910 9582 5936

Zertifikat seit 2010
audit berufundfamilie

Bundesamt
für Sicherheit in der
Informationstechnik