Was haben wir aus KRITIS gelernt?

Angriffe gegen kritische Infrastrukturen

Philipp Neumann

Über mich

Philipp Neumann

Senior Consultant

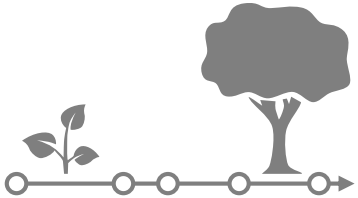
Seit 2015 in der Informationssicherheit tätig:

- Langjährige Erfahrung im Bereich Managementsysteme
- Berät und begleitet Unternehmen bei der Einführung von ISMS
- Spezialthema: GRC-/ISMS-Tools

Zertifizierungen:

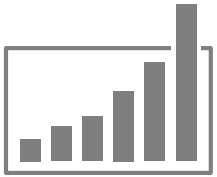
- Lead Implementer gem. ISO 27001
- Zusätzliche Prüfverfahrens-Kompetenz für § 8a BSIG
- IHK-Sachkunde § 34a GewO

Zahlen, Daten und Fakten

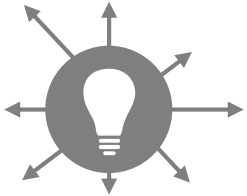


Langjährige Erfahrung
Seit 1992 aktiv

Kompetentes Personal
Über 150 Mitarbeiter



Kontinuierliches Wachstum
17 Mio. € Jahresumsatz



Vielfältige Kompetenzen
620 Projekte bei 350 Kunden

Unsere Standorte

Agenda

1. Erfolgte Angriffe
2. Regularien
3. Umsetzung von KRITIS
4. Umsetzung mit verinice?
5. Schlussfolgerung

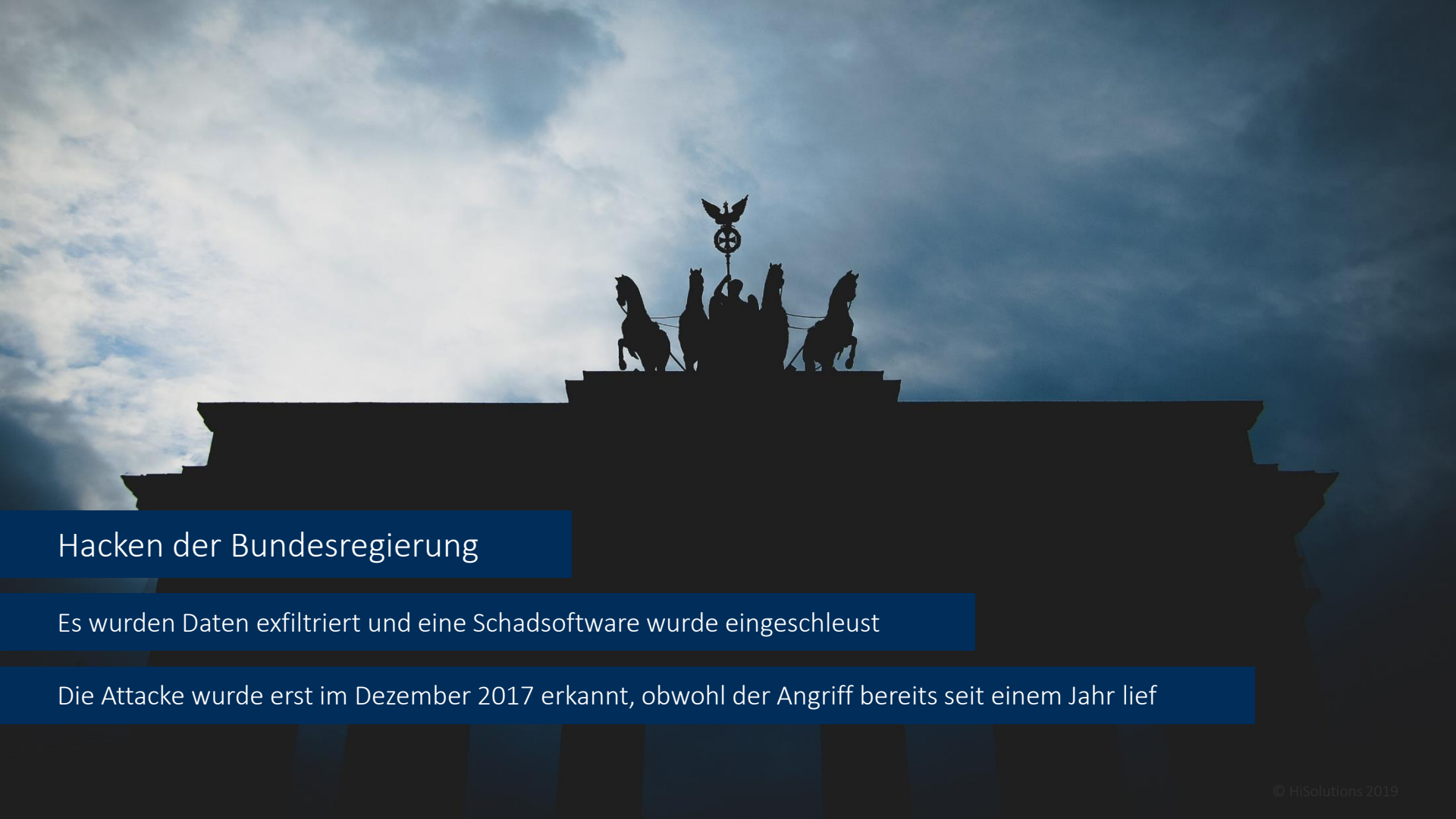
1. Erfolgte Angriffe

Dezember 2015 | Attacken auf das Ukrainische Stromnetz

Auswirkungen: ca. 250.000 betroffene Personen in Kiew und dem Umfeld

Cyber-Angriffe auf deutsche Energieversorger

2017 und 2018 erfolgte eine Reihe großangelegter weltweiter Cyber-Angriffskampagnen



Hacken der Bundesregierung

Es wurden Daten exfiltriert und eine Schadsoftware wurde eingeschleust

Die Attacke wurde erst im Dezember 2017 erkannt, obwohl der Angriff bereits seit einem Jahr lief

2. Regularien

Regularien in Deutschland

- Regulierung für kritische Infrastrukturen begann 2015
- Ziel: Sicherheit der IT-Komponenten von kritischen Infrastrukturen
- Rechtlich verbindlich ab einer Versorgung von mindestens 500.000 Bürgern
- Betreiber in sieben Sektoren müssen ihre IT-Sicherheit nachweisen

KRITIS Sektoren

Korb 1

Deadline Mai 2018
(Energie im Januar 2018)

Energie

IT und TK

Wasser

Ernährung

Korb 2

Deadline Juni 2019

Transport u.
Verkehr

Finanz- und
Versicherungs-
wesen

Gesundheit

Fristen gemäß BSI-KritisV

	Korb 1	Korb 2
		
Maßnahmen	**Fristen**	
Umsetzung der Maßnahmen nach § 8a BSIG & Durchführung der Prüfung	ab sofort	
Lieferung der Nachweise an das BSI	Mai 2018	Juni 2019
Einrichtung einer Kontaktstelle nach § 8b BSIG	November 2016	Dezember 2017

Rechtliche Grundlagen für KRITIS-Betreiber

Grundlage	Inhalt
§ 2 Absatz 10 BSIG	Festlegung der KRITIS-Sektoren & Definition Kritische Infrastrukturen
§ 8a BSIG	IT-Sicherheit in Kritischen Infrastrukturen
§ 8b BSIG	Melde- und Informationswesen
§ 8d BSIG	Abgrenzung des Anwendungsbereich
§ 8e BSIG	Auskunftsverlangen bei KRITIS-Daten
§ 1 BSI-KritisV	Begriffsbestimmungen
§§ 2-5 BSI-KritisV	Definition der Sektoren aus Korb I
§§ 6-8 BSI-KritisV	Definition der Sektoren aus Korb II
Anhänge BSI-KritisV	Anlagenkategorien und Schwellenwerte

Ermittlung des Geltungsbereichs

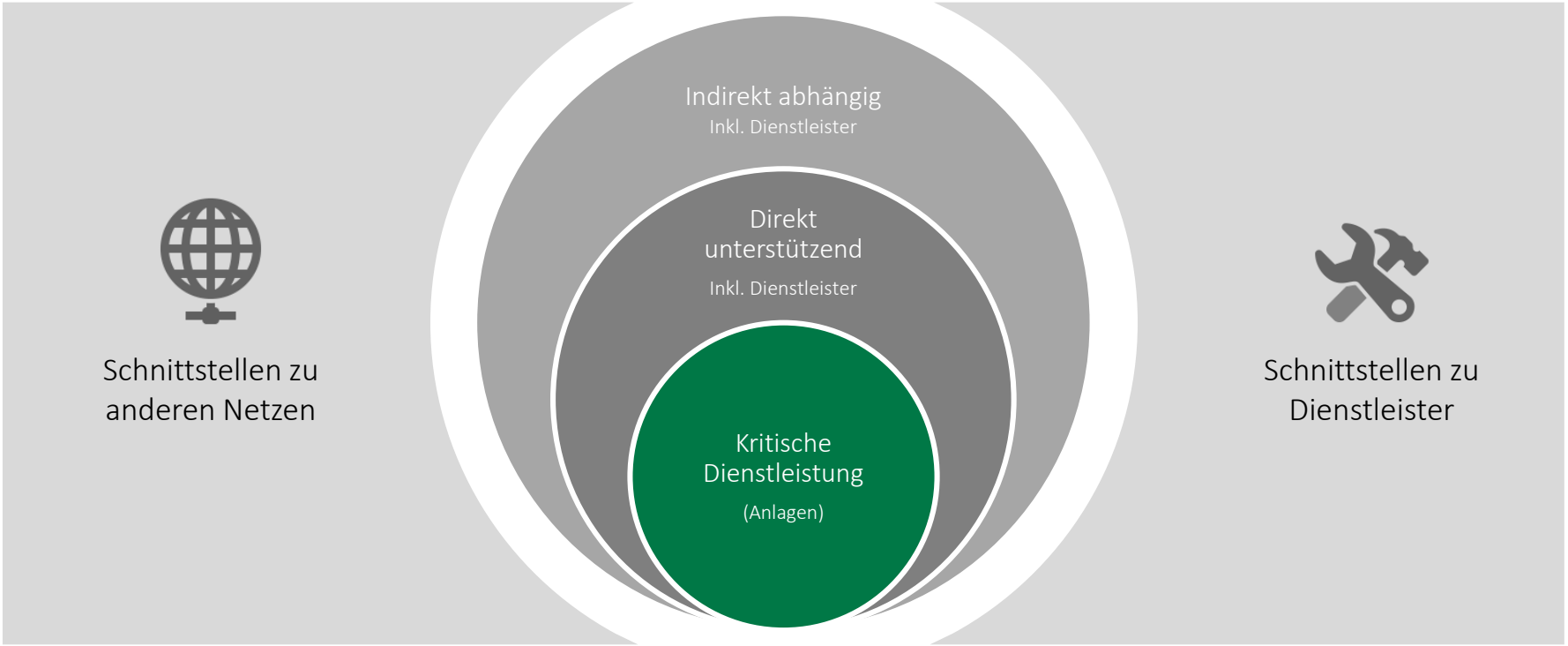
Regelung für Kleinstunternehmen: Mehr als
10 Mitarbeiter oder mehr als 2 Millionen € Jahresumsatz?
[§ 8d Absatz 1 BSIG]

Werden Anlagen zur Erbringung einer kritischen Dienstleistung betrieben?
[§ 2 Absatz 10 BSIG]

Werden kritische Dienstleistungen durch externe Dienstleister erbracht, auf deren Beschaffenheit und Betrieb ein bestimmender Einfluss vorliegt?
[§ 1 BSI-KritisV]

Liegt der Versorgungsgrad dieser Anlagen über den definierten Schwellenwerten?
[Anhänge BSI-KritisV]

Darstellung des Geltungsbereichs (Scoping)



3. Umsetzung von KRITIS

KRITIS – Unterschiede zu anderen Sicherheitsstandards

- KRITIS dient primär dem Schutz der Bevölkerung, nicht des Betreibers.
- Ergebnis der KRITIS Prüfung ist kein Zertifikat, sondern eine Mängelliste mit Sicherheitsmängeln, die zu beheben sind.
- KRITIS prüft die Umsetzung von Sicherheitsanforderungen, nicht deren Planung.

KRITIS – Unterschiede zu anderen Sicherheitsstandards

- KRITIS setzt kein zertifiziertes ISMS voraus! Es muss ein geeignetes ISMS Managementsystem verwendet werden, welches auch ein gemeinsames Management System sein kann.

- Es kann je nach Anlagentyp spezielle Anforderungen geben, welche die oben genannte Aussage aufhebt. So können einzelne Aufsichtsbehörden weitere Anforderungen, wie ein zertifiziertes ISMS nach ISO 27001, aufstellen.

„Stand der Technik“

„Stand der Technik“ ist nicht juristisch definiert:

Sollte mehr als „nur übliche“ Maßnahmen sein

Aber weniger als die aktuellen wissenschaftlichen Standards

Als gute Basis dienen bewährte Industriestandards. Die Umsetzung muss auf Grundlage des zu minimierenden Risikos bewertet werden.

Ist alles sicher nach der Umsetzung (1/3)?

Einige Unternehmen aus Korb 1 haben erst ab 2018 mit der Umsetzung begonnen und wurden bis zum Ende der Frist nicht fertig.

- Es zeigten sich oft Mängel in industriellen Steuerungssystemen oder Automatisierungssystemen.
- Diese Mängel können meist erst nach umfangreichen Umbaumaßnahmen behoben werden.

Ist alles sicher nach der Umsetzung (2/3)?

Teilweise haben wir schnell eingeführte ISMS Systeme erlebt, welche nur auf dem Papier existierten und keinen Mehrwert für das Unternehmen hatten.

- IT-Sicherheit erfordert ein Umdenken bei den beteiligten Personen. Dies kann aber nicht von heute auf morgen passieren.

Ist alles sicher nach der Umsetzung (3/3)?

- Systeme müssen durch Regularien immer mehr vernetzt werden.
- Die Anforderungen an die Sicherheit werden nur langsam nachgezogen.

Beispiel Stromversorgung:

Neue Automationssysteme haben oft WLAN und Bluetooth Unterstützung, welche unzureichend abgesichert ist.

Auch bei Korb 2 starten einige Unternehmen erst in 2019

Das Budget wurde in 2018 nicht eingeplant

Die uns bekannten Projekte in den Sektoren Finanzen und Gesundheit starten langsam.

Beispiel Hessen:
Den Krankenhäusern fehlen Gelder für die Umsetzung der Anforderungen. Eine kleine Anfrage an die Regierung hat gezeigt, dass nur ein Bruchteil für IT-Sicherheit geplant wurde.

Vorgehensweise bei einer Prüfung Teil 1

Zusammenstellung des Prüfteams

- Zusammenstellung des Prüfteams seitens HiSolutions

Auftaktgespräch und Erstellung des Prüfplans

- Definition der gemeinsamen Vorgehensweise sowie Erstellung des Prüfplans

Prüfung der Eignung des Anwendungsbereichs

- Überprüfung des Anwendungsbereichs

Vorgehensweise bei einer Prüfung Teil 2

Dokumentenprüfung und Vor-Ort-Prüfung

- Überprüfung der bereitgestellten Dokumente

Nachbereitung der Vor-Ort-Prüfung

- Überprüfung des Prüfgegenstands in Bezug auf die Anforderungen

Erstellung des Prüfberichts

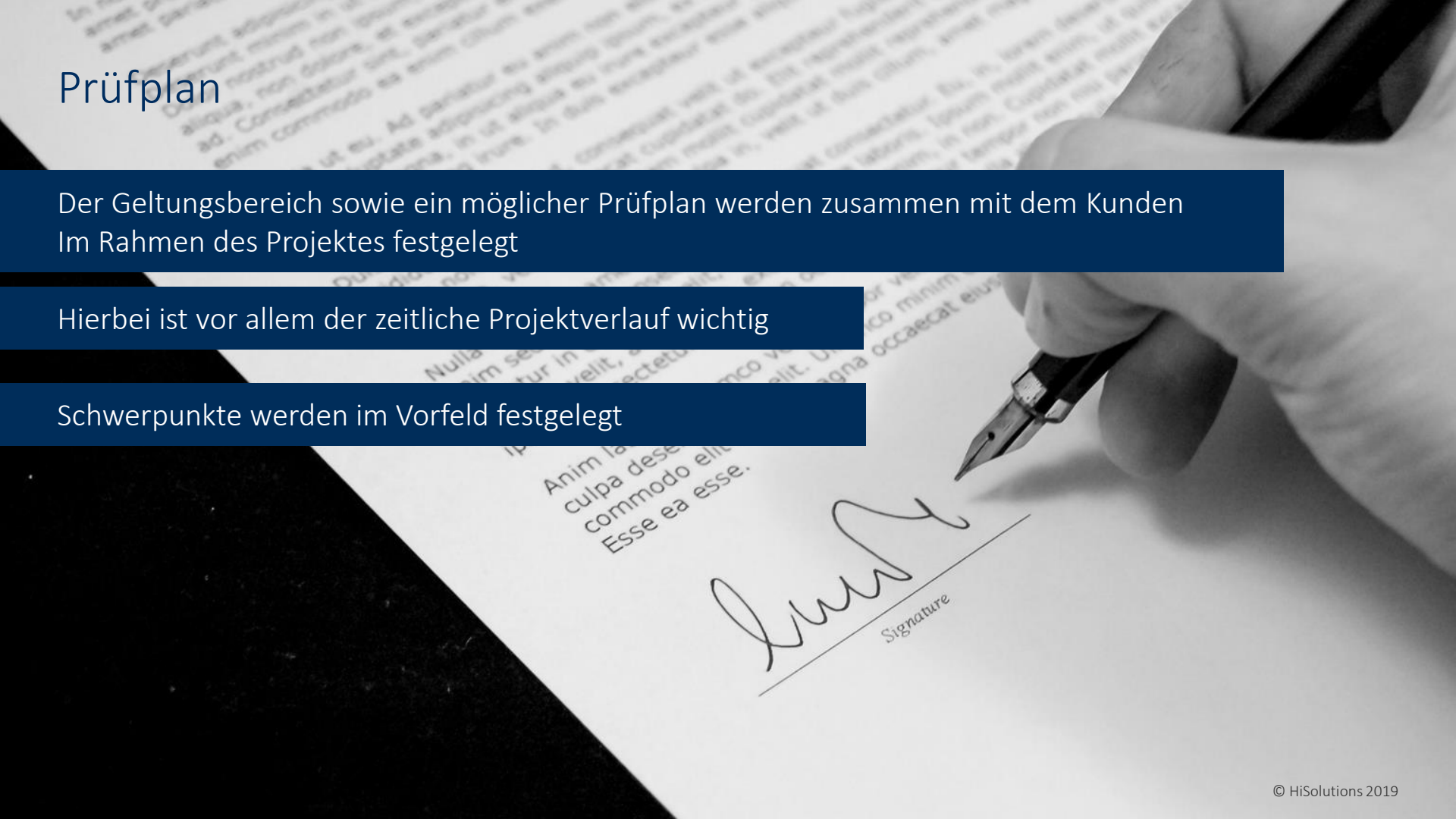
- Bewertung der Feststellungen der Dokumentenprüfung und der Vor-Ort-Prüfung

Prüfplan

Der Geltungsbereich sowie ein möglicher Prüfplan werden zusammen mit dem Kunden Im Rahmen des Projektes festgelegt

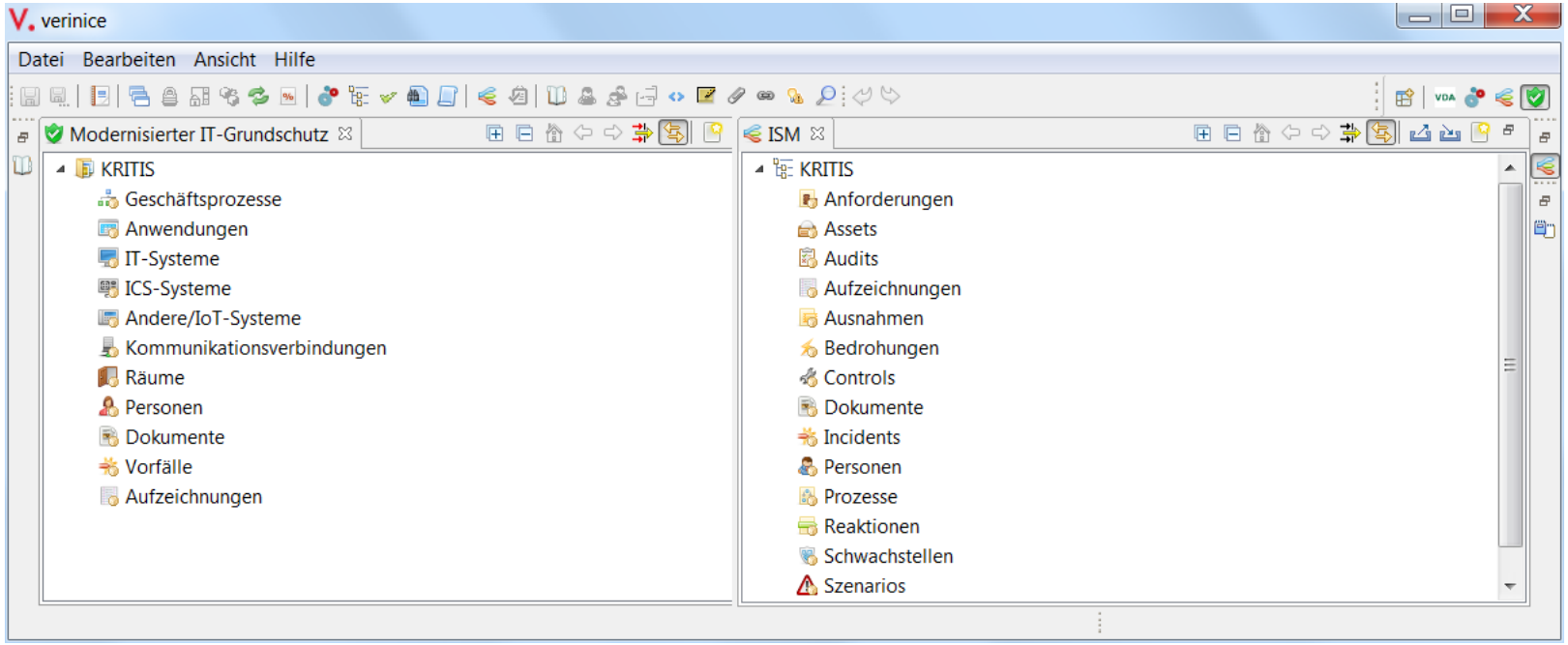
Hierbei ist vor allem der zeitliche Projektverlauf wichtig

Schwerpunkte werden im Vorfeld festgelegt



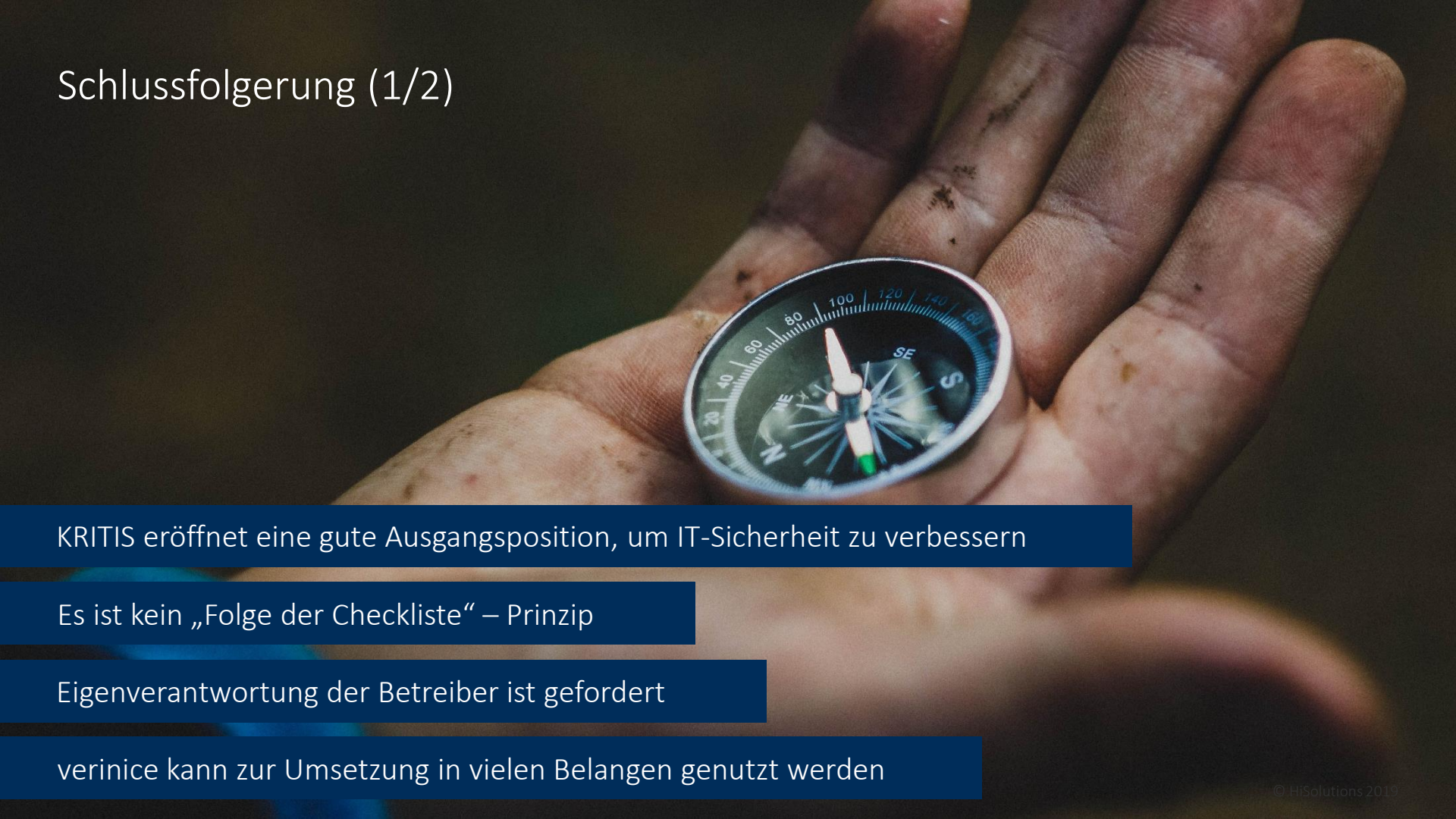
4. Umsetzung mit verinice?

Umsetzung mit verinice?



5. Schlussfolgerung

Schlussfolgerung (1/2)



KRITIS eröffnet eine gute Ausgangsposition, um IT-Sicherheit zu verbessern

Es ist kein „Folge der Checkliste“ – Prinzip

Eigenverantwortung der Betreiber ist gefordert

verinice kann zur Umsetzung in vielen Belangen genutzt werden

Schlussfolgerung (2/2)

KRITIS deckt nur den IT-gestützten Teil der kritischen Infrastrukturen ab!

Beispiel:

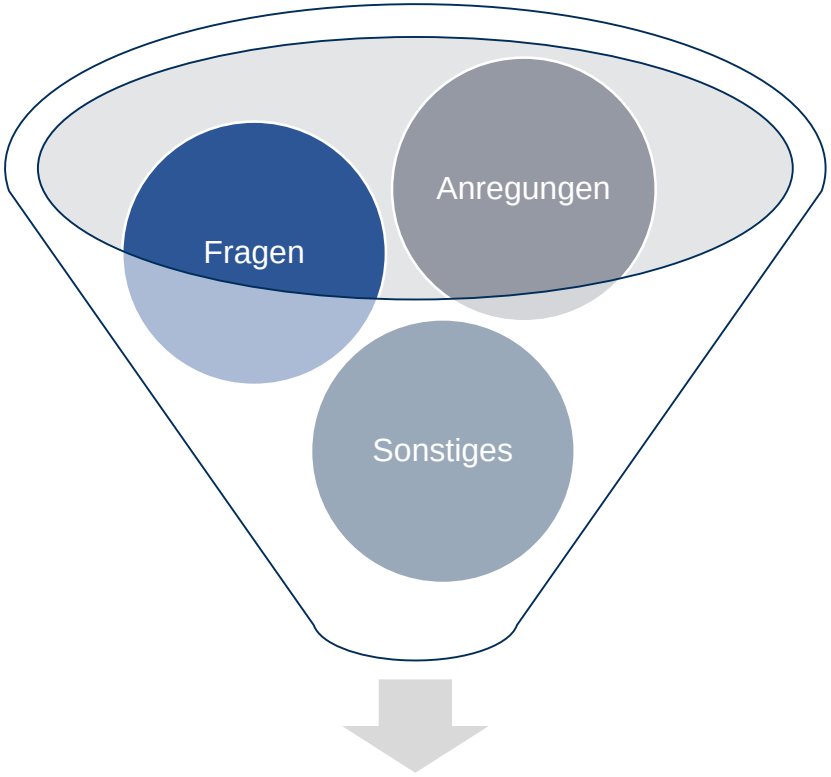
- Wenn die Industrie in Folge von Umwelteinflüssen nicht mehr arbeiten kann, dann fällt dies nicht unter KRITIS!
- Temperaturobergrenzen von 28 Grad für Kühlwasser wurden 2018 vielerorts überschritten. Kraftwerke mussten drosseln oder abgeschaltet werden.

Was Sie aus dieser Präsentation mitnehmen sollten:

1. KRITIS ist ein sinnvoller Ansatz, um die IT-Sicherheit in Unternehmen zu stärken.

2. Er bietet gute Integrationsmöglichkeiten in andere Standards und Normen.

3. KRITIS dient primär dem Schutz der Bevölkerung, nicht der Unternehmen.



Mehrwert

HISOLUTIONS

Bouchéstraße 12 | 12435 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com