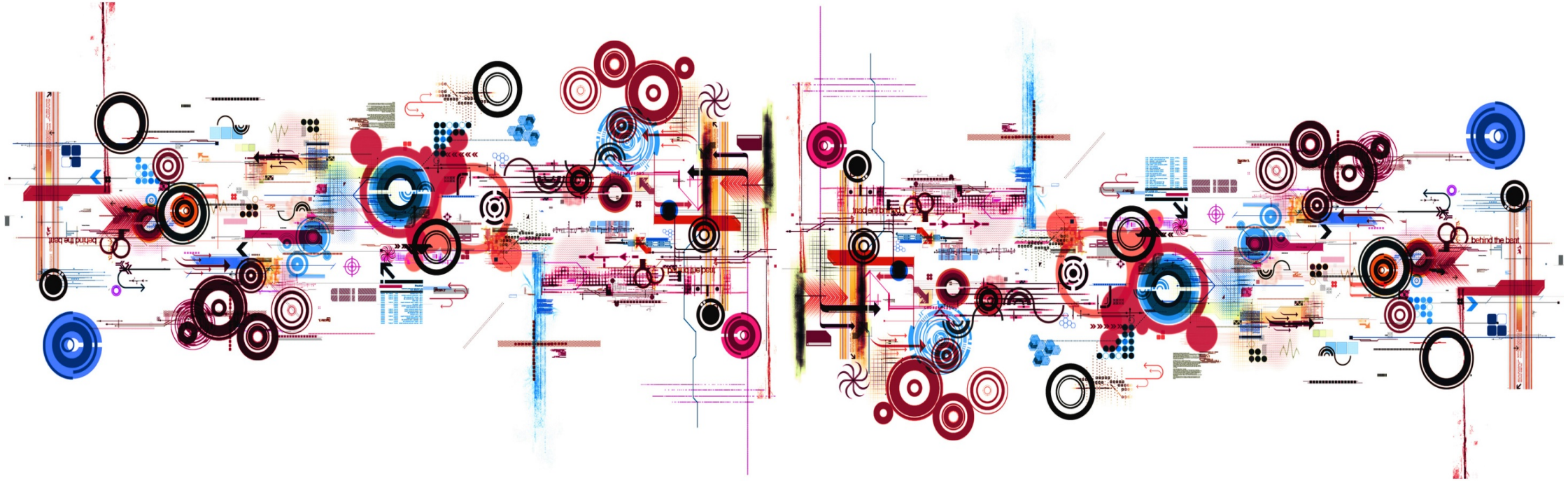
IT-Sicherheit - technische und organisatorische Pflichten nach dem BSI-Gesetz

am Beispiel eines KRITIS-Unternehmens



Basics

Wie ein Bayer ein sicheres Passwort wählt!

Bitte geben Sie ein sicheres Passwort ein.
Leberkas

Entschuldigung, Ihr Passwort ist zu kurz!
Leberkas-Semme

Entschuldigung, Ihr Passwort muss mindestens 1 Zahl enthalten.
1 Leberkas-Semme

Entschuldigung, Ihr Passwort darf keine Leerzeichen enthalten.
50drecksleberkassemmen

Entschuldigung, Ihr Passwort muss mindestens einen Umlaut enthalten.
50drecksleberkässemmelnzefix

Entschuldigung, Ihr Passwort muss mindestens 1 Großbuchstaben enthalten.
50DRECKSleberkässemmelnZEFIX

Entschuldigung, Ihr Passwort muss mindestens 1 Sonderzeichen enthalten
50DRECKSleberkässemmelnZEFIX!!!!!!!

Entschuldigung, Ihr Passwort darf nur Großbuchstaben enthalten, die nicht aufeinanderfolgend sind.
KreizKruzeFixVerdammterScheissDrecklatzkannstMiGleiKreizWeisSonstWo WosIsnDesFiaAScheissSystem50DrecksleberkässemmelnZeFiX!!!!

Entschuldigung, dieses Passwort ist bereits in Verwendung. Bitte wählen Sie ein anderes.

www.meinherzschlag.de

Bedrohungslage Bund und KRITIS-Unternehmen

- Cyber-Angriffe auf die Regierungsnetze finden täglich statt. Neben ungezielten Massenangriffen sind die Regierungsnetze auch gezielten Angriffskampagnen ausgesetzt.
- Im HTTP-Verkehr wurden im Jahr 2017 durchschnittlich rund 500 Schadprogramme pro Monat erkannt und abgewehrt, 28000 gezielte E-Mails mit integrierten Schadprogrammen konnte abgefangen werden.
- Die Analysten des BSI konnten im Berichtszeitraum über 40.000 Angriffe identifizieren, die von den eingesetzten kommerziellen Schutzprodukten nicht detektiert oder blockiert werden konnten. (Quelle: Lagebericht BSI 2018).

Bedrohungslage Bund und KRITIS-Unternehmen

- Die Gefährdungslage in den Kritischen Infrastrukturen ist insgesamt auf hohem Niveau, aber in den verschiedenen Branchen unterschiedlich ausgeprägt.
- KRITIS-Betreiber wie zum Beispiel Energieversorger sehen sich, zusätzlich zu normalen Angriffen aus dem Internet, auch neuen oder fortschrittlicheren Angriffen ausgesetzt. Andere Branchen stehen eher in den hinteren Reihen und sehen sich mit Attacken konfrontiert, die in den exponierteren Branchen schon beobachtet wurden. Die verwendeten Methoden wurden automatisiert und können von Angreifern nun flächendeckend eingesetzt werden. (Quelle: Lagebericht BSI 2018)

Einige Beispiele

- Ransomware im Krankenhaus: Februar 2016, Lukaskrankenhaus in Neuss. Kein Lösegeld gezahlt. Wiederherstellung aus Backups, Unterstützung durch BSI. Interne Kosten 1,0 Mio€
- Angriffe auf Telekom DSL-Router Bundesweit: 27. Nov. 2016, bundesweite Störungen von ca. 900.000 DSL-Router in Haushalten, Zugang zum Internet + davon abhängige Dienste gestört. Angriff erfolgte über Botnet (DDoS-Angriff).

Einige Beispiele

- Gegen Ende des Jahres 2017 hat das BSI über das Nationale Cyber-Abwehrzentrum Hinweise auf einen erfolgreichen CyberAngriff erhalten, von dem einzelne Bundesbehörden betroffen sein sollten. Primäres Ziel des Angriffs war das Auswärtige Amt. Eine von der Hochschule des Bundes betriebene Lernplattform wurde angegriffen, um über diesen Zwischenschritt einen Zugang in das Netz des Auswärtigen Amtes aufzubauen.
- 15. Mai 2018: Mutmaßlich russische Hacker sind in das Netz einer Tochter des Stromkonzerns EnBW eingedrungen. Es handelt sich um Netcom BW, einen regionalen Internetanbieter. Das Stromnetz war (angeblich) nicht in Gefahr. Die Angreifer waren über einen gehackten Zugang eines externen Dienstleisters in das Netz eingedrungen und hatten für einen Zeitraum von (angeblich) wenigen Minuten Zugriff auf einen geringen Teil des Internetverkehrs.

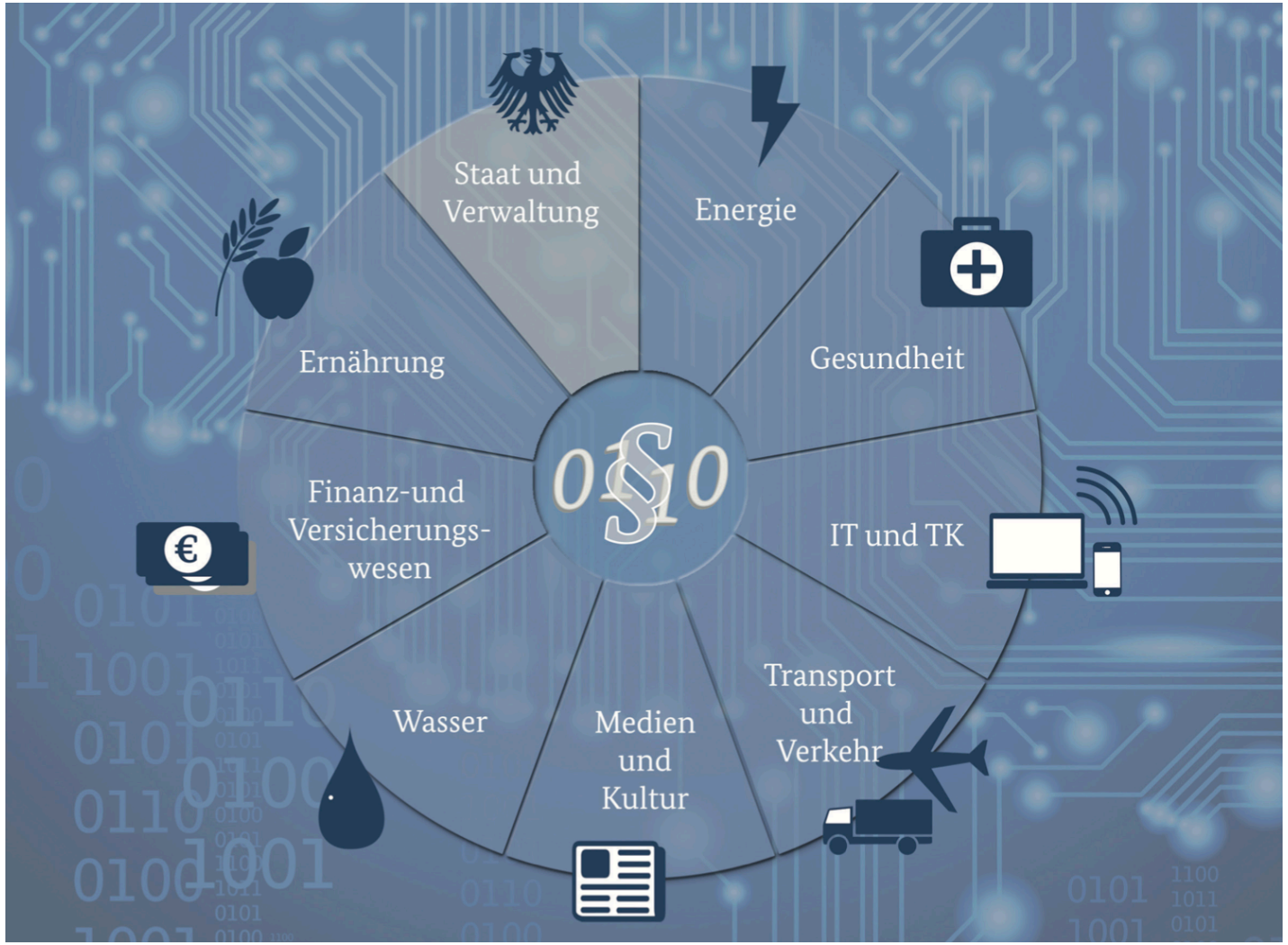
IT-Sicherheit - Regelungsraum

- IT-Sicherheitsgesetz (IT-SiG) – Artikelgesetz mitAuswirkungen auf BSIG, EnergiewirtschaftsG, AtomG, TMG, TKG + x
- BSI-Gesetz
- BSI-Kritis-Verordnung (messbare und nachvollziehbare Kriterien – Schwellenwerte für die Sektoren)
- BSI als nationale Cybersicherheitsbehörde
  - Informationssicherheit durch Prävention, Detektion und Reaktion
  - Für Staat, Wirtschaft und Gesellschaft

KRITIS – was ist das

- § 2 (1) BSIG: Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.
- Die Kritischen Infrastrukturen selbst sind dann in der BSI-Kritis-V näher bestimmt.

Was zählt dazu? Zunächst: 9 Sektoren



Von 3,5 Millionen Unternehmen in Deutschland sind etwa 2000 Anlagen betroffen

Quelle: BSI Broschüre

Sektorenregelungen – Vorgehensweise (Beispiel Energie)

- § 2 BSI-KritisV – Energie
  - die Versorgung der Allgemeinheit
    - mit Elektrizität, Gas, Kraftstoff und Heizöl, Fernwärme
  - Stromversorgung und Gasversorgung werden in den Bereichen Erzeugung, Übertragung und Verteilung von Strom sowie Förderung, Transport und Verteilung von Gas erbracht.
  - Die Kraftstoff- und Heizölversorgung wird in den Bereichen Rohölförderung und Produktherstellung, Öltransport sowie Kraftstoff- und Heizölverteilung erbracht.
  - Die Fernwärmeversorgung wird in den Bereichen Erzeugung von Fernwärme und Verteilung von Fernwärme erbracht.

Voraussetzungen? BSI-Kritis-V

- Je nach Sektor definiert, grober Schwellenwert = Versorgungsgrad an Menschen (500.000)
- Beispiel Energie:
  - Kraftwerk: 420 MW Produktion, = 7,375kWh (Durchschnittsverbrauch eines Kunden) x 500.000
  - Raffinerie: Erzeugter Kraftstoff in Tonnen pro Jahr 420000
  - Tankstellennetz: Verteilter Kraftstoff in Tonnen pro Jahr 420000
  - Fernwärmenetz: angeschlossene Haushalte 250000

Sektorenregelungen – Vorgehensweise (Beispiel Ernährung)

- § 4 BSI-KritisV – Ernährung
  - die Versorgung der Allgemeinheit mit Lebensmitteln
  - Die Lebensmittelversorgung wird in den Bereichen Lebensmittelproduktion und -verarbeitung sowie Lebensmittelhandel erbracht.
- Voraussetzungen:
  - Der ... Schwellenwert (Speisen) ist unter Annahme einer durchschnittlichen Produktionsmenge zur Versorgung einer Person mit Lebensmitteln (Speisen) aller Produktgruppen von 0,869 Tonnen/Jahr sowie eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet: 434 500 t/Jahr = 0,869 t/Jahr x 500 000
  - Getränke (nichtalkoholisch) : 350 Mio l/Jahr = 700 l/Jahr x 500000

Sektorenregelungen – Vorgehensweise (Beispiel Gesundheit)

- § 6 BSI-KritisV – Gesundheit
  - die stationäre medizinische Versorgung (Aufnahme, Diagnose, Therapie, Unterbringung, Pflege und Entlassung)
  - die Versorgung mit unmittelbar lebenserhaltenden Medizinprodukten, die Verbrauchsgüter sind (Herstellung und Abgabe)
  - die Versorgung mit verschreibungspflichtigen Arzneimitteln und Blut- und Plasmakonzentraten zur Anwendung im oder am menschlichen Körper (Herstellung, Vertrieb und Abgabe)
  - die Laboratoriumsdiagnostik (Transport und Analytik)
- Voraussetzungen:
  - Schwellenwerte für 500000 Personen: 181,36 € pP bei Verbrauchsgütern, 9,3 Packungen verschreibungspflichtige Medikamente pP, 3 Laboraufträge pP (d.h. 1,5Mio für ein Labor)

Sektorenregelungen – Vorgehensweise (Beispiel Verkehr)

- § 8 BSI-KritisV – Trasnsport und Verkehr
  - die Versorgung der Allgemeinheit mit Leistungen zum Transport von Personen und Gütern
  - Personen- und Güterverkehr wird durch die Verkehrsträger Luftverkehr, Schienenverkehr, Binnen- und Seeschifffahrt, Straßenverkehr sowie verkehrsträgerübergreifend im öffentlichen Personennahverkehr (ÖPNV) und in der Logistik erbracht.
- Schwellenwerte:
  - Flughafen: 20 Mio Passagiere, München hatte 2018 46,8 Mio
  - Flugsicherung: 17500 Flugbewegungen pro Jahr
  - ÖPNV 125 Mio Fahrgäste, MVV hatte 723 Mio
  - Logistik: 17 MioTonnen pro Jahr (Spedition Kühne&Nagel)

Pflichten/Rechte der KRITIS-Unternehmen

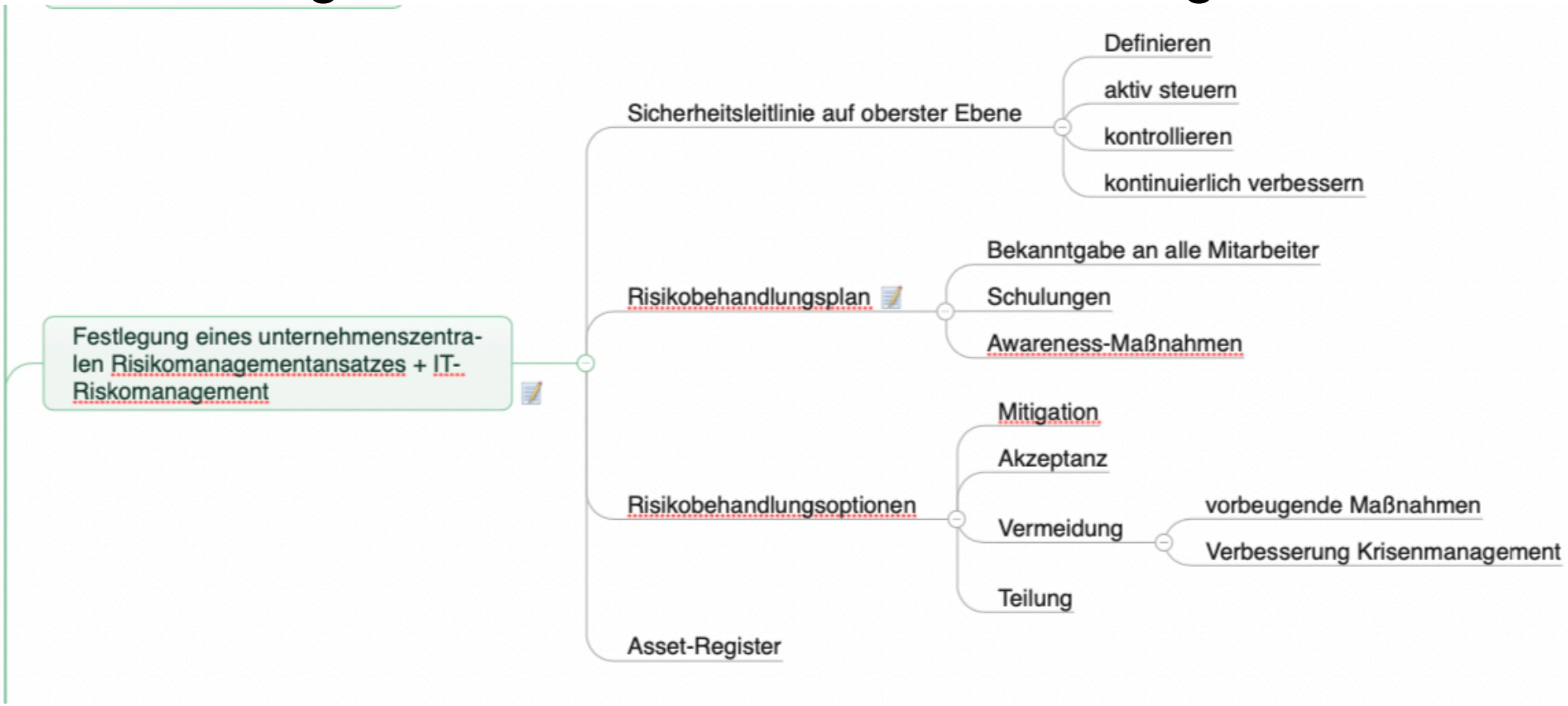
- IT-Sicherheit nach dem Stand der Technik
- Pflicht zur Überprüfung der Absicherung durch Audits (alle zwei Jahre), Beseitigungspflicht bei Mängeln
- Meldepflichten für erhebliche Störungen
- Einrichtung einer Kontaktstelle (Funktionspostfach) zum BSI für Meldungen, 24x7
- Anspruch auf unverzügliche Versorgung mit relevanten Informationen durch das BSI
- Anspruch auf Beratung und Unterstützung durch das BSI
- Entwicklung branchenspezifischer Sicherheitsstandards möglich (B3S)

Gesetzlicher Sicherheitsstandard: § 8 a BSIG

- Betreiber Kritischer Infrastrukturen sind verpflichtet ... angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden.
- Stand der Technik bedeutet: Implementierung eines ISO 27001 konformen Informationssicherheitsmanagementsystems – ISMS oder B3S.
- Auditierung alle 2 Jahre + Übermittlung an BSI einschließlich aufgedeckter Mängel.

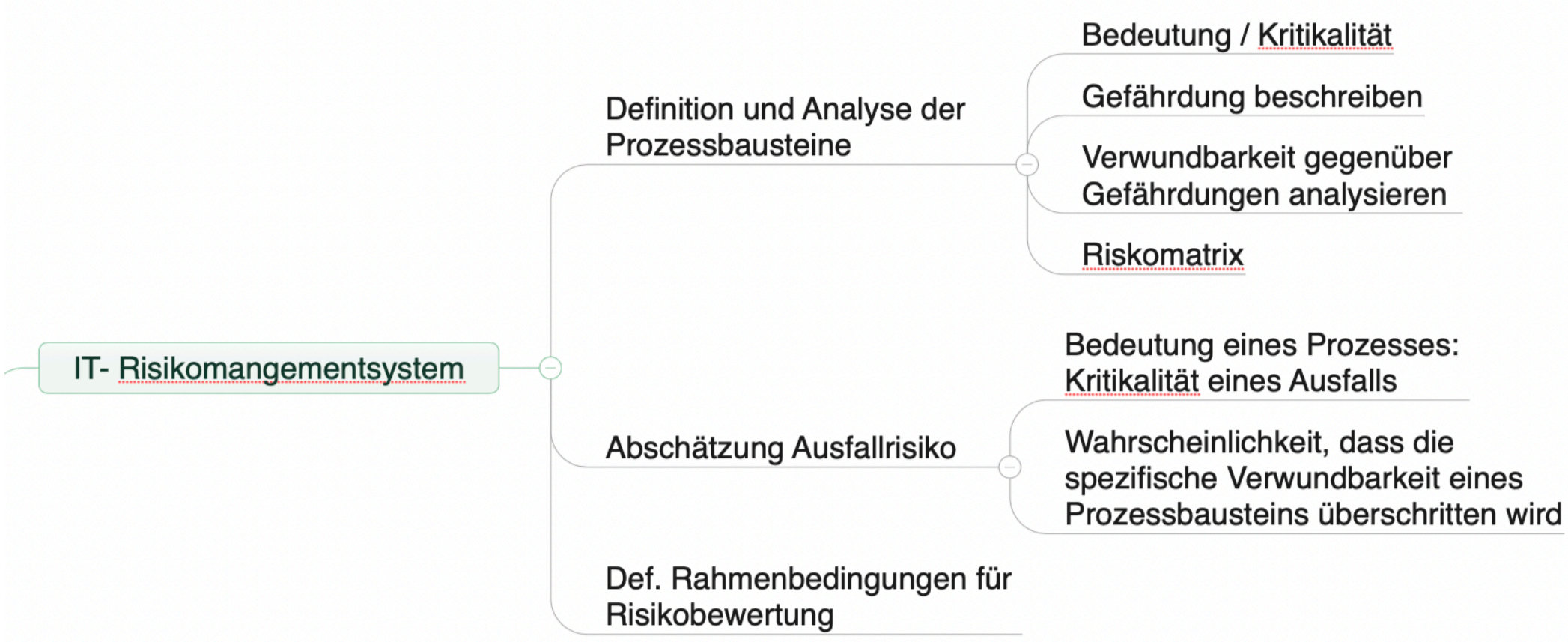
Gesetzlicher Sicherheitsstandard: § 8 a BSIG

- Festlegung eines unternehmenszentralen Risikomanagementansatzes + IT-Riskomanagement



Gesetzlicher Sicherheitsstandard: § 8 a BSIG

- IT-Risikomanagement



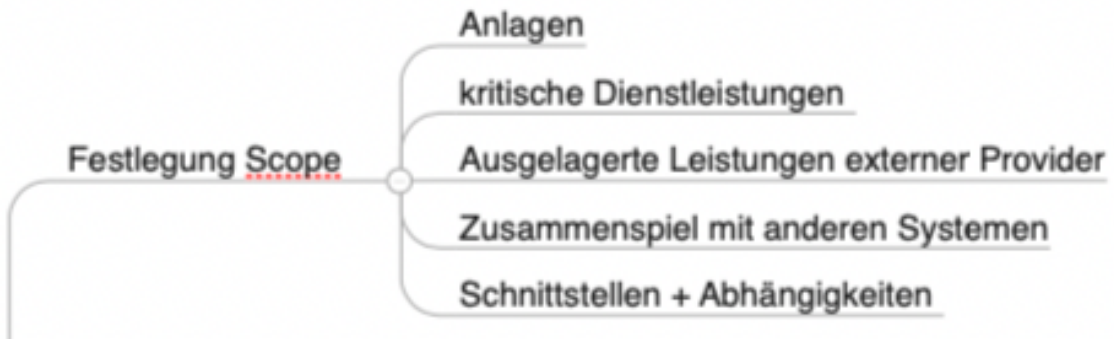
Gesetzlicher Sicherheitsstandard: § 8 a BSIG

- Datenschutzmanagementsystem
- Interne Meldewege
- Technische und organisatorische Maßnahmen (TOM)
- Dokumentations- und Nachweispflichten

Das alles kennen wir aus unseren DSGVO-Projekten.
Hier liegt unser Beratungsansatz!

TOMs

- Festlegung Scope und Prozesse



TOMs Umsetzung

- Umsetzung
  - Business Continuity Management
  - Vorsorge durch Notfall- und Krisenmanagement
  - Realisierung Sicherheitskonzepte
    - Analyse der Infrastruktur unter Hochverfügbarkeitsaspekten, Umsetzung der entsprechenden technischen und organisatorischen Maßnahmen
    - Sicherheitseinstufung von Dokumenten und Klassizierung von Informationen
    - Erstellung und Umsetzung von Konzepten zur kryptografischen Absicherung schützenswerter Informationen
    - Richtlinien zum Einsatz neuer Komponenten in bestehenden IT-Architekturen
    - erweiterte Regelungen und Kontrollen für den Zutritt zu IT-Systemen und den Zugriff auf Daten
    - Auswahl von nachgewiesen vertrauenswürdigen Unternehmen für IT-Sicherheitsdienstleistungen
  - Regelmäßige Überprüfung der Realisierung
  - Schulungen und Sensibilisierungsmaßnahmen
  - IT-Sicherheitsrevision
  - Notfall- und Krisenreaktionsübungen
- Doku
  n

TOMs Dokumentation - Rechenschaftspflicht

- Sicherheitsdokumentation
  - Konzept und Dokumentation des Risikomanagements inkl. Risikoanalyse
  - Beschreibung des Informationssicherheits-managementsystems (ISMS)
  - Notfallkonzept und Beschreibung des Continuity Managements
  - Dokumente des Asset Managements
  - Dokumentation der Prozesse zur baulichen und physischen Sicherheit
  - personelle und organisatorische Sicherheit
  - Konzepte und Dokumentation zur Vorfallserkennung und -bearbeitung
  - Konzepte und Dokumentation von Überprüfungen
  - Richtlinien zur externen Informati-onsversorgung
  - Richtlinien zum Umgang mit Lieferanten und Dienstleistern
  - Sicherheitskonzept

Gesetzliche Meldepflicht Kritis-Unternehmen § 8b (4) BSIG

Betreiber Kritischer Infrastrukturen haben die folgenden Störungen unverzüglich über die Kontaktstelle an das Bundesamt zu melden:

- Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben,
- erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können.
- Die Meldung muss Angaben zu der Störung, zu möglichen grenzübergreifenden Auswirkungen sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur erbrachten kritischen Dienstleistung und zu den Auswirkungen der Störung auf diese Dienstleistung enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.

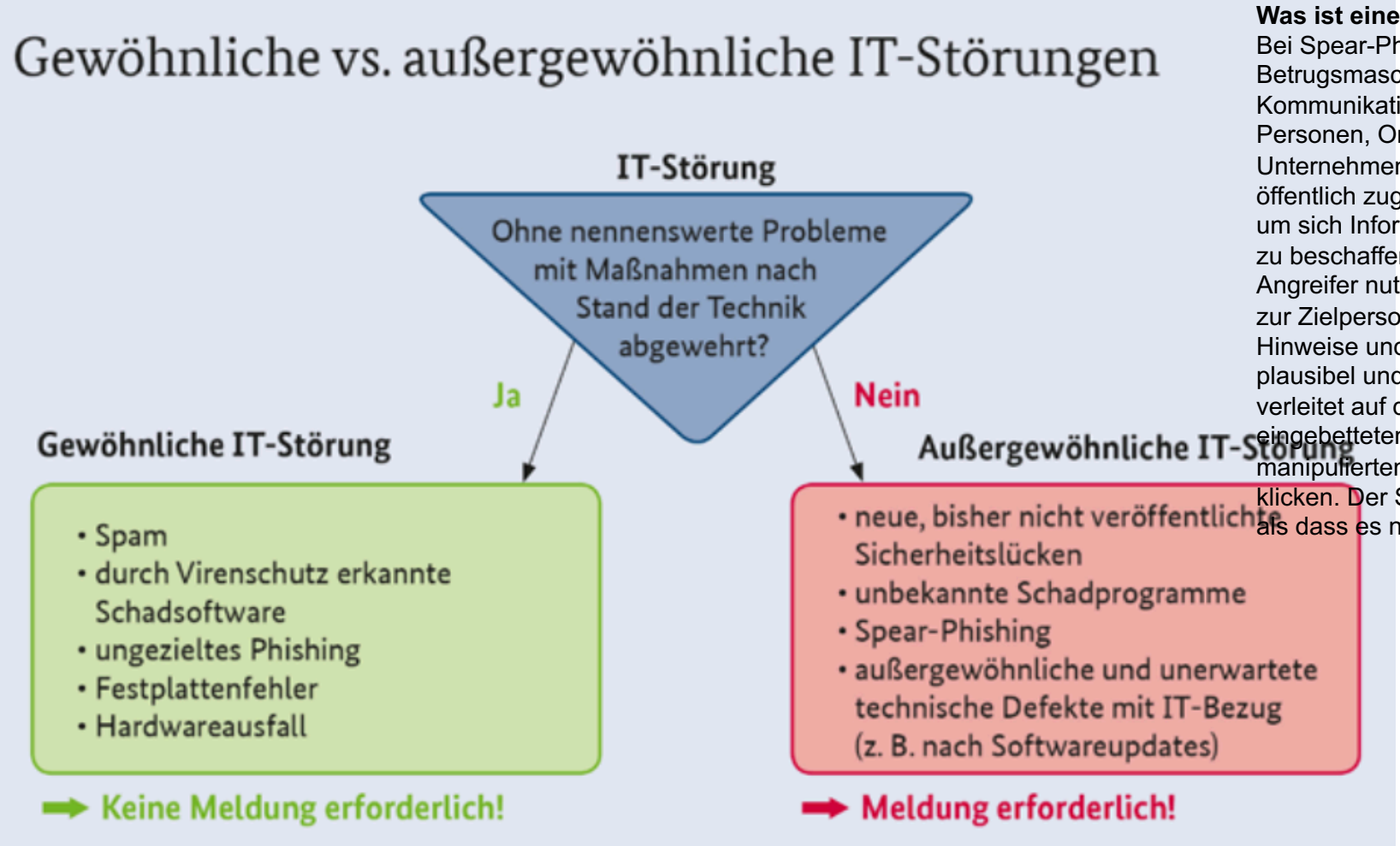
Meldepflicht bei Bundesbehörden

- Nach § 4 Abs. 3 BSIG sind die Bundesbehörden verpflichtet, das BSI unverzüglich zu unterrichten, wenn ihnen Informationen vorliegen, die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik von Bedeutung sind.

Was ist eine Störung?

Quelle: BSI Broschüre

Ok, aber was ist in der IT schon außergewöhnlich?



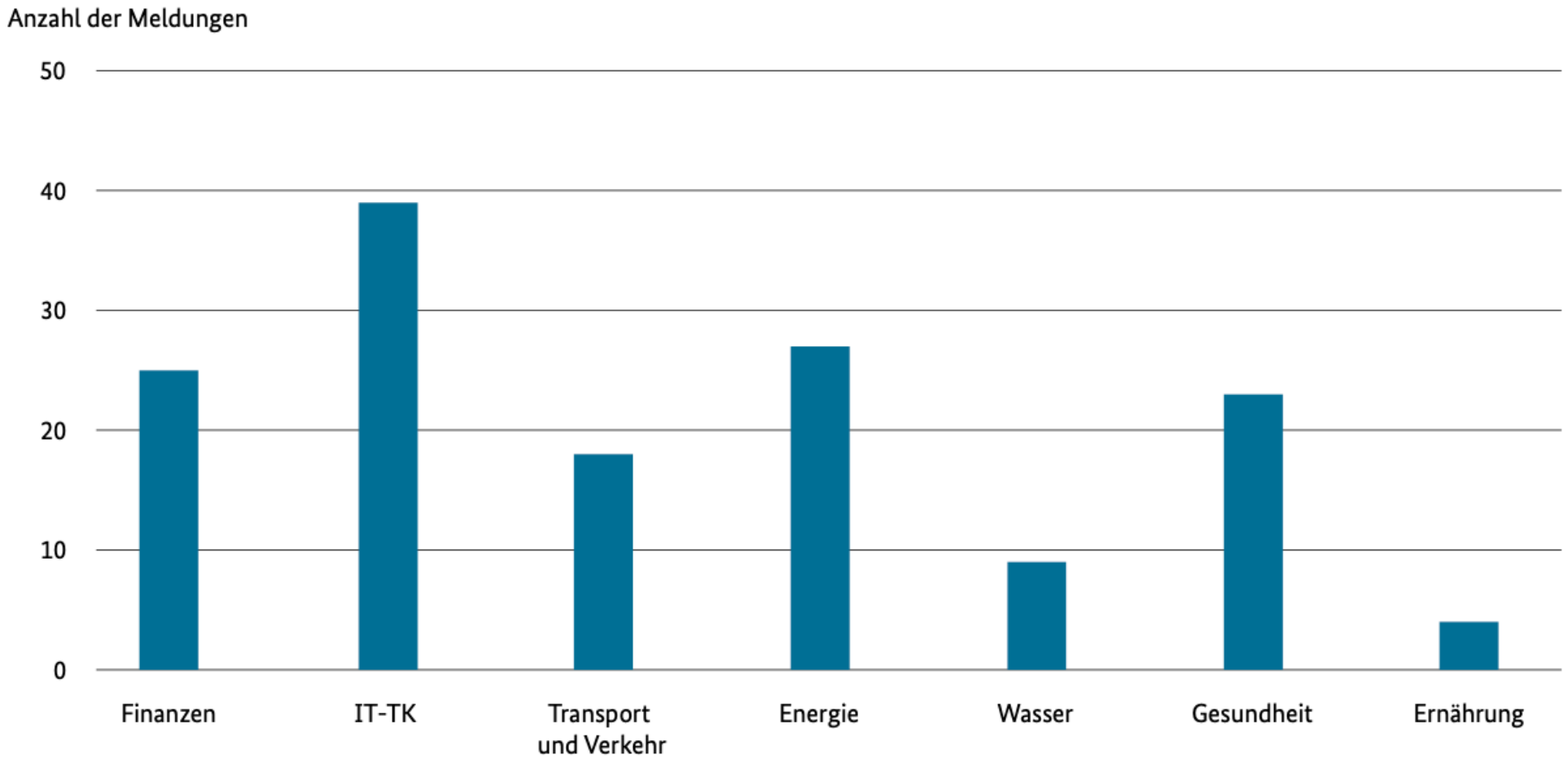
Was ist eine Spear-Phishing-Attacke?
Bei Spear-Phishing handelt es sich um eine Betrugsmasche per elektronischer Kommunikation, die auf bestimmte Personen, Organisationen oder Unternehmen abzielt. Der Angreifer nutzt öffentlich zugängliche und verfügbare Daten, um sich Informationen über die Zielperson zu beschaffen(„Social Engineering“). Der Angreifer nutzt diese Daten, um Vertrauen zur Zielperson aufzubauen. Anliegen, Hinweise und Aufforderungen scheinen plausibel und das Phishing-Opfer wird dazu verleitet auf den z.B. in die E-Mail eingebetteten Link zum Öffnen einer manipulierten Webseite zu klicken zu klicken. Der Sender „weiß einfach zu viel“ als dass es nicht seine Richtigkeit hätte“.

Quelle: BSI Broschüre

Meldepflichtige Vorfälle 2017

- Im Jahr 2017 wurden insgesamt 157 SOFORT-Meldungen von Bundesbehörden an das Referat „Zentrale Meldestelle und Nationales IT-Lagezentrum“ gemeldet.
- Im Berichtszeitraum erreichten das BSI 145 Meldungen aus den KRITIS-Sektoren; die meisten aus dem Bereich IT und Telekommunikation, die zweitmeisten aus dem Energiesektor.

Meldepflichtige Vorgänge nach Sektoren 2017/18



Quelle: BSI Lagebericht 2018

Was macht das BSI? § 3ff BSIG

- Untersuchung von IT-Produkten und Software mit Relevanz für die Sicherheit von Kritischen Infrastrukturen + Zertifikate
- Einrichtung eines BSI-Lagezentrums
- Analyse und Bewertung der eingehenden Meldungen
- Auswertung weiterer Quellen zu den Meldungen
- Warn- und Alarmierungsmeldungen an die Unternehmen mit Handlungsempfehlungen
- Modell: Detektion -> Analyse und Bewertung -> Reaktion mit Handlungsempfehlung sowie bei Bedarf vor Ort Unterstützung durch Mobile Incident Response Teams (MIRT) des BSI

Gemeinsame Initiativen zur Verbesserung Schutzsituation

UP KRITIS

- UP KRITIS Umsetzungsplan KRITIS
- Der UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen.
- Der UP KRITIS adressiert acht der neun Sektoren Kritischer Infrastrukturen. Der Sektor "Staat und Verwaltung" wird durch den UP BUND abgedeckt.
- Ziel der Kooperation UP KRITIS ist es, die Versorgung mit kritischen Infrastrukturdienstleistungen in Deutschland aufrechtzuerhalten.
- Das Dokument "UP KRITIS: Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen -Grundlagen und Ziele-" wurde am 18. Februar 2014 vom Plenum des UP KRITIS verabschiedet.
- Organisation durch eigene Geschäftsstelle, Rat, Branchenarbeitsgruppen, Themenarbeitskreise, Plenum.

Ziele UP KRITIS

UP KRITIS

- Förderung der Robustheit von IKT-Komponenten in kritischen Prozessen
- Austausch über aktuelle Vorkommnisse
- Gemeinsame Einschätzung und Bewertung der Cyber-Sicherheitslage
- Erarbeitung gemeinsamer Dokumente und Positionen
- Auf- und Ausbau von Krisenmanagementstrukturen
- Koordinierte Krisenreaktion und -bewältigung
- Durchführung von Notfall- und Krisenübungen
- Gemeinsames Handeln gegenüber Dritten

UP KRITIS Branchen- und Themenarbeitskreise

UP KRITIS

- Datacenter und Hosting
- Ernährungsindustrie
- Gas
- Internetinfrastruktur
- Kreditwirtschaft
- Lebensmittelhandel
- Medien
- Med. Versorgung
- Mineralöl
- Strom
- Telekommunikation
- Transport und Verkehr
- Versicherungs-wirtschaft
- Wasser/Abwasser

- Anforderungen an Lieferanten
- Audits und Standards
- Industrial Control Systems (ICS)
- KRITIS-Tagung
- Operativer Informationsaustausch
- SPOC-Austausch
- Szenariobasierte Krisenvorsorge
- Transparenzpflichten
- Übungen

Quelle: BSI Broschüre

Interessante Links oder hilfreiche Informationen

- Lagebericht BSI 2018:
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=6
- BSI Orientierungshilfe zu Nachweisen § 8a Abs. 3
- Broschüre des BSI: Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS
- UP KRITIS

Muster und Formulare

Registrierung und Meldung:

- Betreiber finden die zur Registrierung ihrer Kontaktstelle notwendigen Formulare auf dem Melde- und Informationsportal (MIP)
- Meldeformular für KRITIS-Betreiber - Musterbeispiel (PDF, 406KB, Datei ist nicht barrierefrei)
- S/MIME-Zertifikat für Meldungen (FileTypex-pem-file, 2KB, Datei ist nicht barrierefrei) für Meldungen
- Registrierungsformular für KRITIS-Betreiber - Musterbeispiel (PDF, 115KB, Datei ist nicht barrierefrei)
- Anlage 2 zum Registrierungsformular für KRITIS-Betreiber - Musterbeispiel (PDF, 1MB, Datei ist barrierefrei/barrierearm)
- Jegliche Kommunikation mit dem KRITIS-Büro nutzt das S/MIME Zertifikat für die digitale Signatur des KRITIS-Büros (FileTypex-pem-file, 2KB, Datei ist nicht barrierefrei)
- Öffentlicher PGP-Schlüssel des KRITIS-Büros
  Fingerabdruck: A7EE 4481 9359 296E 93EE 9AC8 CF62 1576 0087 18F6
  Schlüsselkennung: CF621576008718F6

Dokumente zu den branchenspezifischen Sicherheitsstandards (B3S):

- Hilfestellung zu B3S: Orientierungshilfe B3S (Version 1.0)
- Englische Hilfestellung zu B3S (neue Version): Orientierungshilfe B3S (englisch)
- Das folgende Formular dient als Hilfestellung bei der Einreichung branchenspezifischer Sicherheitsstandards
- Anlage zur Einreichung von branchenspezifischen Sicherheitsstandards: Mapping Tabelle zur Orientierungshilfe B3S

Dokumente zur Nachweiserbringung nach § 8a (3) BSIG:

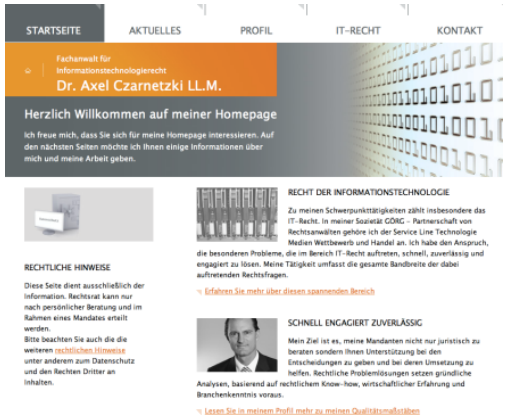
- Datenschutzrechtliche Hinweise zur Erhebung von Daten in den Nachweisdokumenten PE, PS, PD und KI gemäß § 8a Absatz 3 BSIG (PDF, 240KB, Datei ist barrierefrei/barrierearm)
- Nachweisdokument zur Kritischen Infrastruktur: Blatt KI
- Nachweisdokument zur prüfenden Stelle: Blatt PS
- Nachweisdokument zur Prüfungsdurchführung: Blatt PD
- Nachweisdokument zu den Prüfergebnissen: Blatt PE
- Mindestanforderungen an eine Mängelliste
- Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG

Alles zu finden im Downloadbereich der Website des BSI

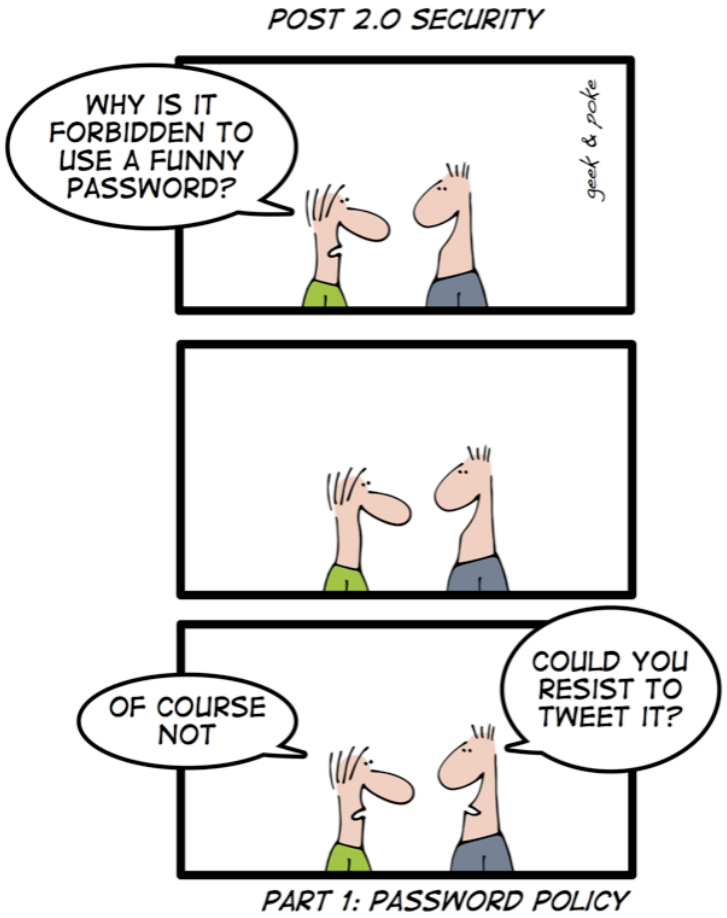
Zum Abschluss

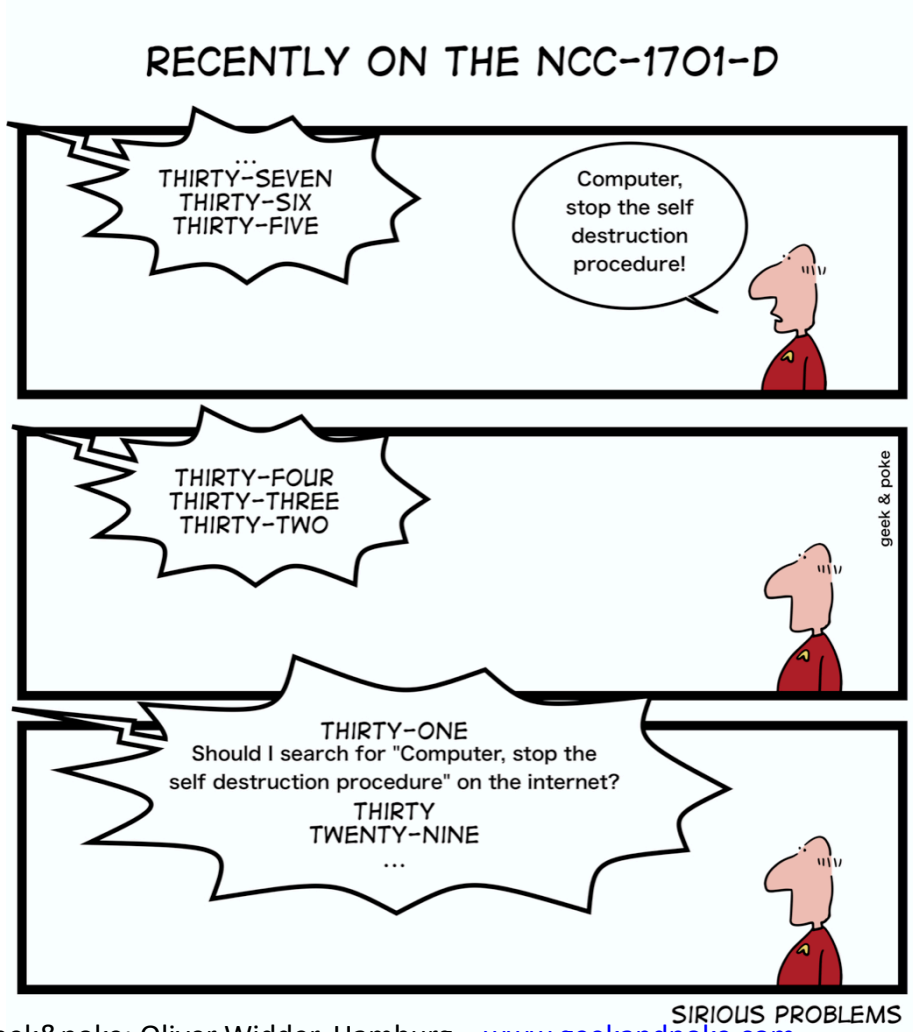
GÖRG

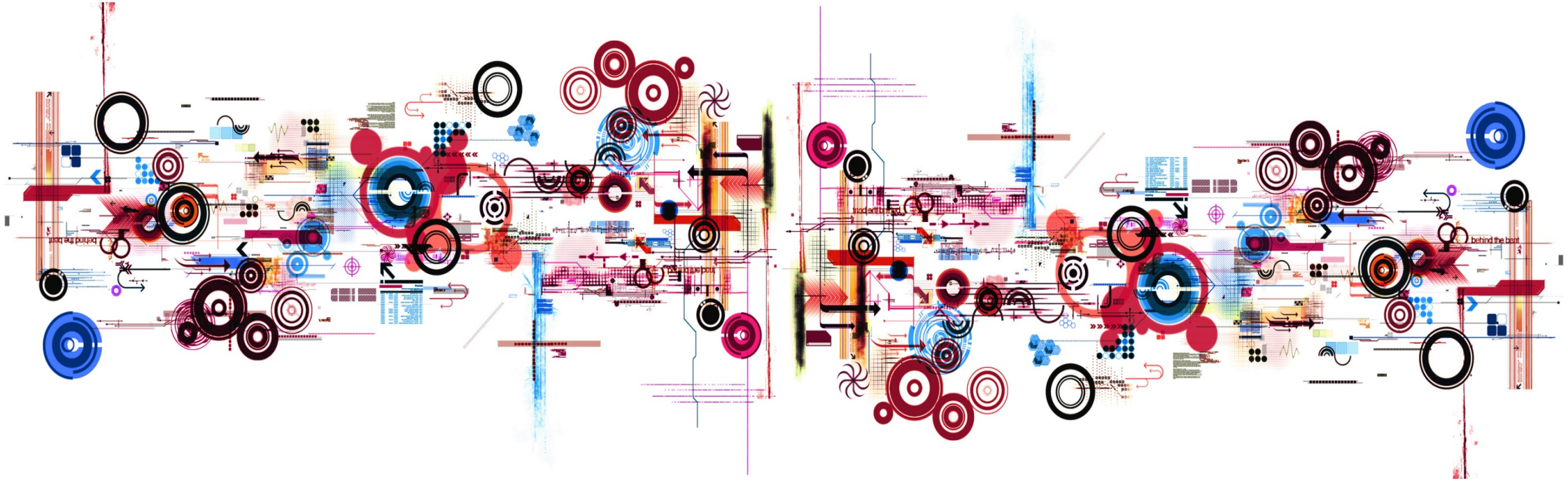
IHRE WIRTSCHAFTSKANZLEI



www.czarnetzki.eu





from geek&poke; Oliver Widder, Hamburg – www.geekandpoke.com

Vielen Dank für Ihre Aufmerksamkeit ☺
Es war mir ein Vergnügen.