TeleTrusT Information Security Professional

TeleTrusT Pioneers in IT security.

T.I.S.P. Community Meeting 2019

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Berlin, 05. - 06.11.2019

Cybersicherheit: Aktuelle Bedrohungslage und davon abgeleitetes strategisches Handeln

Klaus Frank, EnBW Full Kritis Service

Cybersicherheit: Aktuelle Bedrohungslage und davon abgeleitetes strategisches Handeln ›

IT. Sicher. Machen.

EnBW Full Kritis Service
Klaus Frank
6. November 2019

Aktuelle Herausforderungen

EnBW

Zunehmende Vernetzung führt oft dazu, dass jede Schwachstelle im System über das Internet gezielt angegriffen werden kann

Umsetzung des **IT-Sicherheitsgesetzes** nach BSI Kritis-Verordnung sowie branchenspezifischen Sicherheitsstandards (B3S)

Einhaltung der **Datenschutz-Grundverordnung** (EU-DSGVO)

Fehlende Expertise sowie Mangel an **Zeit und Ressourcen**

Erhöhte Gefahr von **schwerwiegenden Cyber-Angriffen** (z. B. Emotet)

Gefahr von **funktionsbeeinträchtigenden Eingriffen/Störungen** bei kritischen Infrastrukturen

Risk Barometer der Allianz Versicherung

EnBW

Platz 1

37 %

Betriebsunter-brechungen*

Platz 1

37 %

Cybervorfälle

Platz 3

28 %

Naturkatastrophen

Platz 6

19 %

Feuer und Explosionen

Platz 5

23 %

Marktentwicklungen

Platz 4

27 %

Veränderungen in Gesetzgebung und Verordnung

Bem.: * Cybervorfälle sind zudem die am meisten gefürchteten Auslöser von Betriebsunterbrechungen.
Quelle: Allianz AGCS Risiko Barometer 2019

Erfolgreiche Angriffe der letzten 6 Monate

Trojaner „RobbinHood“ in Baltimore

Gesamtschaden: ca. 18 Mio. US-Dollar

Ransomware-Angriff auf Schulen in Louisiana

US-Bundesstaat ruft Notstand aus, genauer Schaden unbekannt

Angriff auf Capital One

Massiver DDOS-Angriff auf Wikipedia

diverse Webseiten von Wikipedia nicht erreichbar

Apr | Mai | Jun | Jul | Aug | Sep

Spionage-Angriff „Winnti“ auf Konzerne

Lösegeldzahlung von 600.000 US-Dollar

Malware-Befall „Sodinokibi“ auf DRK Einrichtungen

Mehre Tage nur noch Arbeiten ohne IT möglich

Patientendaten ungeschützt im Netz

In Deutschland 13.000 Patientendatensätze, weltweit Millionen

Quellen: Heise, Presseportal, Tagesschau

Beispiel: Angriff im Finanzwesen

Capital One

Was? Hackerin stiehlt Daten von ca. 100 Millionen Bankkunden

Wie? Angriff erfolgte über Schwachstelle in der falsch konfigurierten Firewall

Wann? Juli 2019

Schaden: Bank erwartet aufgrund des Angriffs Mehrkosten von rund 100 Millionen USD

Cybersicherheit ist eine existenzielle unternehmerische Herausforderung

EnBW

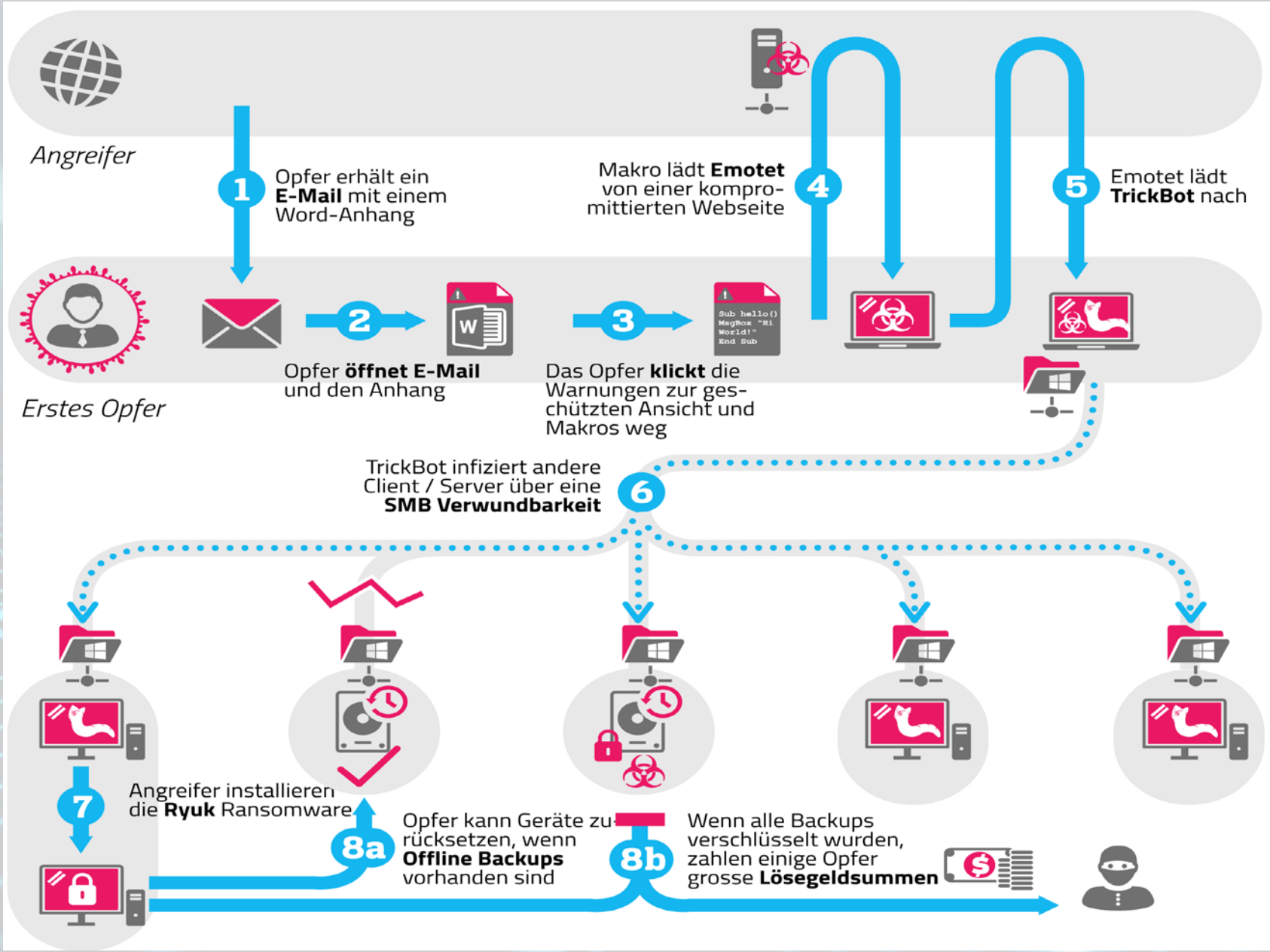
Änderung der **Qualität der Bedrohungen**

*„Es ist nicht die Frage **ob, sondern wann** man erfolgreich angegriffen wird und dies überhaupt/ rechtzeitig wahrnimmt.“*

- **Spezifisch**: immer häufiger **branchenspezifische** oder firmenspezifische Angriffswellen
- **Opfer**: mehr **Fokus auf IT-Dienstleister** (Kundenzugang per Fernwartung)
- **Schaden**: mehr **Härte** bei Erpressung -> bis zur **Auslöschung der Firma** (teils inkl. Back-ups)
- **Tatwaffen**: sehr **dynamische Weiterentwicklung** der erfolgreichen Trojaner wie Emotet und GandCrab

Russland: 67 Prozent

Beispiel Emotet

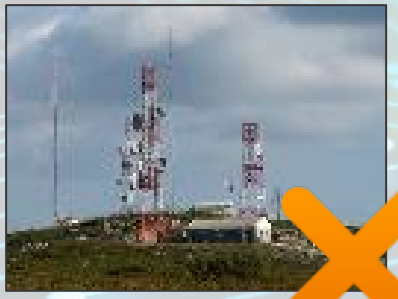


Quelle: Schweizer Melde- und Analysestelle Informationssicherung MELANI (Link)

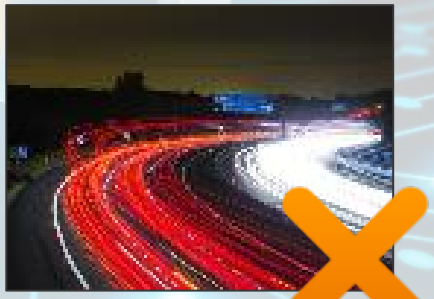
Cybersicherheit ist eine existenzielle unternehmerische Herausforderung

Echte Krisenszenarien möglich

Strom-
versorgung



Kommunikation



Transport
und Verkehr

- **Mittelfristiger verketteter Ausfall** von kritischen Infrastrukturen bei regionaler/ nationaler Krisensituation
- Auch bei **staatlicher großflächiger Cybersabotage** sollten kritische Infrastrukturen weiter funktionieren

Cybersicherheit ist eine existenzielle unternehmerische Herausforderung

Gefahren durch **Störfallszenarien**

- **natürliche** Gefährdungen (Unwetter, Sonnenstürme etc.)
- **zivilisatorische** Gefährdungen (Brand, Flugzeugabsturz etc.)
- vorsätzliche **Straftaten** von **Einzel-/Innentätern**
- Geschäftsmodelle für **organisierte Cyberkriminalität**
- staatl. **Wirtschaftsspionage** oder staatl. **Hacking** (z. B. zur Geldbeschaffung)
- staatl. **angeordnete Zerstörung** von Infrastrukturen (z. B. Cyberangriff der USA auf den Iran im Juni 2019)

Rechtslage

Erwartungen zum **IT-Sicherheitsgesetz 2.0**

- **schnellere** Prävention
- mehr **Befugnisse für Durchgriff** für das BSI (inkl. **Sensorik** vor Ort)
- gleiches **Strafmaß wie Datenschutz**
- erweiterter Geltungsbereich (Sektor **Entsorgung**, Kritis-„**Kernkomponenten**“)
- bedarfsweiser Durchgriff auf Kritis-**Lieferanten** und **andere Infrastrukturen**
- mehr **Rechte/Pflichten** für Kritis-Betreiber (z. B. Krisenkommunikationssystem)
- Präventionsmaßnahmen zur **Großkrisenbeherrschung**

Strategische Handlungsfelder zur Verbesserung der Cyber-Resilienz

- Vertiefung der **Zusammenarbeit von Diensten** (BSI, LKA, LfV) **und Industrie** auf Landes-/Bundesebene
- **Begrenzung der digitalen Abhängigkeit der Europäer** durch kooperative Geschäftsmodelle in Deutschland und Europa
- Konzeption, Bau und Absicherung von **schnellen, sicheren und stabilen IT-Infrastrukturen**
- Weiterentwicklung der Konzepte zur **Beherrschung von Großkrisen**

Cyberschutzprogramm ›

Am Beispiel der Kritis-Branche
„Gesundversorgung im Krankenhaus“

IT. Sicher. Machen.

EnBW Full Kritis Service
Klaus Frank
6. November 2019

Konzept des Cyberschutzprogramms

Messen der richtigen KPIs zum Nachweis der Cybersicherheitsqualität pro IT Infrastruktur (Anlage)

Wissen über das wahre Lagebild, die Bedrohungen und die aktuellen Angriffswellen

Maßnahmen gegen aktuelle Lage durch technische und organisatorische Mittel

Branchenspezifische Risikolandkarte BW = Erster Schritt zu einem zentralen Lagebild kritischer Infrastrukturen in BW

Krankenhaus
IT-Infrastruktur

M2

Innenmessung
IT und OT

Messung
Prozessreifegrad
(Interview)

M3

Digitaler
Fußabdruck im
Internet

M1

Cybersecurity
Leitstand BW
Technik / Analysten

LKA

Innenministerium

Brancheverbände/BSI

EnBW Full Kritis Service

EnBW

Kontakt:

Klaus Frank (Leiter FKS)
k.frank@kk.enbw.com
Mobil: +49 160 94608500

Jürgen Franke (Leiter FKS Vertrieb)
j.franke@enbw.com
Mobil: +49 173 3420062

www.enbw.com/kritis

0800 0 KRITIS
kritis@enbw.com