Cybersicherheit: Aktuelle Bedrohungslage und davon abgeleitetes strategisches Handeln ›

EnBW Full Kritis Service
Ihre IT. Sicherer. Machen.
Klaus Frank, Sönke Pingel, Frank Brech
20.09.2019

Bedrohungslage (1/2)

Beispiele von Angriffen der letzten 6 Monate (seit April 2019)

2019

Apr

Spionage-Angriff „**Winnti**“ auf Konzerne[1]

- kein Abfluss sensibler Daten bekannt, Schaden nicht absehbar

Mai

Emotet-Befall bei Heise Verlag[2]

- Schaden bei weit über 50.000€

Jun

Trojaner „**RobbinHood**“ in Baltimore[6]

- Gesamtschaden wird auf 18 Mio. US-Dollar geschätzt

Ransomware-Angriff auf Riviera Beach in Florida[7]

- Lösegeldzahlung von 600.000 US-Dollar, tatsächlicher Schaden wohl deutlich höher

Jul

Malware-Befall „**Sodinokibi**“ **DRK** Einrichtungen[3]

- mehrere Tage nur noch Arbeiten ohne IT möglich

Ransomware-Angriff auf Schulen in Louisiana[8]

- US-Bundesstaat ruft Notstand aus, genauer Schaden unbekannt

Aug

Cyberattacke auf die **Messe Stuttgart**[4]

- finanzieller Schaden aktuell noch unbekannt

Massiver **DDOS**-Angriff auf Wikipedia[9]

- diverse Webseiten von Wikipedia nicht erreichbar (auch deutschsprachige Webseite)

Sep

Patientendaten ungeschützt im Netz[5]

- in Deutschland 13.000 Patienten-datensätze, weltweit Millionen

Quellen: Heise, Presseportal, Messe-Stuttgart Tagesschau – Links:1: https://www.presseportal.de/pm/69086/4330907; 2: https://www.heise.de/ct/artikel/Trojaner-Befall-Emotet-bei-Heise-4437807.html;
3: https://www.heise.de/newsticker/meldung/Zurueck-zu-Bleistift-und-Papier-Schadsoftware-legt-Klinikserver-lahm-4473927.html 4: https://www.messe-stuttgart.de/newsroom/details/cyberattacke-auf-die-messe-stuttgart/
5: https://www.tagesschau.de/investigativ/br-recherche/patientendaten-101.html 6: https://www.heise.de/newsticker/meldung/Ransomware-fuegt-Baltimore-Millionenschaden-zu-4442881.html
7: https://www.heise.de/newsticker/meldung/Ransomware-Angriff-Behoerden-einer-Stadt-in-Florida-zahlen-600-000-US-Dollar-an-Hacker-4451978.html
8: https://www.heise.de/newsticker/meldung/US-Bundesstaat-Louisiana-ruft-Notstand-wegen-Erpressungstrojaner-Angriff-aus-4479912.html 9: https://www.heise.de/newsticker/meldung/Massiver-DDOS-Angriff-auf-Wikipedia-4516131.html

Bedrohungslage (2/2)

Informationssicherheit wird zur existenziellen unternehmerischen Frage!

Änderung der Qualitäten der Bedrohungen

- **Opfer:** Fokus auf **IT-Dienstleister** (Kundenzugang per **Fernwartung)**
- **Härte:** Erpressung -> **Auslöschung der Firma** (teils inkl. Back-ups)
- **Intelligenz:** sehr **dynamische Trojaner** wie Emotet und GandCrab

Echte Krisenszenarien möglich

- Bei einer echten regionalen oder nationalen Krisensituation können kritische Infrastrukturen **mittelfristig und verkettet** ausfallen.

kein Strom → keine normale Kommunikation → kein normaler Verkehr

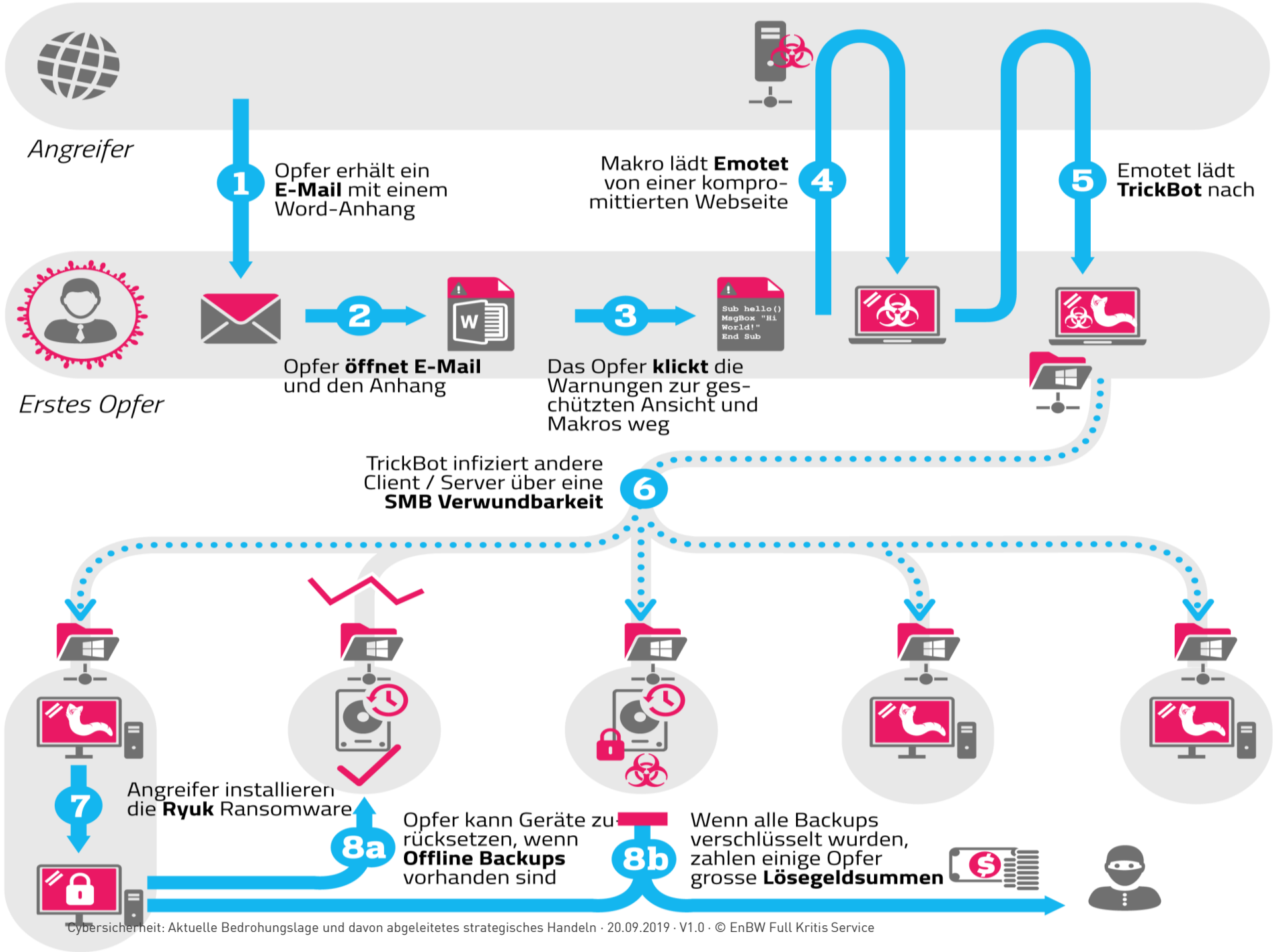
- Auch bei einem aggressiven Akt einer **Hacktivistengruppe** oder einer **staatlich gesponsorten** großflächigen **Cybersabotage** sollten **kritische Infrastrukturen** zu unser aller Wohl weiter **funktionieren**.

Störfallszenarien / Tatwaffen / Tätermodell

- **natürliche** Gefährdungen (inkl. Sonnensturm)
- **zivilisatorische** Gefährdungen
- vorsätzliche Straftaten als **Einzel-/Innentäter**
- Geschäftsmodelle f. **organisierte Kriminalität**
- spezifisches Ziel von **Hacktivistengruppen**
- staatl. Wirtschaftsspionage / Geldbeschaffung
- staatliche unterschwellige Cybersabotage
- staatlicher Hybridangriff (inkl. EMP, Jammer)

→ **exponentielle Entwicklung**, insb. für **technologie-affine Cyberkriminalität**

→ *„Machen Sie sich stets bewusst: Sie leben mit ihrem Unternehmen auf einem aktiven **Schlachtfeld zwischen Nationalstaaten**!“*
(Zitat eines bekannten Redners auf der IMI 2018)



„Emotet“ Infektionsverlauf

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

Rechtslage
Erwartbare Änderungen im IT-Sicherheitsgesetz 2.0 (ca. Ende 2019)

Ziele:

- **schneller** werden in der Prävention, mehr **Befugnisse** für Durchgriff
- **Fokus** verbreitert und konkretisiert, gleiches **Strafmaß** wie Datenschutz

Wesentliche Erwartungen:

- erheblich **tiefere Eingriffsmöglichkeiten für BSI** bei kritischen Infrastrukturen (ganzheitlicher Ansatz inkl. **Sensorik**, aber **ohne Strafverfolgungsbefugnis/-verpflichtung**)
- **erweiterter Geltungsbereich** (Kritis-Sektor **Entsorgung, Kritis-„Kernkomponenten“,** neue Kategorie „**Infrastrukturen im besonderen öffentlichen Interesse**“ z. B. Großunternehmen, Rüstung, Kultur&Medien - ohne Überwachung)
- **Optionale Erweiterungen** der Kompetenzen des BSI **bei begründetem Bedarf** (**NICHT-Kritis**-Infrastrukturen, **Kritis-Lieferanten**, Untersuchungen von Produkten und Systemen)
- etwas **mehr Rechte und Pflichten** für Kritis-Betreiber (einheitliches **Krisenkommunikationssystem, Angriffserkennungssystem, Vertrauenserklärung** der Hersteller/Lieferkette der Kritis-Kernkomponenten)
- mehr Vorbereitung und **Präventionsmaßnahmen** zur **Großkrisenbeherrschung**

Fazit

Strategische Handlungsfelder zur Ausprägung wirksamer Cyberresilienz

Vertiefung der Zusammenarbeit von Diensten und Industrie
(Handlungsspielräume für Ideen, z. B. als reguliertes Geschäft)

Begrenzung der wachsenden **digitalen Abhängigkeit der Europäer** durch **kooperative Geschäftsmodelle** (z. B. Leuchtturm-Zweckverbände, nur so hinreichende Skalierung)

gesicherte Branchennetze als Basis für weitere Digitalisierung (z. B. mit zentralem **Landesmasterplan Glasfaser und Cybersicherheit 2025** statt kommunaler Einzel-Förderung)

(Cyber-)**Störfallszenarienbetrachtung** für realistische, mehrschichtige, staatliche Cyberangriffe, zur Sicherstellung des **Betriebs kritischer Infrastrukturen auch in Großkrisen / Cyberkrieg**

mehr Sicherheit, Standardisierung und Effizienz durch **Zentralstrukturen,** zur **Bündelung der Mittel und Kompetenzen** im Ländle (nur so Dynamik beherrschbar)

stärkere Landesvorgaben, Schaffung eines kosten-gedeckten **Leistungsangebots für Informationssicherheit** als **zentraler Service und Standortfaktor**

Baden-Württemberg kann Pionier werden, wenn die Umsetzung jetzt gebündelt gestartet wird.

Vielen Dank.

Nutzen auch Sie die Erfahrung der EnBW AG.

EnBW Full Kritis Service – 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

enbw.com/kritis

EnBW