CCCamp 2019

Manuel (HonkHase) Atug

#Defensive statt #Offensive am Beispiel von KRITIS (aka Ethik rekalibrieren)

Manuel (HonkHase) Atug

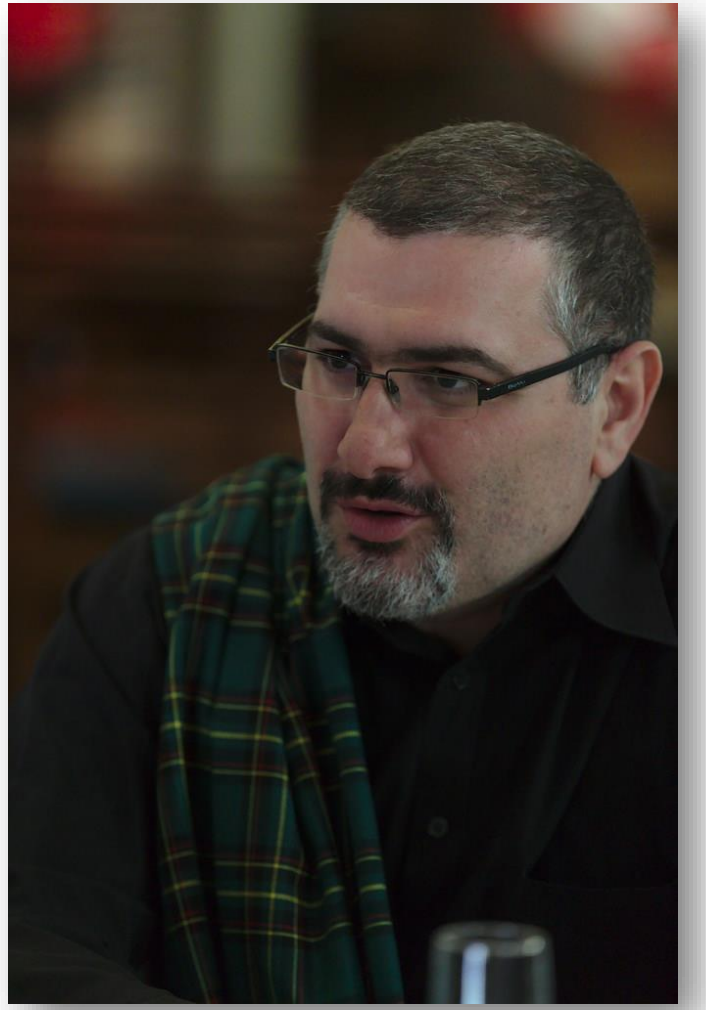
Manuel (HonkHase) Atug

- Senior Manager bei der HiSolutions AG
- Diplom-Informatiker & Master of Science in Applied IT Security
- seit über 23 Jahren in der Informationssicherheit tätig
- Spezialthemen: KRITIS und Ethik

Seit ~23 Jahren Aktiv in so n paar Vereinen:

- Chaos Computer Club e.V., Chaos Computer Club Cologne e.V., c-base e.V., Digitale Kultur e.V., ISACA, GI e.V., FIfF e.V., Freie Software Freunde e.V., Geraffel Core Member
- Leitung der AG KRITIS: https://ag.kritis.info
- @HonkHase

AG KRITIS

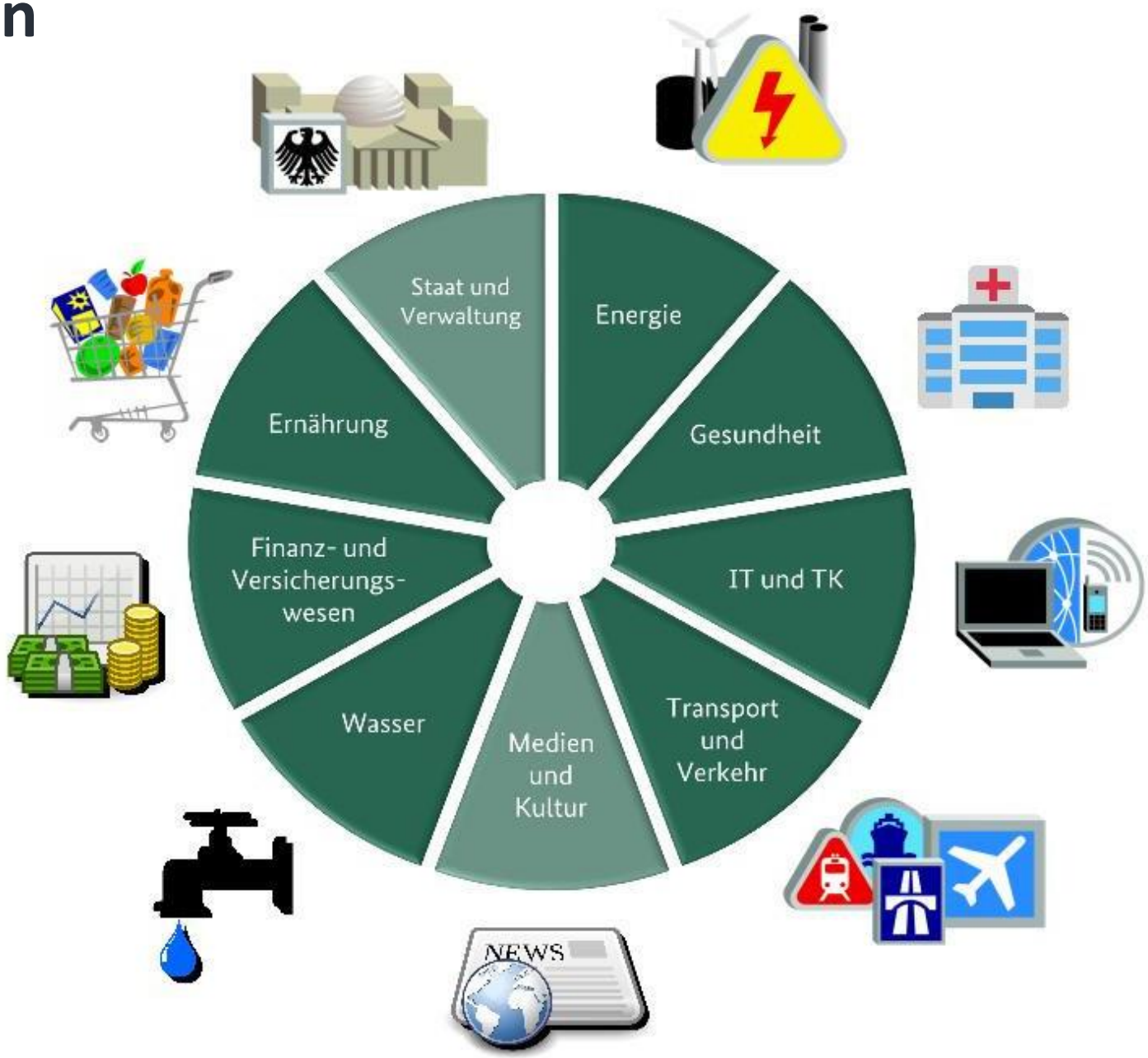


Warum Defensive statt Offensive?

Kritische Infrastrukturen…

- Eine Gesellschaft ohne Strom oder Trinkwasser ist undenkbar
- Diese unverzichtbaren Grundlagen der Gesellschaft werden Kritische Infrastrukturen (KRITIS) genannt
- Kritische Infrastrukturen sind in neun unterschiedliche Sektoren aufgeteilt, für die jeweils fachspezifische Regularien und Vorschriften existieren

KRITIS Sektoren



Quelle: BSI

KRITIS in Deutschland

- Primärziel: Vermeidung von Versorgungsengpässen für die Gesamtbevölkerung
- Ansatz: Sicherheit der IT-Komponenten von kritischen Infrastrukturen
- Rechtlich verbindlich ab einer Versorgung von mindestens 500.000 Bürgern

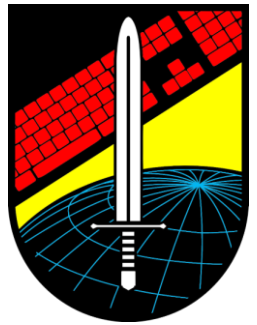
- KRITIS: primär Schutz der Bevölkerung, nicht des Betreibers
- Kritische Infrastrukturen: oftmals identische Komponenten
- Vernetzung: Immer mehr Komponenten werden an das Internet verbunden
- Durch den Staat zurückgehaltene 0day Lücken in kritischen Infrastrukturen bedrohen die Bevölkerung
- Cyberabwehr in Defensive statt „aktive Cyberabwehr“ in Offensive (Hackback), so dass kritische Infrastrukturen nicht gefährdet, sondern geschützt werden

#Cyberwar und #HackBack

- KDOCiR (Kommando Cyber- und Informationsraum)
  - Zentrum Cyber Operationen (ZCO)
    - Kernauftrag des ZCO ist das Planen, Vorbereiten und **Führen** von Cyber-Operationen (CO) zur Aufklärung und **Wirkung** (durch Cyber-Wirkketten)

Interne Verbands-abzeichen:

KDOCiR



ZCO

Rechtlicher und organisatorischer Rahmen?

- Rechtliche Fragen zu #Hackback und aktive Cyberabwehr sind seit Jahren in Arbeit
- Bundesregierung (Drucksache 19/11920) geht von digitalen Cyberwaffen auf kritischer Infrastruktur in Deutschland aus
- Kauf & Entwicklung von digitalen Cyberwaffen durch die Bundesregierung wird explizit nicht verneint. „nur deren Einsatz“

Preisliste für digitale Cyberwaffen

Capabilities	Apple iOS
Component	Any default component
First stage	Remote Code Execution
Second stage	Privilege Escalation
Interaction	**No user interaction**
Persistency	✔
Payout	**Up to 4.0M USD**

Second stage	Sandbox Escape and Privilege Escalation	Privilege Escalation	Privilege Escalation	Privilege Escalation
Interaction	Browse a web page	**No user interaction**	Run exploit in VM	Run exploit in VM
Payout	**Up to 1.5M USD**	**Up to 1.0M USD**	**Up to 500K USD**	**Up to 250K USD**

Bugfense Zero-Day Hitlist http://bugfense.io/index.html

#Cyberwar und #HackBack

- Gelebt wird eine **wissenschaftsfeindliche Sicherheitspolitik** (wie bei der Klimapolitik)
- Mehr Security?
- Nope -> mehr Cyber**UN**sicherheit

Wünsch Dir was!

Marktpreise für 0days…

…sind nicht zu unterschätzen, Staaten feuern den Markt an

4 Mio wurden dem BKA bereitgestellt, um 0days kaufen zu dürfen

BKA bezahlte knapp 6 Millionen Euro für Staatstrojaner

Schon vor zehn Jahren hat das BSI dem Bundeskriminalamt bei der Programmierung eines Staatstrojaners geholfen und Quellcode beigesteuert

Das BKA besitzt mittlerweile gleich drei einsatzbereite Staatstrojaner

Was man haben will: Kein legaler Handel von 0days, keine Beteiligung durch Staaten!

Vulnerabilities Equities Process? Nein Danke!

Forderungen des BMI

- Der Staat hortet 0days via Vulnerabilities Equities Process (VEP) nach US-Vorbild
- Mitnahmegeschäft: BSI hat dann einen weiteren Zielkonflikt #Defensive vs. #Offensive (vgl. Staatstrojaner)

Was man haben will: die Ächtung digitaler Waffen!

“Aktive Cyberabwehr” aka #Hackback

Forderungen des BMI

- Computer Network Intervention (CNI):
  Cyberwar führen, baut dazu bis 2021 die Streitkräfte aus (KdoCiR)
- BND ebenfalls geeignet…
- Cyber-Abwehrzentrum (Cyber-AZ) bewertet & entscheidet
  -> danach Gremium (Kanzleramt, Auswärtiges Amt, BMJV + BMI)

Was man haben will: Eine defensive Cybersicherheitsstrategie & Evaluierung der vorhandenen Gesetze und Maßnahmen!

“Aktive Cyberabwehr” aka #Hackback

Forderungen des BMI

- **Änderung von IT-Sicherheitsgesetz 2.0 & Änderung von Verfassungsschutzgesetz**
- **Internes Eckpunktepapier mit 4-Stufen-Plan**
  - „Stilllegen“ von Internetleitungen & Servern, von denen eine Cyberattacke ausgeht
  - Fremdes Netzwerk hacken, Daten verändern oder Daten löschen

Was man haben will: Eine defensive Cybersicherheitsstrategie & Evaluierung der vorhandenen Gesetze und Maßnahmen!

Decrypt --all Messenger*.*

Forderungen des BMI

- Nach Vorbild der Australier (Gesetz zur "Beihilfe und zum Zugang" zu Telekommunikation):
  Einsichtnahme in alle verschlüsselten Messenger-Texte (Exfiltration)
- **Australier: Staatstrojaner, Backdoors, Zwang der Anbieter**
- **Deutschland: „auf richterliche Anordnung Chats in lesbarer Form an Behörden geben“**
  Gilt für alle Messenger: Whatsapp, Threema, Signal, Telegram

Änderung des Grundgesetz ist dafür erforderlich!

Juni 2019 geheim tagender Bundessicherheitsrat

Was man haben will: Eine starke Verschlüsselung ohne Hintertüren!

Herr Horst Seehofer
Bundesminister des Innern, für Bau und Heimat

- **Herr Vitt**
  Staatssekretär; Beauftragter der Bundesregierung für Informationstechnik
  - **Herr MinDir Könen**
    Abteilung CI Cyber- und Informationssicherheit
  - **Herr MinR Dr. Grosse**
    Referat CI 6
    Grundsatz Cyberfähigkeiten der Sicherheitsbehörden

Wieso #Defensive statt #Offensive am Beispiel von KRITIS

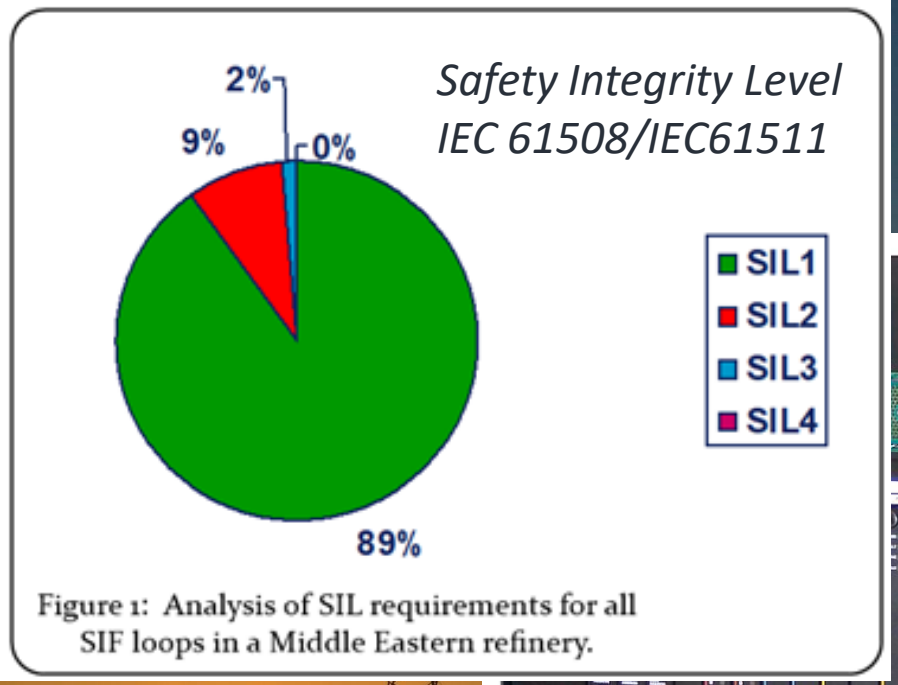


Figure 1: Analysis of SIL requirements for all SIF loops in a Middle Eastern refinery.

Triconex Tricon

Attacken auf das Ukrainische Stromnetz

- Dezember 2015 + Dezember 2016
- Auswirkungen: ca. 250.000 betroffene Personen in Kiew und dem Umfeld
- **TRITON: passiver Implant mit Remote Access Funktion**

Safety-PLC gemäß Safety Instrumented System (SIL3)
Firmware wurde im RAM gezielt manipuliert

Cyber-Angriffe

- Deutsche Energiebranche in 2017 und 2018 Ziel von großangelegten weltweiten Cyber-Angriffskampagnen
- Laut BSI „keine Hinweise“ auf erfolgreiche Zugriffe auf Produktions- oder Steuerungsnetzwerke
- Erfolgreiche Angriffe sind keine Theorie!

Daher müsse man das IT-Sicherheitsgesetz fortschreiben

Weitere Angriffe und Ausfälle in 2018

Angriffe:

- US-Krankenhaus von Ransomware teilweise lahmgelegt

Ausfälle:

- Schwere Computerpanne am Frankfurter Flughafen
- USV Ausfall bei einem deutschen Hoster
- Computerausfall der europäischen Flugsicherung Eurocontrol
- Belgischer Luftraum durch technische Probleme gesperrt
- Kfz-Zulassung in ganz Deutschland ausgefallen
- Flugbetrieb in Hamburg nach Stromausfall eingestellt

Und nun?

- Unabhängigkeit des BSI vom BMI
- Strikt defensive Cybersicherheitsstrategie
- Ächtung von ABCD-Waffen (inkl. Digitalen Waffen)
- Evaluierung der vorhandenen Gesetze und Maßnahmen
- Bevölkerungsschutz durch fixen von Schwachstellen durch Hersteller

Strikt defensive Cybersicherheitsstrategie

- Im KRITIS-Umfeld eingesetzte Software grundsätzlich als Open Source oder Quellcode in treuhänderischer Verwaltung
- Keine Bereitstellung von Budgets für Behörden, Dienste und Agenturen, um 0days kaufen zu dürfen
- Verpflichtung für alle Behörden, Dienste und Agenturen, ihnen bekannt gewordene Schwachstellen über das BSI an den Hersteller zu melden

Unabhängigkeit des BSI

Evaluierung aller Optionen (fachliche Unabhängigkeit, starke Unabhängigkeit, andere Abhängigkeit, Digitalministerium)

Vielversprechende Option: § 1 BSIG Änderung zur Grundlage technisch-wissenschaftlicher Erkenntnisse

„Das BSI führt seine Aufgaben auf der Grundlage wissenschaftlich-technischer Erkenntnisse nach den Anforderungen der jeweils fachlich zuständigen Ministerien durch.“

What‘s Next?

@HonkHase

HonkHase@kritis.info

www.blablasecurity.de

ag.kritis.info

AG KRITIS