BerlinSides X

#Defensive statt #Offensive
(aka Ethik rekalibrieren)

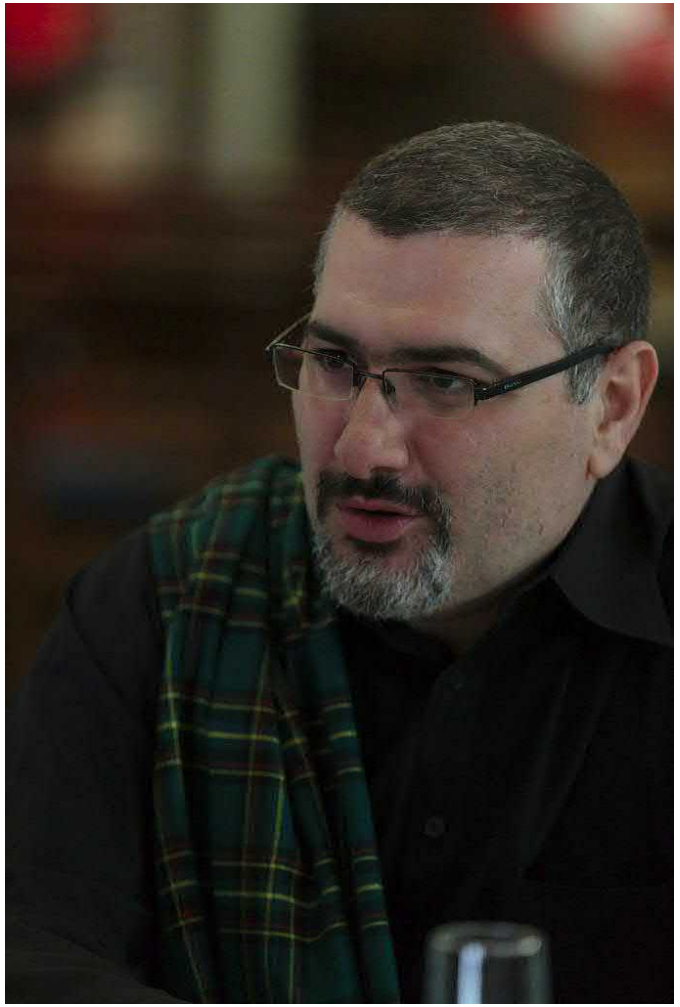
Manuel (HonkHase) Atug

Über mich
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



AGENDA

1. Warum Defensive statt Offensive?
2. Wünsch Dir was!
3. Wieso Defensive statt Offensive am Beispiel von KRITIS
4. Und nun?

1. Warum Defensive statt Offensive?

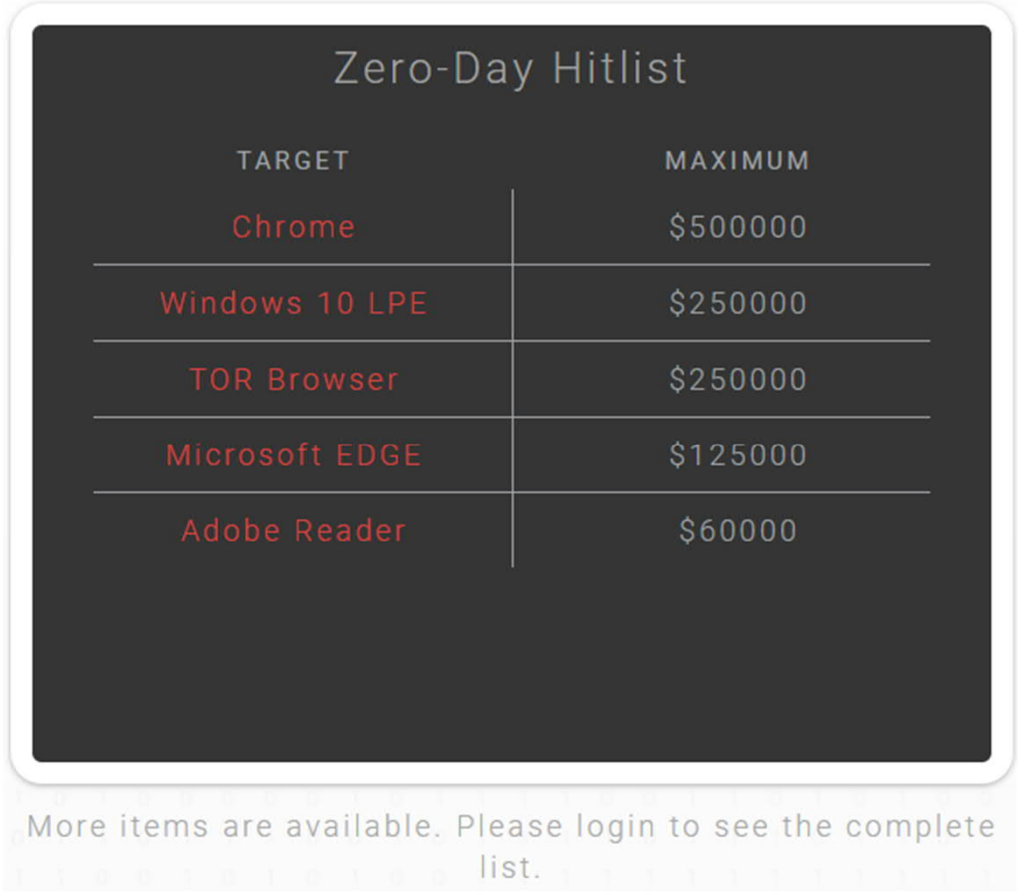
Wie alles halt so anfängt…

- 2018 gab es eine Offensive Con in Berlin, die ich verschmäht hatte! Geht ja garnicht!!!eins!!elf!!
- Teilnehmer berichteten von 0day-Händlern vor Ort und den Marktpreisen für „Government“
- Ich wollte mir ein eigenes ethisches Bild in 2019 machen… habe aber kein Ticket erhalten.
- Un wat nu?

1. Mit Geraffel, c-base und anderen Defensive diskutieren statt Offensive zu beobachten und nix zu tun!
2. Vorträge zu Defensive statt Offensive halten, um sich zu Ethik auszutauschen & zu rekalibrieren

DefensiveCon 2020
Am 7.2.-8.2.2020
Freitag & Samstag
auf der c-base

Preisliste Exodus Intelligence - Zero-Day Hitlist



Exodus Intelligence Zero-Day Hitlist https://rsp.exodusintel.com

Preisliste von Zerodium

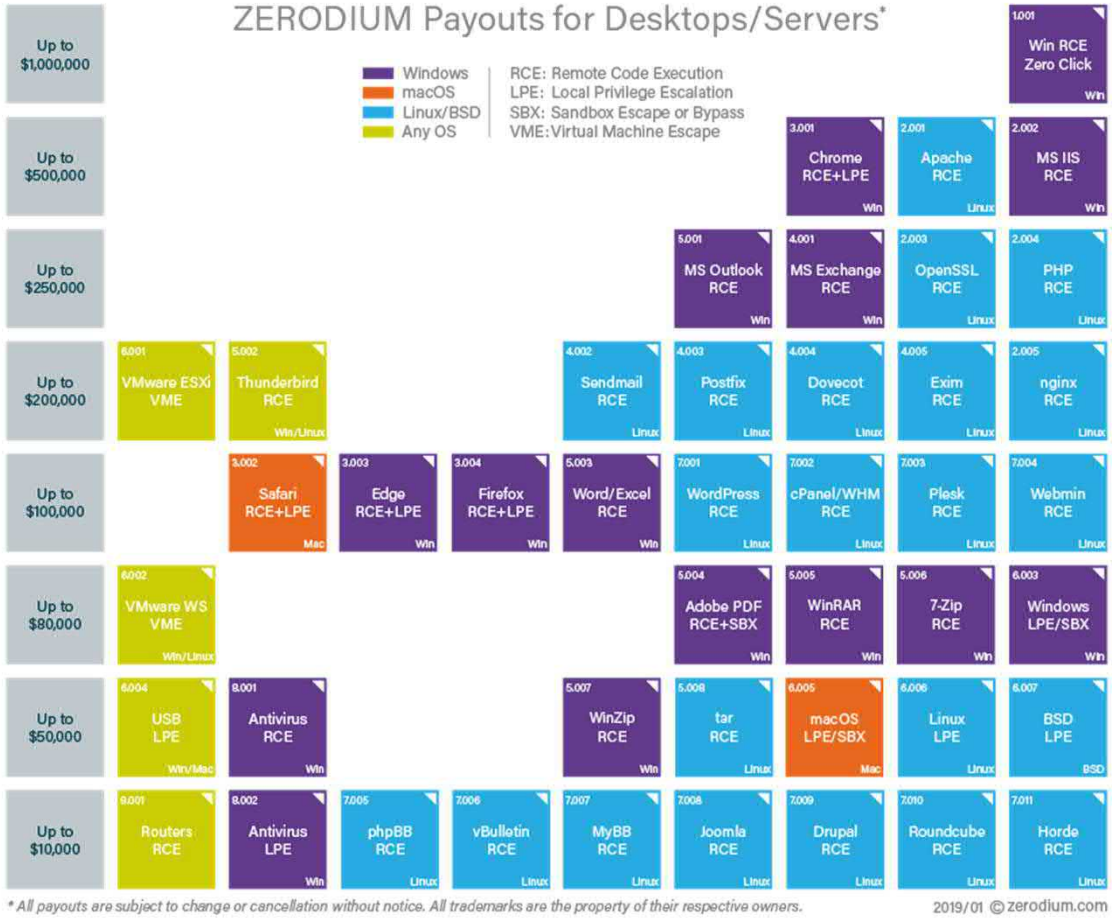
New Payouts Highlights

Jan. 7, 2019 - Payouts for the majority of Desktops/Servers and Mobile exploits have been increased. Major changes are highlighted below:

Modification	Details
Increased Payouts (**Mobiles**)	**$2,000,000** - Apple iOS remote jailbreak (Zero Click) with persistence (previously: **$1,500,000**) **$1,500,000** - Apple iOS remote jailbreak (One Click) with persistence (previously: **$1,000,000**) **$1,000,000** - WhatsApp, iMessage, or SMS/MMS remote code execution (previously: **$500,000**) **$500,000** - Chrome RCE + LPE (Android) including a sandbox escape (previously: **$200,000**) **$500,000** - Safari + LPE (iOS) including a sandbox escape (previously: **$200,000**) **$200,000** - Local privilege escalation to either kernel or root for Android or iOS (previously: **$100,000**) **$100,000** - Local pin/passcode or Touch ID bypass for Android or iOS (previously: **$15,000**) NOTE: Payouts were also increased for other products including: RCE via documents/medias, RCE via MitM, ASLR or kASLR bypass, information disclosure, etc.
Increased Payouts (**Servers/Desktops**)	**$1,000,000** - Windows RCE (Zero Click) e.g. via SMB or RDP packets (previously: **$500,000**) **$500,000** - Chrome RCE + SBX (Windows) including a sandbox escape (previously: **$250,000**) **$500,000** - Apache or MS IIS RCE i.e. remote exploits via HTTP(S) requests (previously: **$250,000**) **$250,000** - Outlook RCE i.e. remote exploits via a malicious email (previously: **$150,000**) **$250,000** - PHP or OpenSSL RCE (previously: **$150,000**) **$250,000** - MS Exchange Server RCE (previously: **$150,000**) **$200,000** - VMWare ESXi VM Escape i.e. guest-to-host escape (previously: **$100,000**) **$80,000** - Windows local privilege escalation or sandbox escape (previously: **$50,000**) NOTE: Payouts were also increased for other products including: Thunderbird, VMWare Workstation, Plesk, cPanel, Webmin, WordPress, 7-Zip, WinRAR, etc.

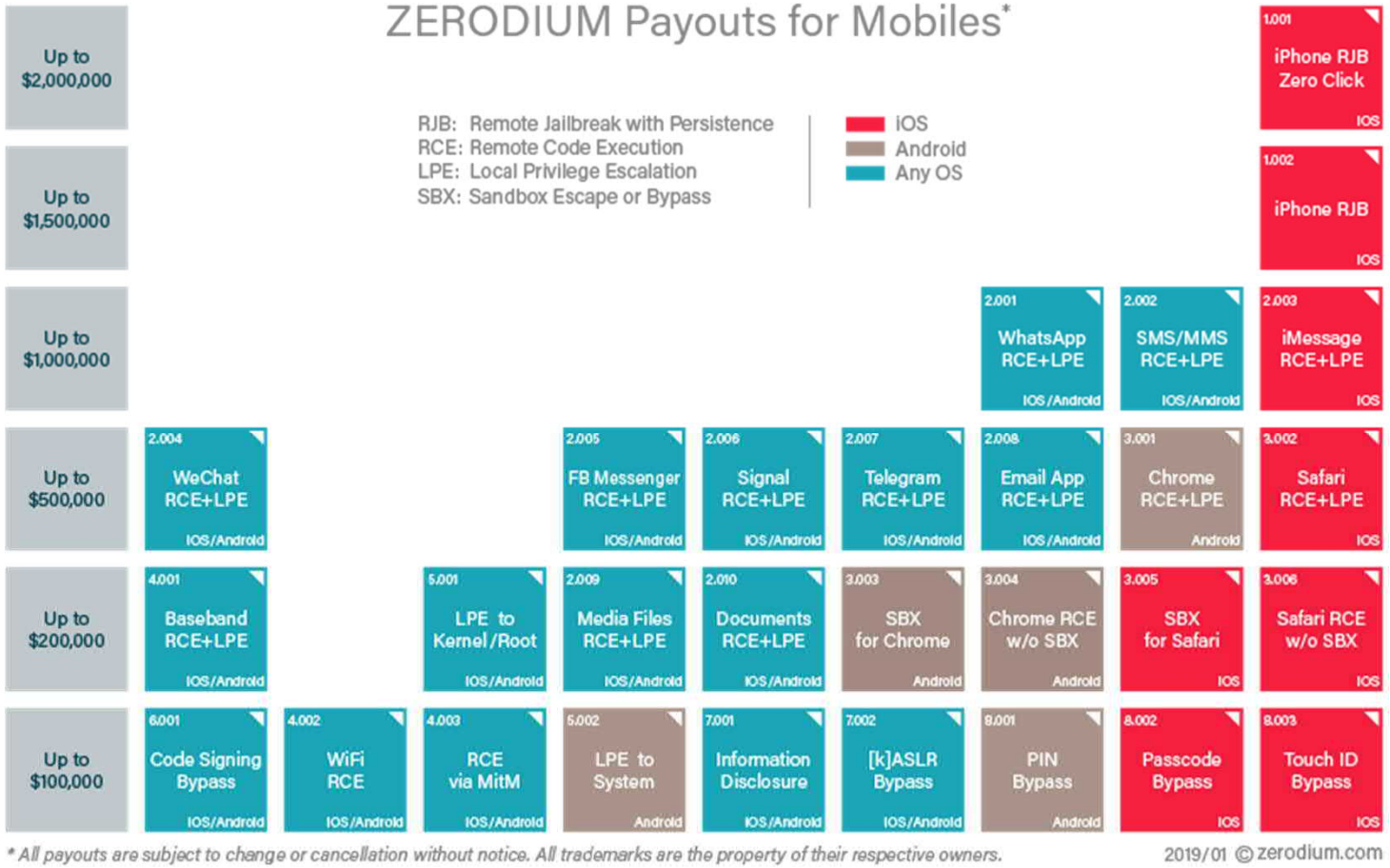
Zerodium Hit List https://www.zerodium.com/program.html

Preisliste von Zerodium - Desktop / Server



Zerodium Hit List (Desktop / Server) https://www.zerodium.com/program.html

Preisliste von Zerodium - Mobiles



Zerodium Hit List (Mobiles) https://www.zerodium.com/program.html

Preisliste Bugfense - Zero-Day Hitlist

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

2. 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!

https://netzpolitik.org/2018/it-sicherheit-das-bka-verhindert-dass-sicherheitsluecken-geschlossen-werden/

Vulnerabilities Equities Process? Nein Danke!

Neueste Forderungen

- Das BMI wünscht:
  dass der Staat 0days horten darf und
  einen Vulnerabilities Equities Process (VEP) nach US-Vorbild aufsetzt

- Die Stiftung Neue Verantwortung singt im Lied fröhlich mit:
  Schwachstellen-Management für mehr Sicherheit
  Wie der Staat den Umgang mit Zero-Day-Schwachstellen regeln sollte

Was man haben will: die Ächtung digitaler Waffen!

“Aktive Cyberabwehr” aka Hackback

Neueste Forderungen

- Das BMI wünscht "Computer Network Intervention" (CNI):
  Cyberwar zu 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)

- **Änderung von IT-Sicherheitsgesetz 2.0 & Änderung von Verfassungsschutzgesetz**
  Internes Eckpunktepapier mit 4-Stufen-Plan
  - „Stilllegen“ von Internetleitungen & Servern, von dem 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*.*

Neueste Forderungen

- Das BMI wünscht nach dem Vorbild der Australier (Gesetz zur "Beihilfe und zum Zugang" zu Telekommunikation):
  Einsichtnahme in alle verschlüsselten Messenger-Texte

- **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!

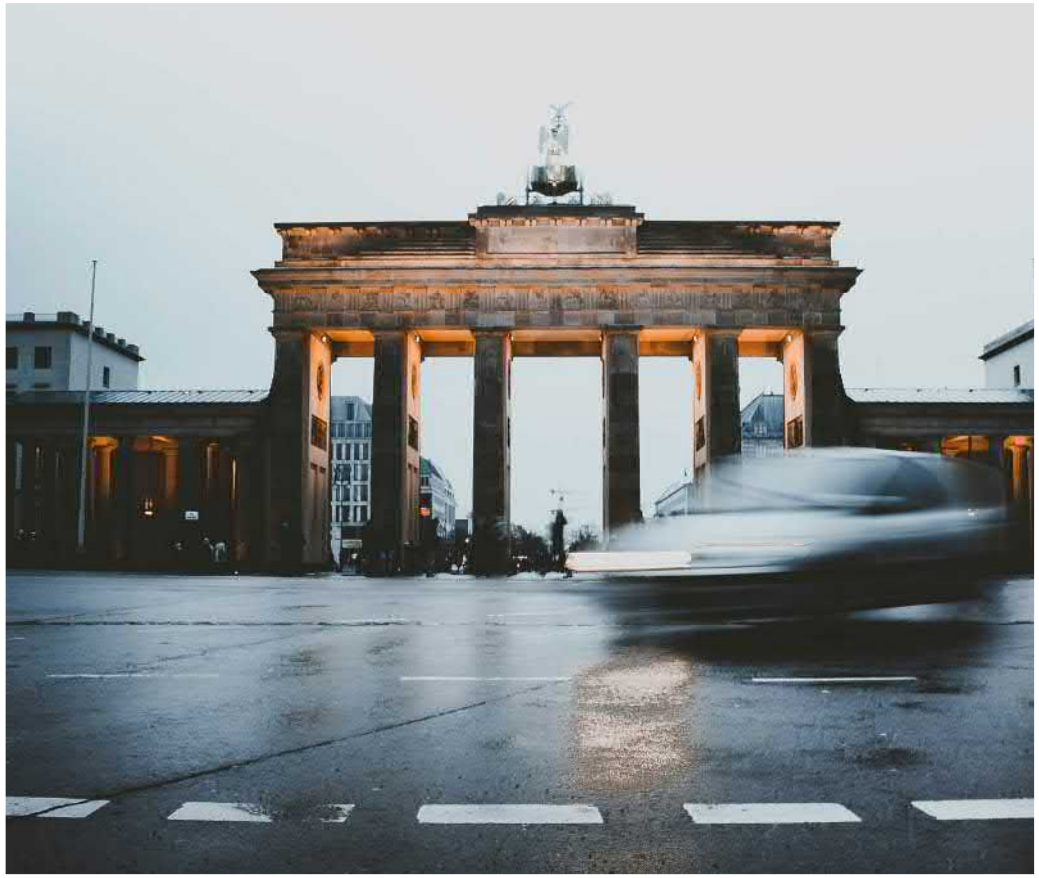
Wer beim BMI?

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

3. Wieso Defensive statt Offensive am Beispiel von KRITIS

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
- Sektoren aktuell: Energie, IT & TK, Transport & Verkehr, Gesundheit, Wasser, Ernährung, Finanzen & Versicherungen

Attacken auf das Ukrainische Stromnetz

Zielgerichtete Angriffe auf die Stromversorgung

- Dezember 2015
- Wiederholte Attacke im Dezember 2016
- Auswirkungen: ca. 250.000 betroffene Personen in Kiew und dem Umfeld

Firmware der Stromunterbrecher wurde gezielt manipuliert

Cyber-Angriffe auf deutsche Energieversorger

2017 und 2018 erfolgte eine Reihe großangelegter weltweiter Cyber-Angriffskampagnen

Cyber-Angriffe

- Deutsche Unternehmen aus der Energiebranche waren und sind 2017 und 2018 das Ziel von großangelegten weltweiten Cyber-Angriffskampagnen.

- Laut BSI liegen derzeit keine Hinweise auf erfolgreiche Zugriffe auf Produktions- oder Steuerungsnetzwerke vor. Es sei nur eine Frage der Zeit, bis neue, erfolgreiche Angriffe ausgeübt würden.

Daher müsse man das IT-Sicherheitsgesetz fortschreiben

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

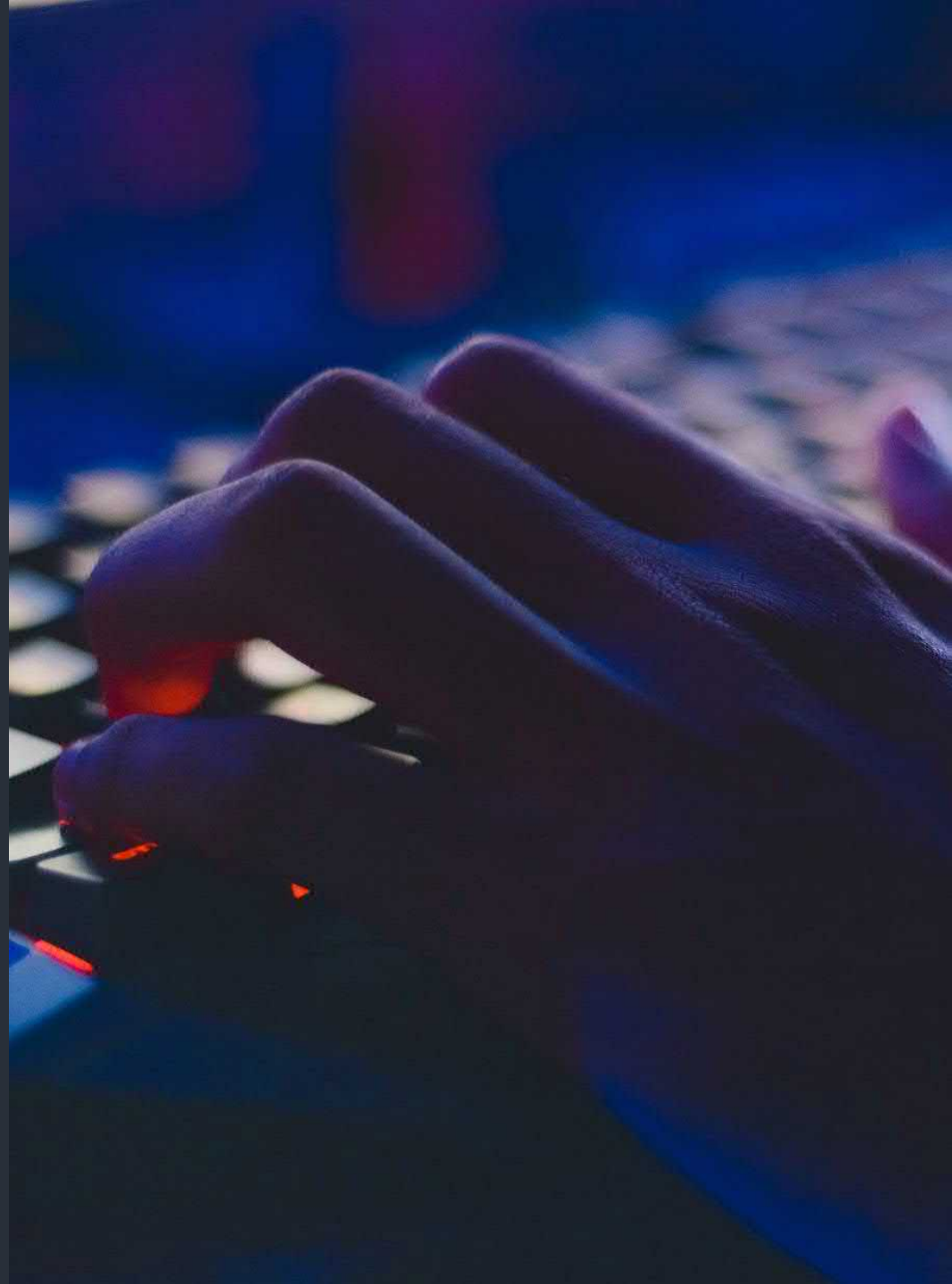
Weitere Angriffe und Ausfälle in 2018

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



- KRITIS dient primär dem Schutz der Bevölkerung, nicht des Betreibers.
- Kritische Infrastrukturen setzen oftmals identische Komponenten ein
- 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 werden!

4. Und nun?

Schlussfo[lge|rder]rung (1/2)

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

Schlussfo[lge|rder]rung (2/2)

Strikt defensive Cybersicherheitsstrategie für Deutschland!

- 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 vom BMI sicherstellen!
  1. Evaluierung aller Optionen (fachliche Unabhängigkeit, starke Unabhängigkeit, andere Abhängigkeit, Digitalministerium)
  2. 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.“

Was ihr mitnehmen solltet:

1. Wir wollen eine strikt defensive Cybersicherheitsstrategie für Deutschland
2. Wir wollen ein unabhängiges BSI, losgelöst vom BMI
3. Wir wollen keine ABCD-Waffen, auch nicht unter dem Deckmantel Staatstrojaner
4. Bevölkerungsschutz fängt bei der Kommunikation vorhandener Schwachstellen an den Hersteller

Das Leben nach der NSA?
www.kokosnusspflücker.de

Kontaktdaten:

HonkHase

honkhase@blablasecurity.de |
+49 555 FTWTFCYBERWEHR

www.honkhase.de |
www.blablasecurity.de