PrivacyWeek 2021

Manuel (HonkHase) Atug

Desolate Deutsche Netzpolitik

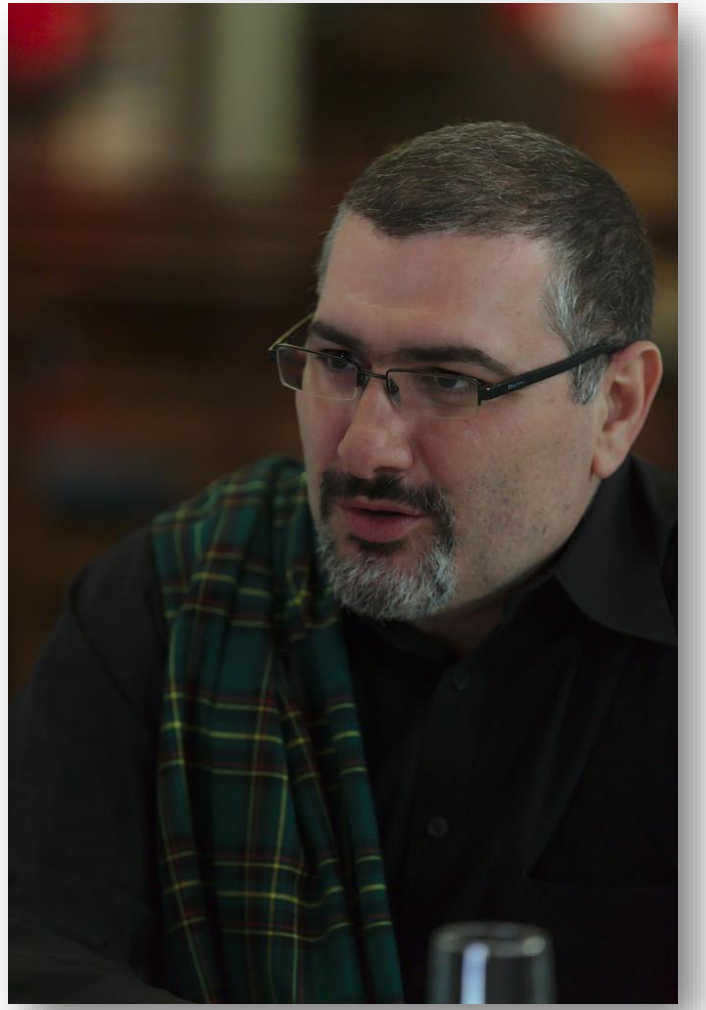
Manuel (HonkHase) Atug

Manuel (HonkHase) Atug

Ich habe #KRITIS im Endstadium

Head of Business Development bei der HiSolutions AG

- Diplom-Informatiker, Master of Science in Applied IT Security, Ingenieur
- > 23 Jahren in der Informationssicherheit tätig
- KRITIS, Hackback, Ethik, Cyberresilienz, Bevölkerungsschutz



- Gründer der AG KRITIS: https://ag.kritis.info
- @HonkHase

AG KRITIS

Cybercrime Shootingstar Ransomware

Schlimmes Cyber ist schlimm!

Mehr als 500 Millionen Dollar mit Ransomware in den USA erpresst

Mehr als eine halbe Milliarde Euro haben US-Firmen allein im ersten Halbjahr 2021 nach Angriffen mit Erpressungstrojanern gezahlt. Die Attacken werden immer häufiger.

*Durchschnittliche Lösegeldforderung auf 5,3 Millionen US-Dollar gestiegen – eine **Zunahme um 518 Prozent** (847.000 US-Dollar im Jahr 2020)*

*Durchschnittlich gezahltes Lösegeld beträgt 570.000 Dollar – ein **Anstieg um 82 Prozent** (312.000 Dollar im Jahr 2020)*

Moin Deutschland - Zufällig ausgewählte Beispiele?

RANSOMWARE

Über 100 Behörden wurden bereits gehackt und erpresst

Bisher gibt es keine offiziellen Zahlen zu Ransomware-Angriffen auf staatliche Einrichtungen. Laut einer Recherche gibt es mindestens 100 Fälle.

MALWARE

Mehrere Kliniken nach Hackerangriff vom Netz genommen

Neben den Kliniken seien auch Bildungseinrichtungen von dem Malware-Angriff betroffen. Sicherheitshalber wird nun mit Papier und Stift gearbeitet.

Läuft. Nicht.

Deutschland so: German Grundishkeit!

Deutschland wird zur Bundestrojanerrepublik

Alle 19 Geheimdienste haben ab nun die Lizenz zum Einsatz von Schadsoftware. IT-Sicherheitslücken können deshalb offengehalten werden, präventive Cyberangriffe sind die beste Verteidigung - Sicherheitsexperte Manuel Atug über die neue deutsche „Cybersicherheitsstrategie."

Wir gucken euch alle

Seit 5:23 Uhr wird zurück gecybert!

Cybersicherheit: Seehofer für Nutzung von Zero-Day-Exploits und für Hackbacks

Innenminister Horst Seehofer hat einen Entwurf für eine Cybersicherheitsstrategie vorgelegt. Er plant einen Angriff auf Verschlüsselung und mehr Staatshacking.

Digitale Souveränität? Hold my beer! Die Cybersicherheitsstrategie für Deutschland 2021

8.3.11 Die Digitale Souveränität der Sicherheitsbehörden durch den Ausbau der ZITiS stärken

Was wollen wir erreichen?
Die ZITiS wird in die Lage versetzt, Werkzeuge und Methoden zu entwickeln, zu bewerten und zentral zur Verfügung zu stellen, die den Sicherheitsbehörden ein selbstbestimmtes Handeln ermöglichen, eine krisenfeste Versorgungssicherheit gewährleisten und deren Cyberfähigkeiten signifikant stärken.

Quelle: https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cyber-sicherheitsstrategie/cyber-sicherheitsstrategie-node.html

Ja richtig gelesen. Es ging nie um eure digitale Souveränität, Ihr Pappnasen. Nur um die digitale Souveränität der Sicherheitsbehörden!

Lölz, es geht um innere Sicherheit nicht um eure

Cyber El Dorado für Nachrichtendienste

Snowden war erst der Anfang…

Globale Überwachungs- und Spionageaffäre

Die **Globale Überwachungs- und Spionageaffäre** entstand aus Enthüllungen von als Top Secret gekennzeichneten Dokumenten der National Security Agency (NSA)

Die so gewonnenen Daten werden auf Vorrat gespeichert.

Amnesty International kritisiert das neue BND-Gesetz als unzureichend in Bezug auf den Schutz der Privatsphäre. Der Bundestag hat heute das neue Gesetz zur Kontrolle des Bundesnachrichtendienstes verabschiedet. Zuvor hatte das Bundesverfassungsgericht in Karlsruhe eine bessere Kontrolle des BND gefordert.

Mehr Heu bei der Suche nach der Nadel

On a large scale: Think Big (Data)

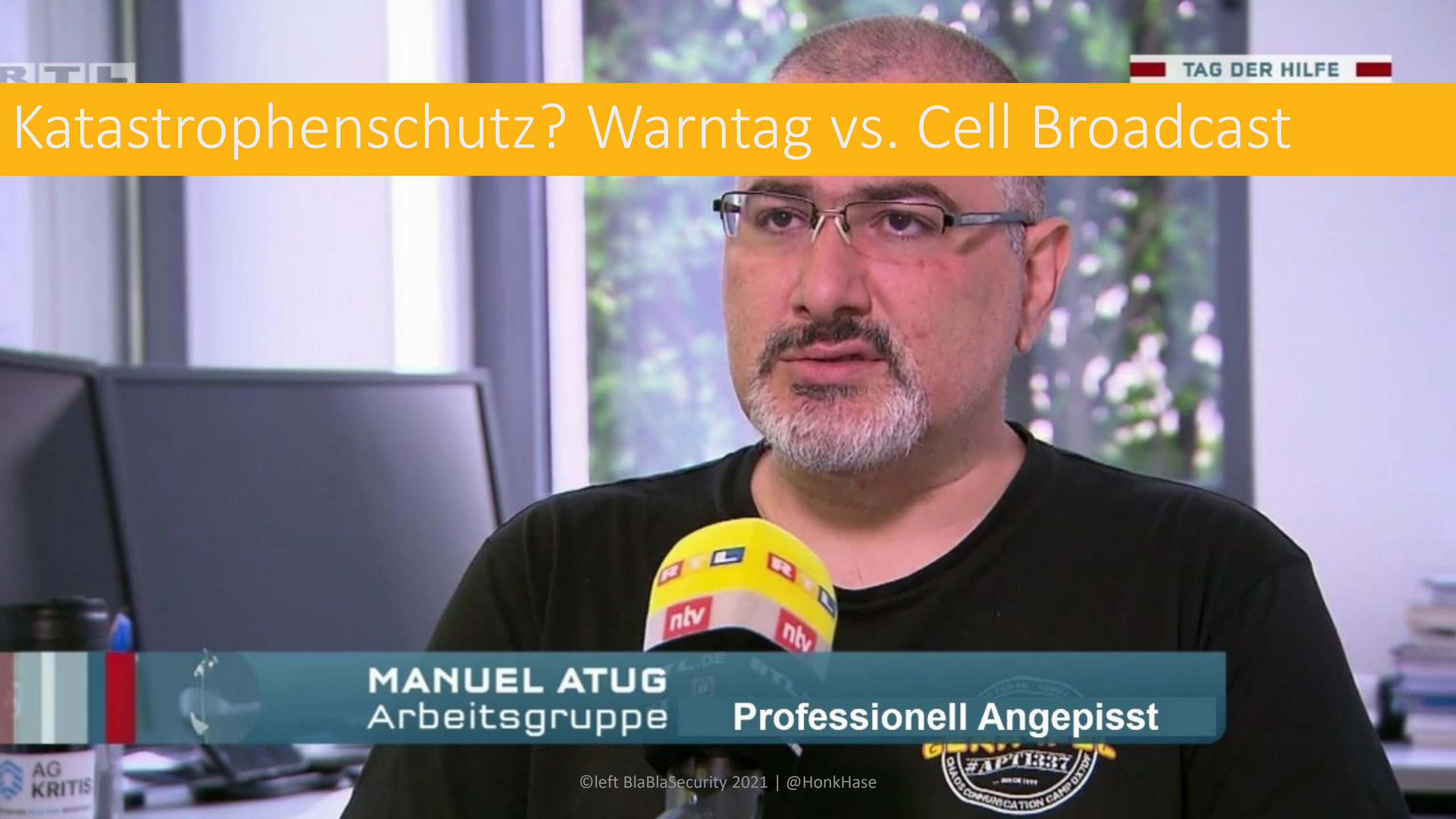
- Weltweite automatisierte Massenüberwachung in der globalen Überwachungs- und Spionageaffäre nimmt stetig und kontinuierlich zu
- Dafür optimierte Gesetze (seit 9/11) und weil wegen gegen Terrorismus & KiPo!!1!elf!!!

  https://twitter.com/HonkHase/status/1203225440313319425
- Analog hat schlecht skaliert. Siehe DDR und Orwell

- **Digitalisierung bringt Automatisierung bringt Skalierung**

- Günstige Festplatten unterstützen die Vorratsdatenmentalität der Sicherheitsbehörden und Nachrichtendienste

Katastrophenschutz? Warntag vs. Cell Broadcast



How to fail Warntag und Sirenentests?

Traurige Realität statt sinnvolles Miteinander

- Januar 2020: BBK Präsident beim Bundestagsausschuss
- ca. 30 Jahre nach letztem Test klappt das bestimmt sofort
- BBK ausschließlich für den Spannungs- und Verteidigungsfall
- Zuständig für Katastrophenschutz sind Bundesländer und nicht BBK
- Richtlinien- oder Weisungskompetenz gibt es nicht
- Ländergrenzen-überschreitende Ereignisse wie Hochwasserlagen, Cyber-Angriffe, Pandemien oder großflächige Strom- und Infrastrukturausfälle erfordern übergeordnete Führungsebene
  - Dienstvorschriften in den entsprechenden Behörden und Organisationen mit Sicherheitsaufgaben enden faktisch auf der Landesebene als höchste Instanz

Prävention ist nicht sexy

Olle Kamellen seit 1967… BBK das „das vergessene Amt“

- „Ämterwirrwarr und mangelhafte Koordination, Fehlbeschaffungen oder Fehlkonstruktionen, parkinsonsche Bürokratie wie technische Typenvielfalt stellen den Erfolg des Bonner Zivilschutzes von vornherein in Frage.“ Es gibt, so tadelte die SPD-Bundestagsabgeordnete Annemarie Renger, „viele Überschneidungen, Doppelarbeit und dadurch unnötige Kosten und leider kein Ergebnis.“ Und der Hamburger Innensenator Heinz Ruhnau spottet, es gebe „für jede Katastrophe einen besonderen Verein“

Organisations- und Fehlerkultur? Fehlanzeige!

Zukünftige Übungen? „Übung war ein voller Erfolg“

- BBK Präsident wurde anschießend Abberufen
- Scheitern bei Übungen wie dem Warntag ist keine Option!
- Desaströse Ergebnisse? Nene!
  - Übungen so wählen, das sie nix bringen
  - aber auch keine Fehlerzustände aufzeigen
  - dann gegenseitiges Schulterklopfen
  - End of Story

Mehr schlechte Laune gefällig? https://ag.kritis.info/2020/09/21/weggewarnttag-der-warntag2020/

Paradebeispiel Cell Broadcast

BMI so: nene, lass mal

- CellBroadcast gibt es seit 1999. 20 jähriges… yay!
- Nutzung in USA seit 2006 „Wireless Emergency Alerts“ (WEA). Aha.
- BMI kennt es seit 2001 (2. Gefahrenbericht der Schutzkommission). Ignore
- BnetzA beschäftigt sich 2007/2008 damit. BMI in einer Drucksache aus 2008 dazu: „Nach einem erfolgreichen Test in den Niederlanden wird dieses System im internationalen Rahmen unter Beteiligung des BBK ab 2009 untersucht“. Ende.
- Nutzung in Niederlande seit 2012 „NL-Alert“. CB-Tests erreichen mehr als 90% der Bevölkerung. Aha.

Mehr schlechte Laune gefällig? https://ag.kritis.info/2021/07/23/ab-wann-ist-etwas-grob-fahrlaessig-historie-von-cell-broadcast-in-deutschland/

Dann halt als EU-Richtlinie?

BMI so: ach nööööh

- 2018: EU-Richtlinie 2018/1972 gibt CB-Umsetzung bis Juni 2022 vor. Yay. Jetzt kommt es aber.
- Artikel 110, Absatz 2 lässt alles, was „gleichwertig“ ist, zu. Mmmh.
- Ach ja! Die Apps NINA, KATWARN usw. Exitstrategie nix tun.
- Flutkatastrophe Ahrtal. Nix geht mehr. Vermeidbare Todesfälle.
- Seehofer so: Yay Cell Boradcast und 80 Mio für Sirenen.

/me selbst betroffen gewesen https://heise.de/-6142714

KRITIS sind offenbar kritisch aber nicht resilient

Kritik wegen KRITIS wirkungslos

BMI so: Wir sind n+1 mal die Lotusblüte

- Fazit IT-SiG v1.0 in 2015?
  - Anhörung 2015: *„Worin sich alle Beteiligten einig waren ist der Punkt, dass eine Regelung von IT-Sicherheitsstandards dringend geboten ist. Dass das IT-Sicherheitsgesetz in der aktuellen Entwurfsfassung das gebotene Mittel ist, ist jedoch unwahrscheinlich.“ via netzpolitik.org*
- Fazit Anhörung IT-SiG v2.0 in 2021?
  - Ausnahmslos alle sechs Sachverständigen haben das Gesetz kritisiert und zerrissen!
  - „Gesetzentwurf nur bedingt geglückt“
  - „Handlanger der Sicherheitsbehörden und Nachrichtendienste“
  - „Unbestimmtheit der Eingriffsvoraussetzungen“ bemängelt
  - „Keine Strategie, keine Evaluierung“
  - „Ein herber Verlust für die Bürger“
  - Deutscher Bundestag titelt selbst: „Wenig Beifall für das geplante IT-Sicherheitsgesetz 2.0“

Mehr schlechte Laune gefällig? Empfehle Popcorn fürs Video https://ag.kritis.info/2020/09/21/weggewarnttag-der-warntag2020/

„Evaluierte“ BSI-Kritisverordnung 2021…

Offensichtlich „vergessene“ Fragestellungen

- Auswirkungen sektorübergreifender KRITIS Betreiber vs gemeinsam genutzte Anlagen?
- Pauschaler Regelschwellenwert von 500.000 Personen neu zu bewerten?
- Daher Ver- und Entsorgungsbetriebe von Städten wie Bielefeld, Bonn, Münster, Karlsruhe, Mannheim, Augsburg, Wiesbaden, Braunschweig oder Aachen mit ihrer Einwohneranzahl weiterhin nicht als kritischen Infrastrukturen gezählt?

Mehr schlechte Laune gefällig? https://ag.kritis.info/2020/09/21/weggewarnttag-der-warntag2020/

Es wirkt eher, als habe das BMI das Feedback der Aufsichtsbehörden und des BSI eingesammelt und in ein Update einfließen lassen. Evaluierung anyone?

Einmal mit Profis…

Wer evaluiert hat, fragt ihr?

Schauen wir mal rein:

- Es gibt es keinerlei Informationen zu Umfang, Methodik und Ergebnissen dieser Evaluierung
- Es gibt keinen Nachweis der Unabhängigkeit der Evaluierenden
- Es gibt keinen Nachweis der Expertise der Evaluierenden

Mehr schlechte Laune gefällig? https://ag.kritis.info/2021/05/07/stellungnahme-der-ag-kritis-zum-bsi-kritisv-entwurf-vom-22-04-2021/

Wie jetzt, noch mehr schlechte Laune?

Endlos weitere Beispiele…

Desolat, können wir! Hold my beer XXL

- Hackerparagraf § 202a-d StGB
  https://www.gesetze-im-internet.de/stgb/
- Akademische Experten zerlegen Überwachungspläne der EU
  https://fm4.orf.at/stories/3018803/
- Netzaktivist: „Das beste Digitalministerium bringt nichts, wenn da Dobrindt oder Scheuer sitzen“
  https://www.rnd.de/politik/netzaktivist-das-beste-digitalministerium-bringt-nichts-wenn-da-dobrindt-oder-scheuer-sitzen-7f7ecfdd-aa70-4198-9984-6fbf2bd612f9.html
- "Man muss Gesetze kompliziert machen" - Horst Seehofer
  https://www.sueddeutsche.de/politik/seehofer-datenaustauschgesetz-1.4479069
- LucaApp – der Twitter MegaThread (derzeit über 920 Einträge)
  https://twitter.com/HonkHase/status/1377129093007765507
- ID Wallet – fümpf Blockchains anoyne?
  https://lilithwittmann.medium.com/mit-der-id-wallet-kannst-du-alles-und-jeder-sein-au%C3%9Fer-du-musst-dich-ausweisen-829293739fa0
  Fachwissen und Hintergründe zu diesem Abgrund: Blockchain + SSI = ID?
  https://medium.com/@ckahlo/blockchain-ssi-id-d7e51d98d050
- CDUconnect App? Anzeige ist raus!
  https://lilithwittmann.medium.com/wenn-die-cdu-ihren-wahlkampf-digitalisiert-a3e9a0398b4d
- Modern Solution App? Hausdurchsuchung statt Dankeschön
  https://www.golem.de/news/nach-datenleck-hausdurchsuchung-statt-dankeschoen-2110-160269.html
- „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ Äh ja ne ist klar jetzt. Danke, liebe Cybersicherheitsstrategie
- Grundgesetz Änderung, damit zukünftig Hackback's durchgezogen werden können. Danke Teil 2, liebe Cybersicherheitsstrategie
- „verantwortungsvollen Umgang mit 0-day-Schwachstellen und Exploits fördern“ Danke Teil 3, liebe Cybersicherheitsstrategie
- Digitale Bildungspolitik mit Medienkompetenz und IT Knowhow? Gibt es nicht!
  Wir bleiben gefälligst eine Industrienation und Fabrikarbeiter müssen her, was für ne Informationsgesellschaft?

#anzünden oder #Brandroden?

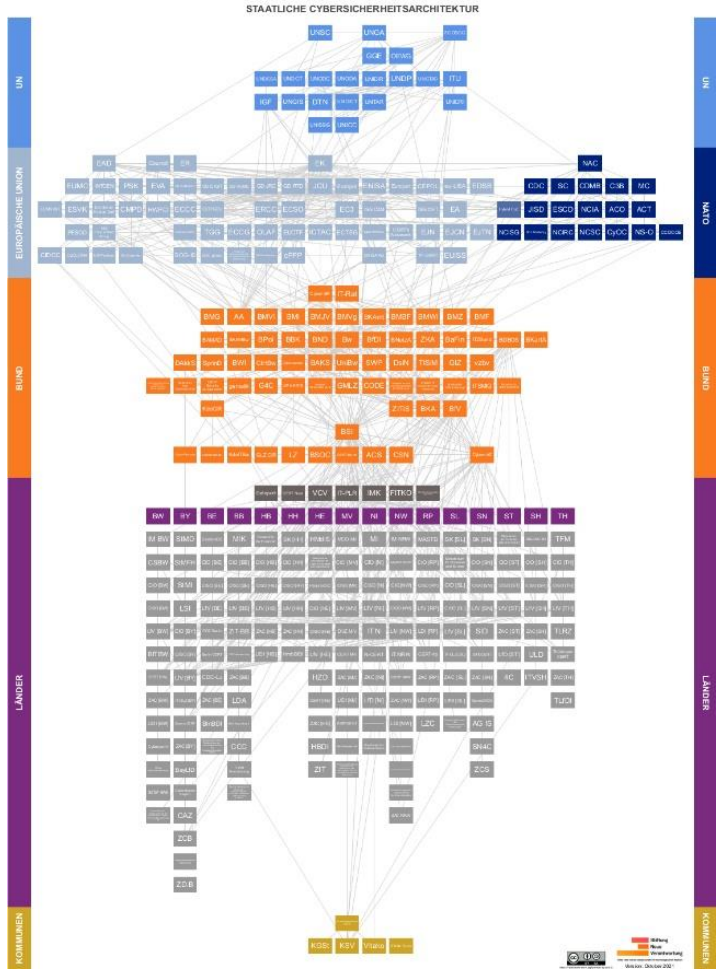
Beteiligung hoffnungslos?

Botschaft an Behörden, Politik & Wirtschaft:

Die SicherheitsforscherInnen Community sagt nicht, ob ihr unsichere Apps betreiben sollt oder nicht

Sie zeigt euch nur, wie krude defekt die sind!

Deutschlands staatliche Cybersicherheitsarchitektur



186 Seiten CybErklärBär Begleittext nötig!

Und wenn alles nicht hilft gegen den Wahnsinn?

Das Leben nach der NSA?

Kokosnusspflücker!

www.kokosnusspflücker.de