MNG Rämibühl – Blockwoche 2018

IT-Security

Zürich, 7. Februar 2018

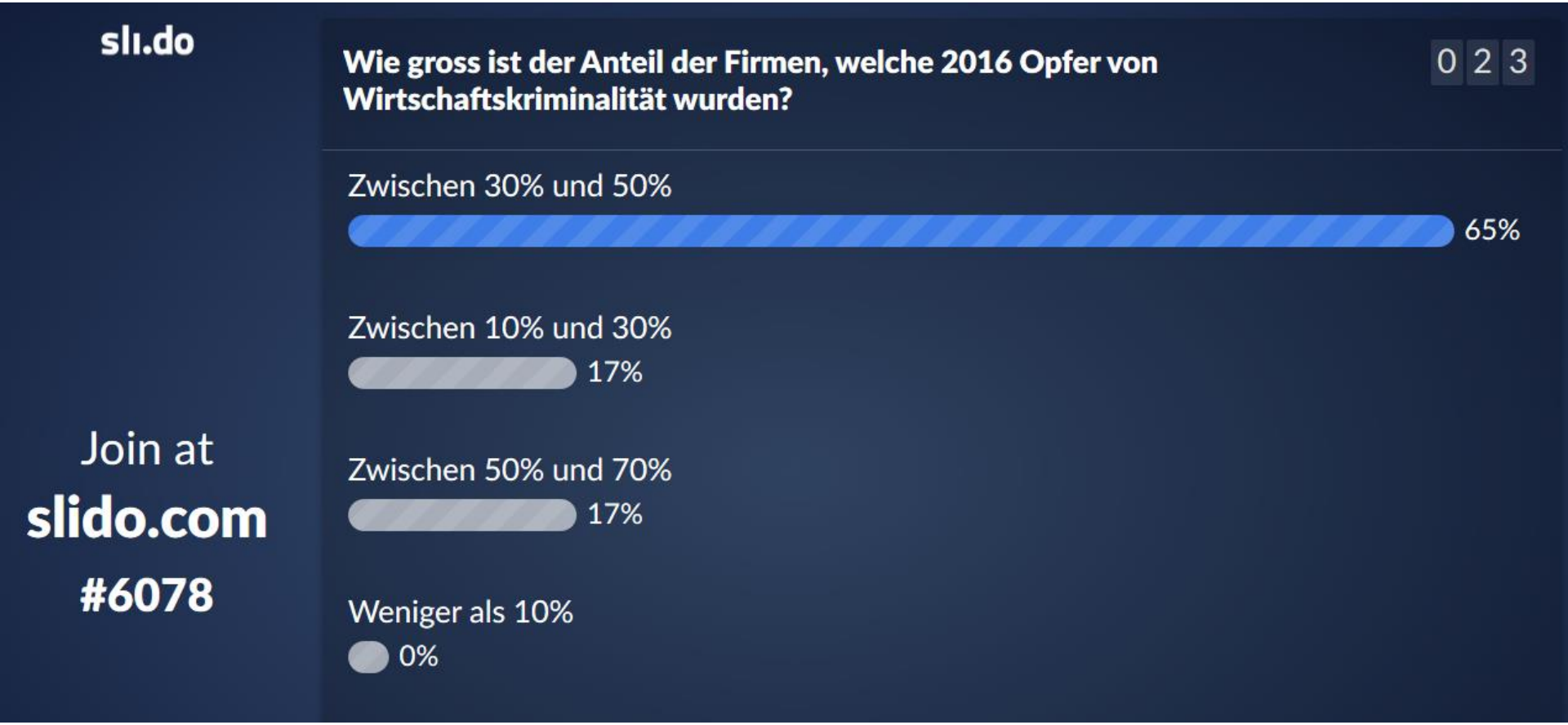
Christian Birchler

Folien: www.cnlab.ch → Publikationen

IT-Security, relevant für alle

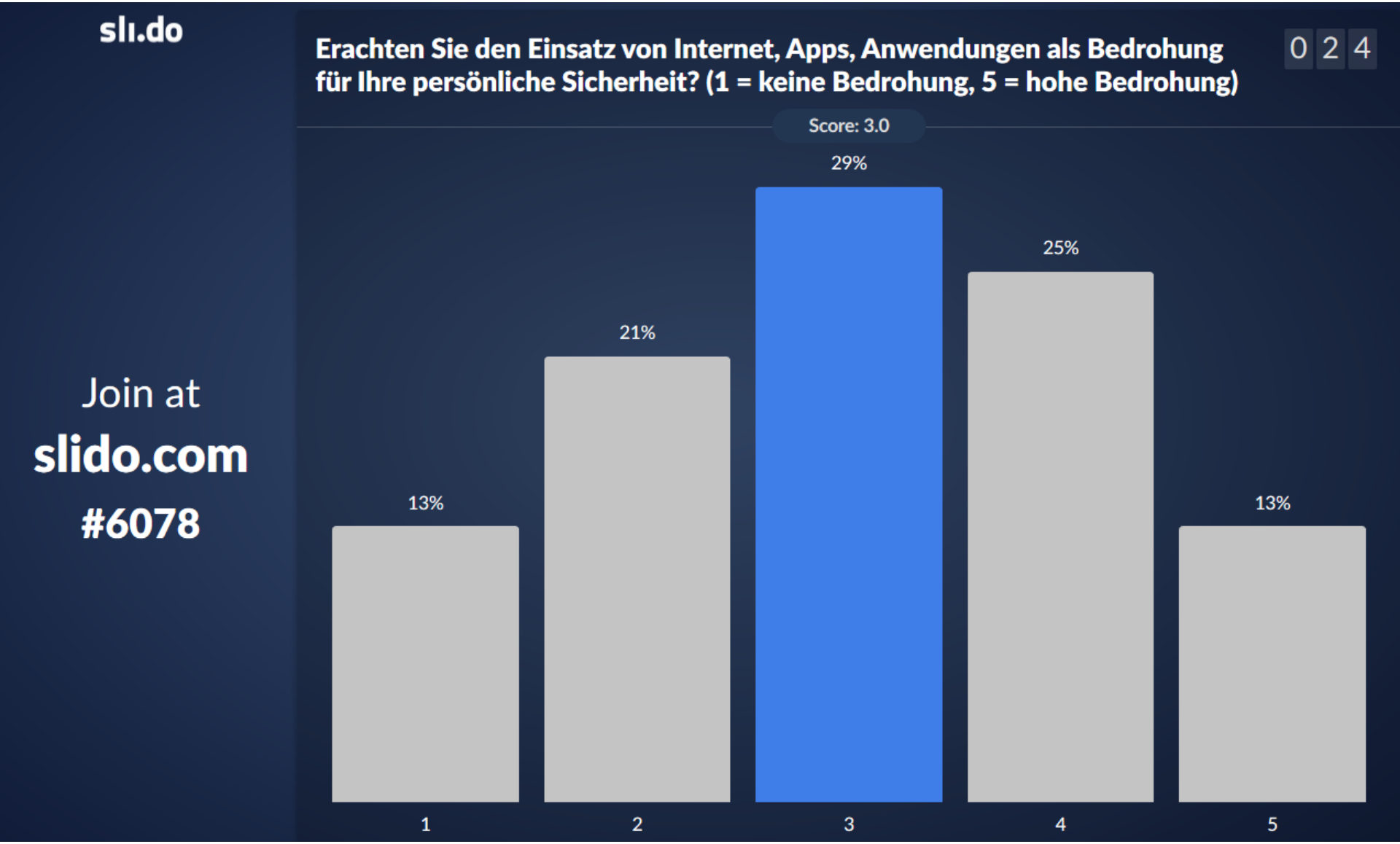
- Meine Kommunikation ist online
- Meine Informationen beziehe ich online
- Mein Geld verwalte ich online
- Meine Bewerbung erstelle und versende ich online
- Meine Abos verwalte ich online

Poll



Quelle: https://www.pwc.com (Cybercrime)

Poll



Quelle: https://www.pwc.com (Cybercrime)

IT-Security ist aktuell!

netzwoche NEWS STORYS MEINUNGEN STUDIEN DO

Statistik des Hasso-Plattner-Instituts

Noch nie gab es so viele Sicherheitslücken wie 2017

Mi 31.01.2018 - 15:18 Uhr | Aktualisiert 31.01.2018 - 15:18
von Oliver Schneider

Das Hasso-Plattner-Institut hat 2017 mehr als 11'000 Software-Sicherheitslücken registriert. Damit erreichte die Zahl der Schwachstellen einen Rekordwert. Probleme ortet das HPI vor allem bei veralteter Software und im Internet der Dinge.

(Source: REDPIXEL.PL / Shutterstock.com)

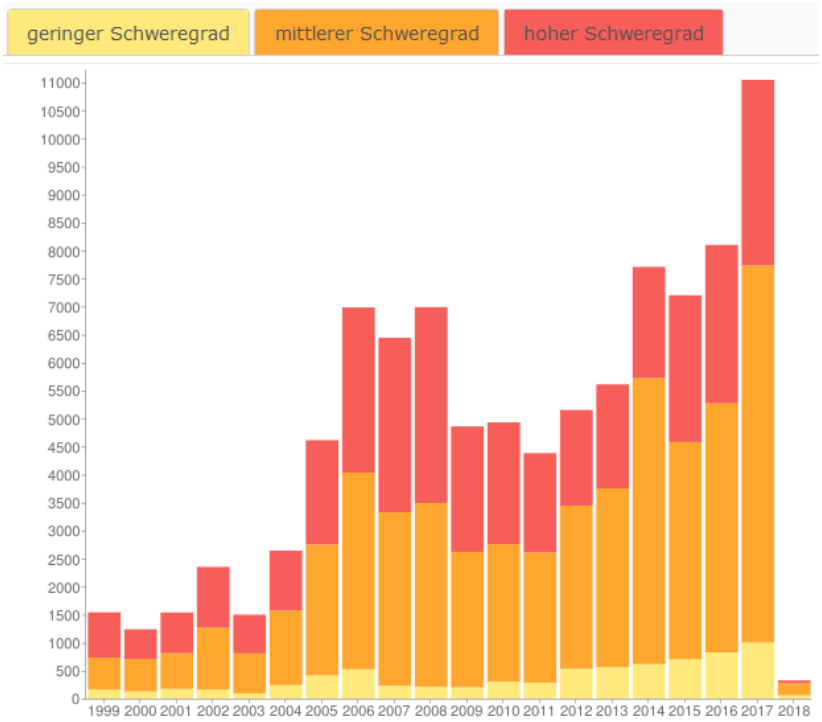
Das Potsdamer Hasso-Plattner-Institut (HPI) hat aus Anlass des E
Datenschutztages Statistiken zur Zahl der global registrierten Sof
Sicherheitslücken veröffentlicht. Wie das HPI in einer Mitteilung s
die Schwachstellen im vergangenen Jahr einen Rekordwert von 11
3000 mehr, als das Institut 2016 registriert habe.

gere Kolle. Esse ich Goji-Beeren, ist das ein Statement.

Lockerer Umgang mit Smartphones

BERN. Letzte Woche wurde bekannt, dass die Sicherheit von US-Soldaten möglicherweise gefährdet ist, weil eine Fitness-App ihre Laufrouten aufgezeichnet hatte. In der Schweizer Armee ist man im Umgang mit solchen Programmen relativ locker. «Wenn eine Übung an einem geheimen Ort durchgeführt wird, können die Kommandanten die Smartphones der Militärangehörigen kurzfristig einziehen», sagte Armeesprecher Daniel Reist gestern. So soll verhindert werden, dass Ortungsdienste von Smartphones den Standort bekannt geben. Verordnungen zur Nutzung des Smartphones oder von Programmen gibt es aber keine. SDA

Zahl des Tages



Zahl der vom HPI seit 1999 verzeichneten Software-Schwachstellen. (Source: Screenshot hpi-vdb.de/HPI)

Quelle: 20minuten, 6. Februar 2018

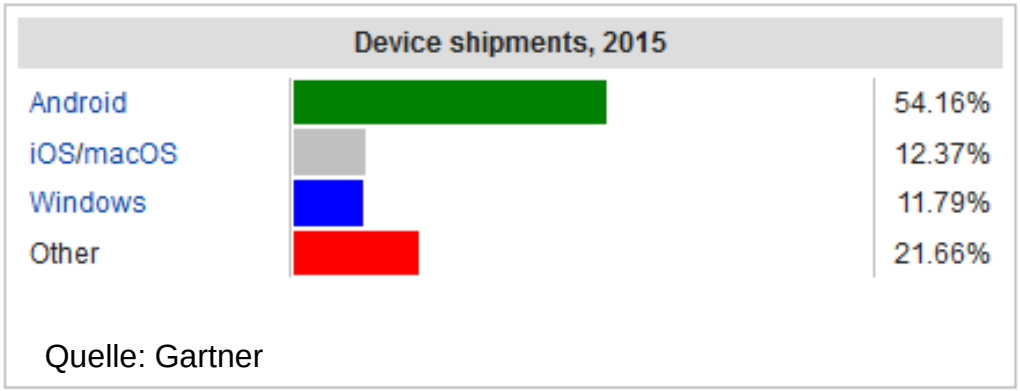
IT-Security ist wichtig

Worldwide Devices Shipments by Device Type, 2016-2019 (Millions of Units)

Device Type	2016	2017	2018	2019
Traditional PCs (Desk-Based and Notebook)	220	204	193	187
Ultramobiles (Premium)	50	59	70	80
Total PC Market	270	262	264	267
Ultramobiles (Basic and Utility)	169	160	159	156
Computing Device Market	439	423	423	423
Mobile Phones	1,893	1,855	1,903	1,924
Total Device Market	2,332	2,278	2,326	2,347

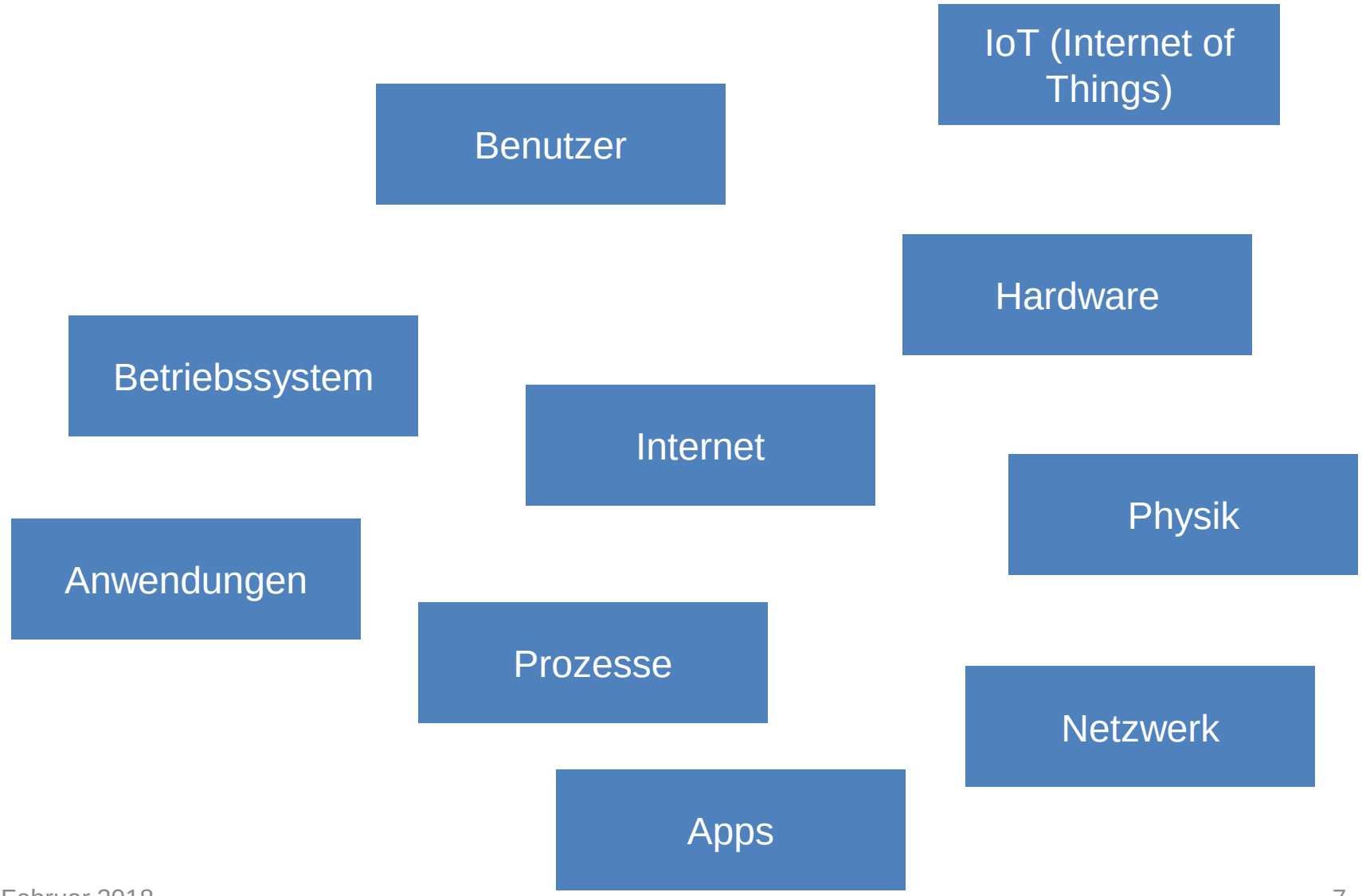
Source: Gartner (January 2018)

Weltbevölkerung 2017:
7.6 Milliarden



Quelle: Gartner

IT-Security ist relevant

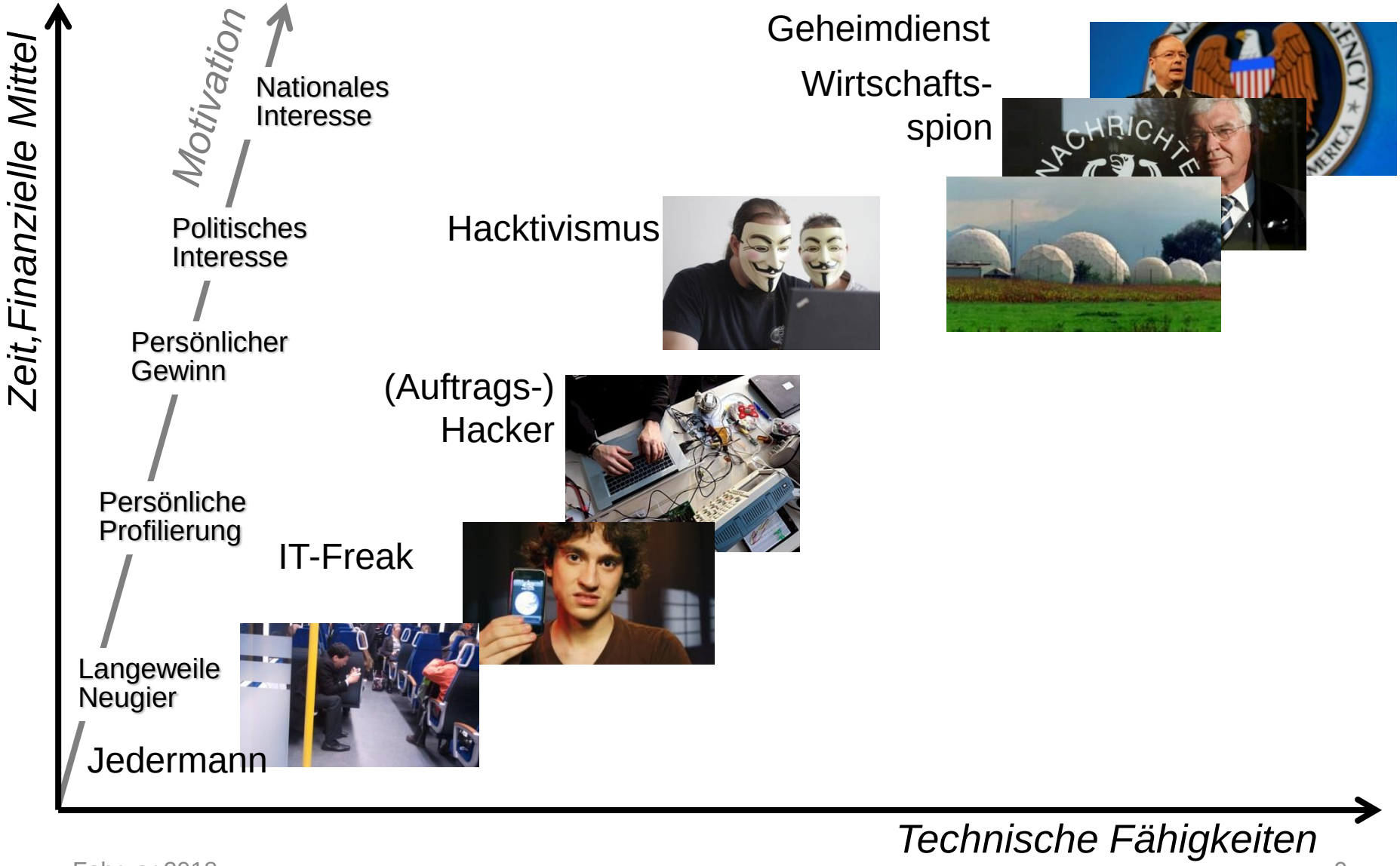


Sichere IT

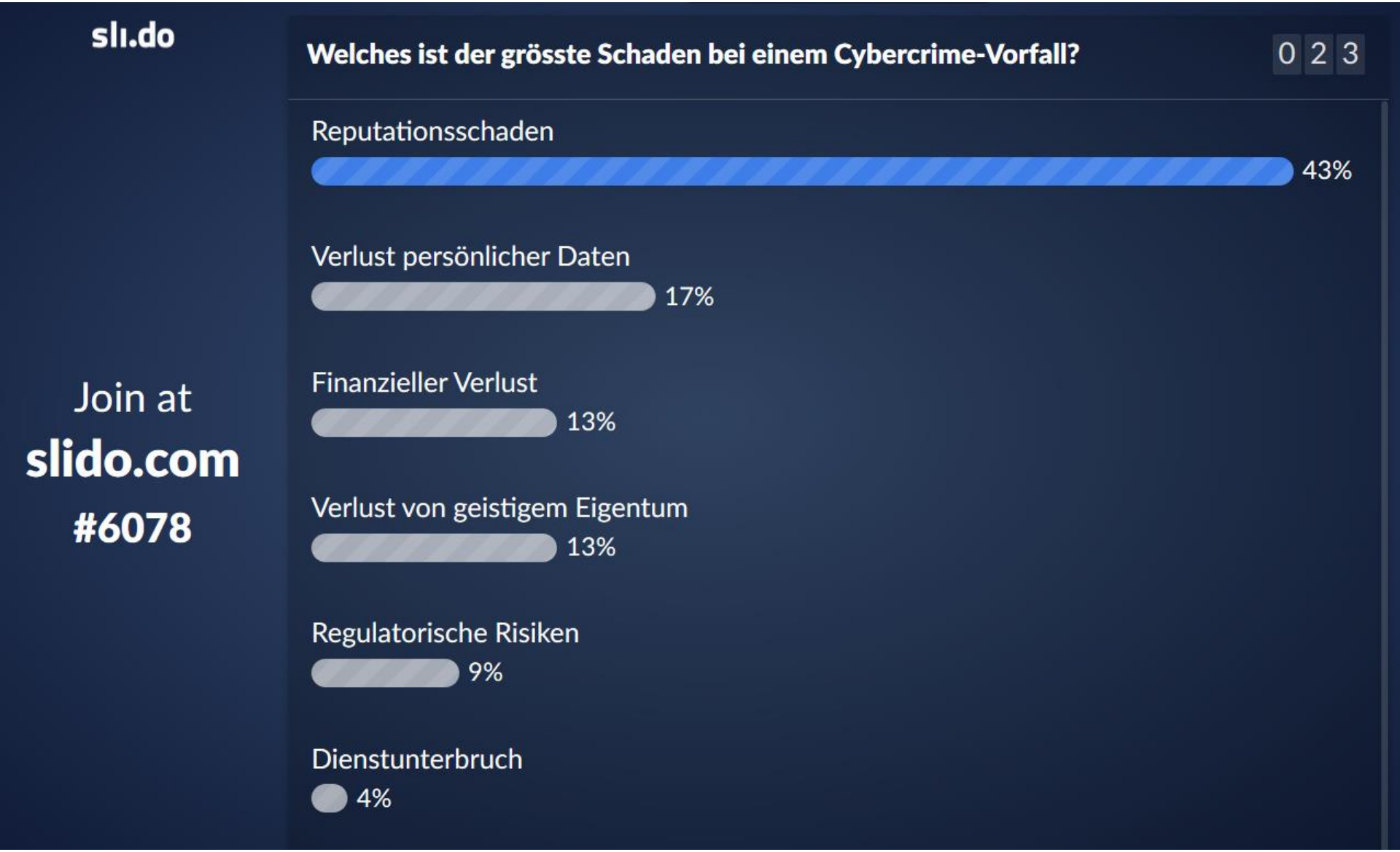
- Schutz vor unerlaubtem Zugang (Verarbeitung, Transport, Speicherung)
- Schutz vor Veränderbarkeit
- Verfügbarkeit der Systeme und Daten

Massnahmen:
- Aktuelle Software (Versionen/Patching)
- Kontrollen (Authentisierung/Autorisierung)
- Schadcode Schutz
- Datensicherung
- Angemessene, aktuelle und etablierte Prozesse
- Protokollierung
- Verschlüsselung
- Physische Sicherheit
- Kritische Benutzer

Bedrohung in Funktion von Motivation und Mitteln (Angreiferkategorien)



Poll



Quelle: https://www.pwc.com (Cybercrime)

IT-Security Modell: CIA

- **C**onfidentiality (Vertraulichkeit)
  Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden.

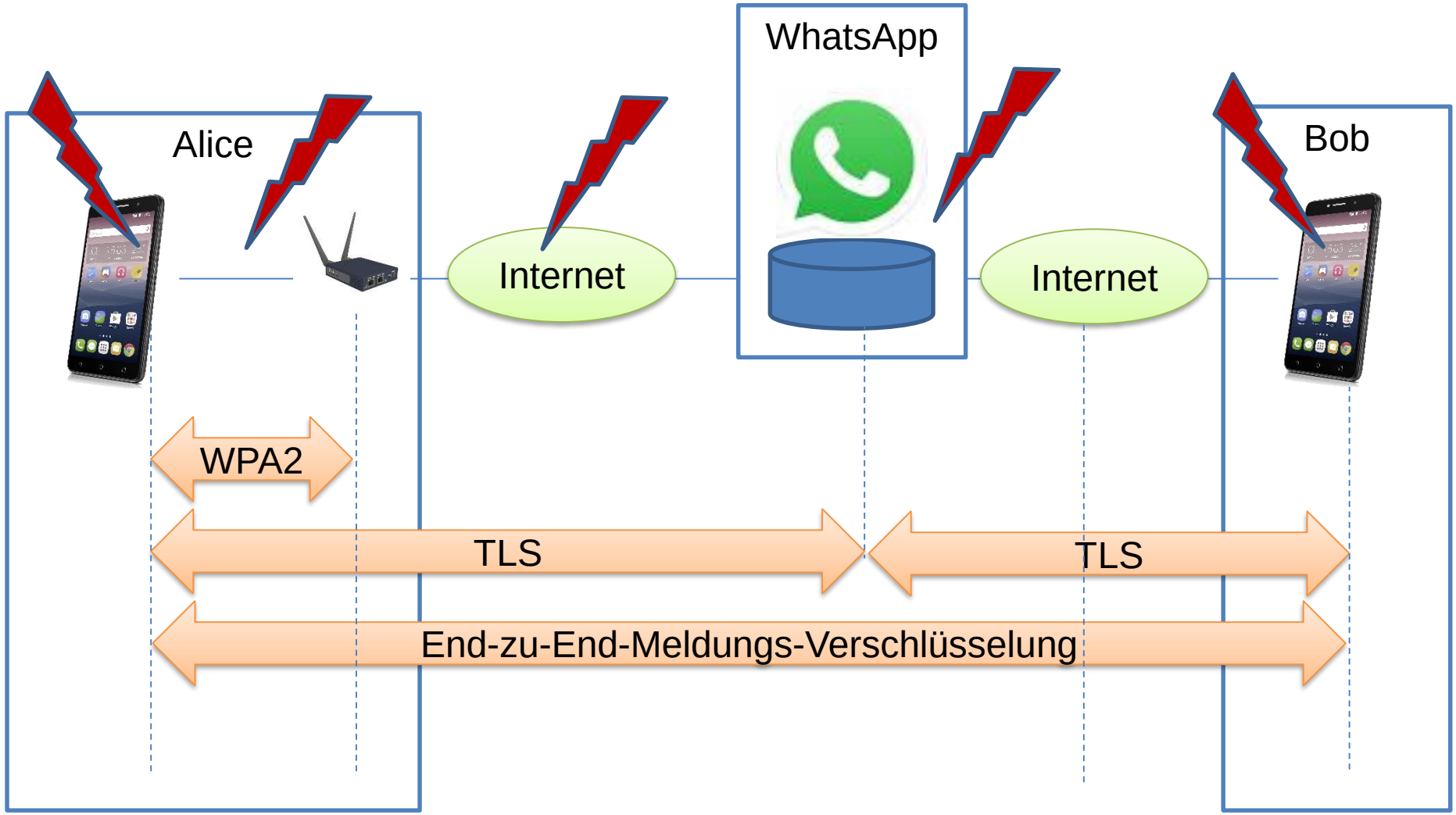
- **I**ntegrity (Integrität)
  Daten dürfen nicht unbemerkt verändert werden. Alle Änderungen müssen nachvollziehbar sein.

- **A**vailability (Verfügbarkeit)
  Verhinderung von Systemausfällen; der Zugriff auf Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet sein.

Quelle: https://de.wikipedia.org/wiki/Informationssicherheit

https://www.youtube.com/watch?v=QVXeewaisEI

Sichere Datenübertragung

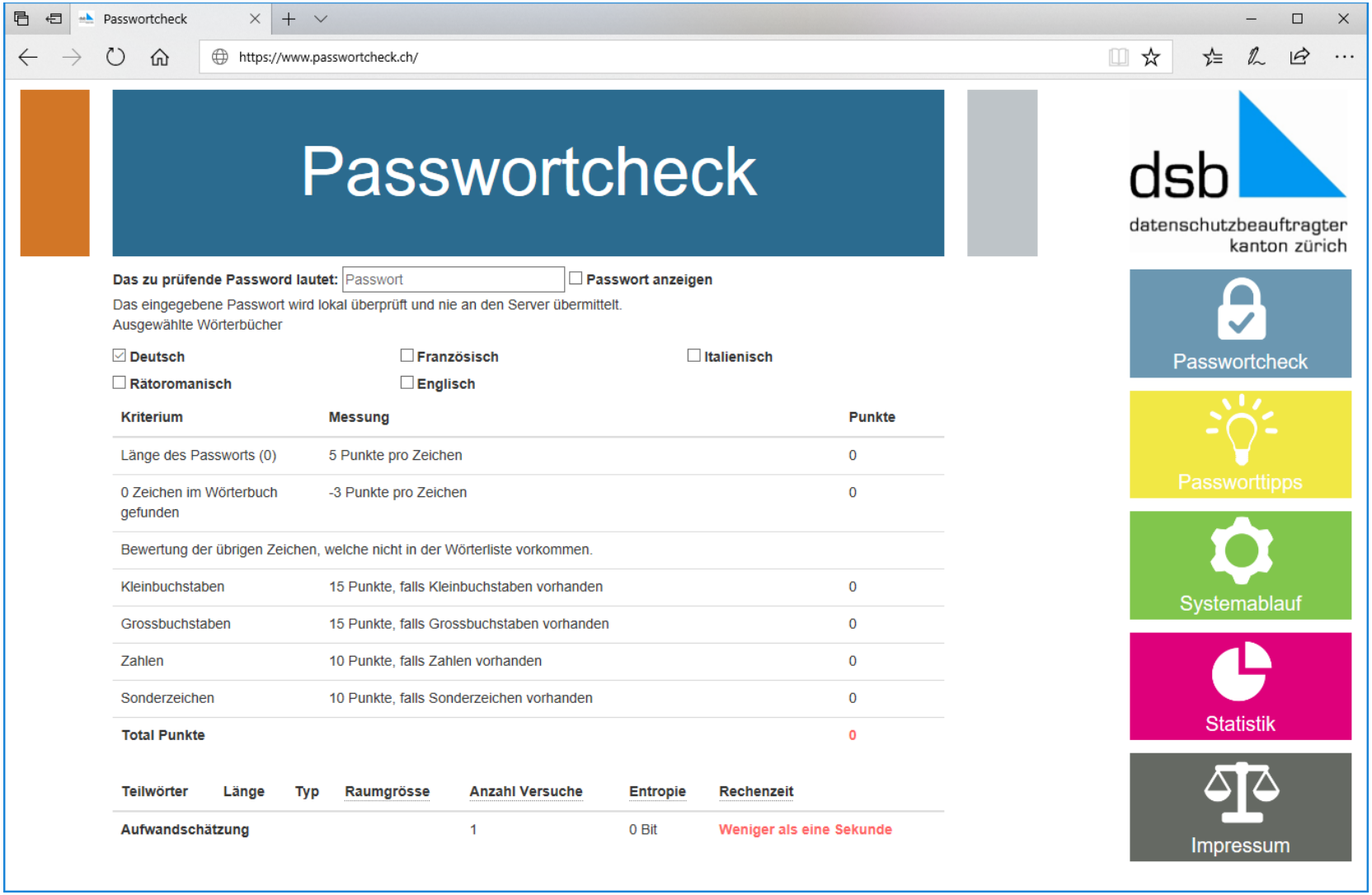


Kreditkarten Fraud
Episodenfilm: “Disconnect”

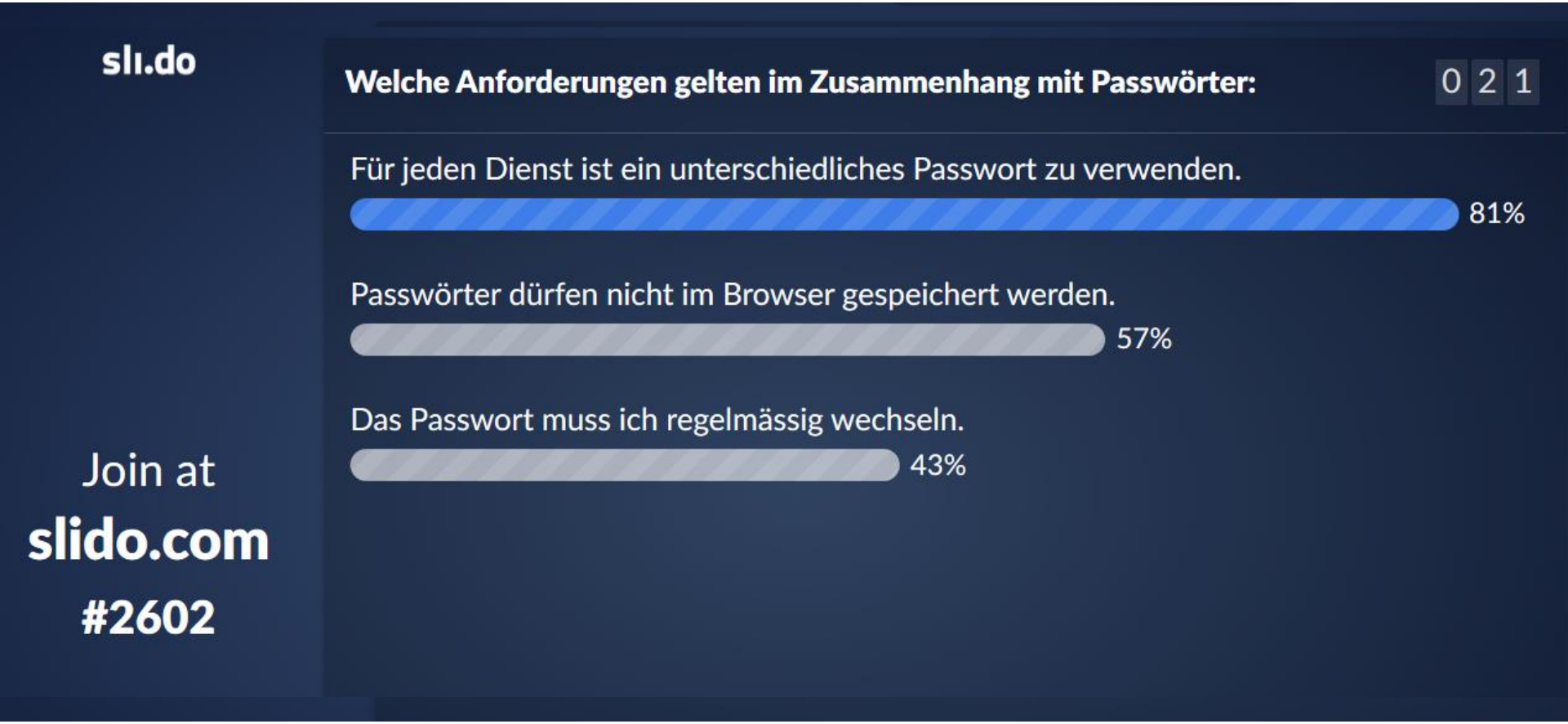
https://www.youtube.com/watch?v=diVZzQvk9e0
Sequenz: 26:05 – 27:40 https://youtu.be/diVZzQvk9e0?t=1555
32:30 – 35:10 https://youtu.be/diVZzQvk9e0?t=1947

https://www.passwortcheck.ch/

Passwortcheck

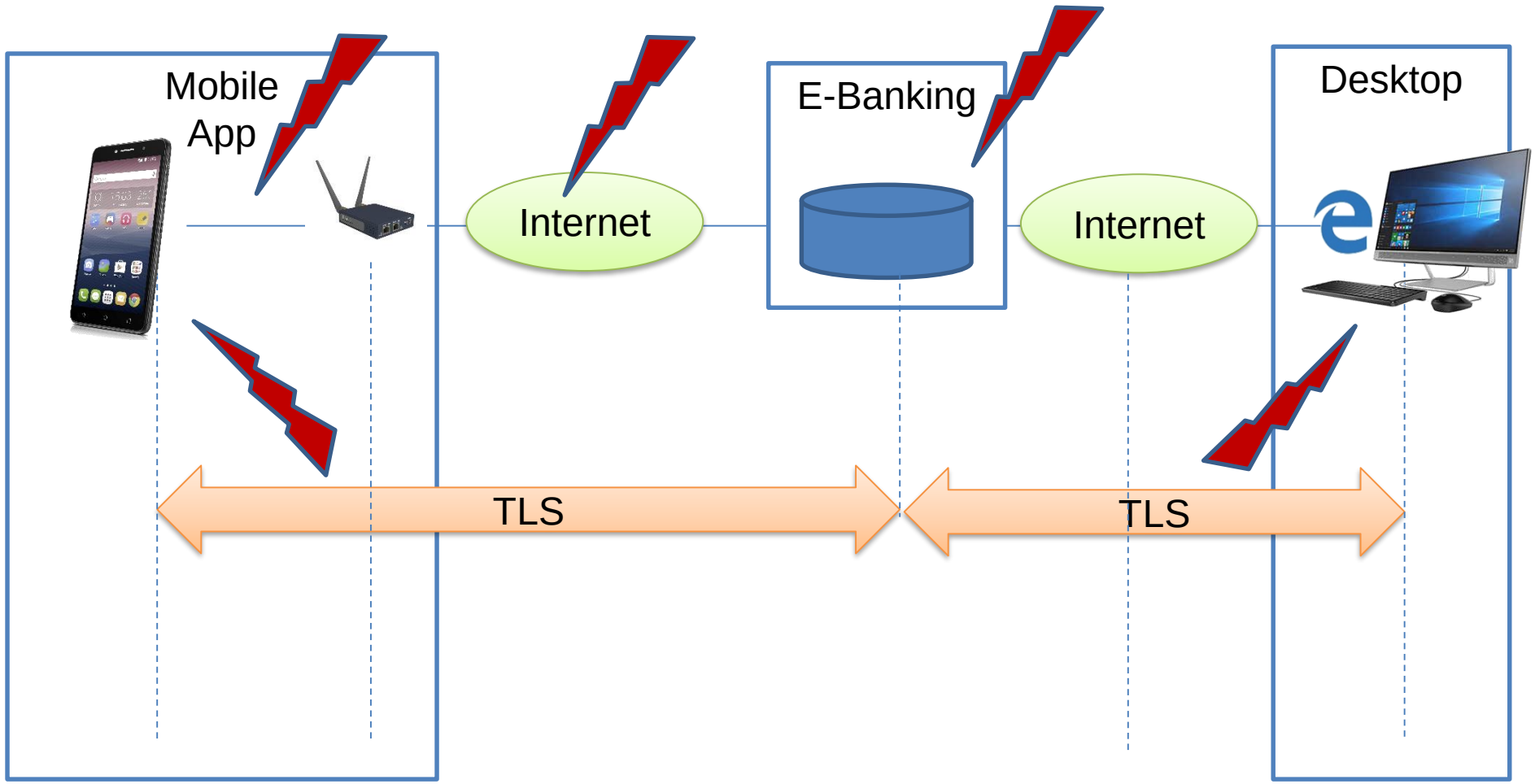


Poll



Quelle: https://www.pwc.com (Cybercrime)

Integrität



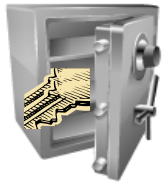
Eingebaute Sicherheitsmechanismen «Hardware»

Geräte-PIN

- Schutz gegen interaktive Verwendung des Gerätes
- Schutz gegen Zugriff über andere Schnittstellen (z.B. USB)

Schlüsselspeicher (Keychain)

- Sichere Ablage von «sensitiven» Informationen
- Schutz gegen unberechtigten Zugriff auf dem Gerät, im Backup, usw.



Speicherverschlüsselung

- Schutz gegen physischen Zugriff auf den Speicher
- Schutz gegen Zugriff mit modifiziertem Betriebssystem

Eingebaute Sicherheitsmechanismen «Betriebssystem»

Zugriffskontrolle auf OS-Stufe

- Optimale Trennung von Anwendungen auf Betriebssystem-Stufe
- Einsatz von Betriebssystem-Benutzern mit eingeschränkten Rechten

Update-Funktionalität

- Schnelle Aktualisierung von Betriebssystem und Apps

Integritätskontrolle auf OS-Stufe

- Schutz gegen «Rooting» / «Jailbreaking»
- Sicherstellen, dass alle Sicherheitsmechanismen intakt sind

Eingebaute Sicherheitsmechanismen «Apps»

Sandbox

- Logische Trennung (Separierung) von Apps
- Zugriffe auf Betriebssystem-Funktionen und Hardware einschränken

Integritätskontrolle Apps

- Inhaltliche und technische Kontrolle der Apps im Store
- Verwendung von digitalen Signaturen

Rechtesteuerung

- Vergabe von Zusatzrechten durch Benutzer (z.B. Zugriff auf GPS, Internet)

Backup

- Regelmässige Erstellung von Backups mit einfacher Restore-Möglichkeit
- Sichere Ablage der Backup-Daten

App Store - Integritätskontrolle Apps

Apple

- Prüfung:
  - Verwendete API, Methoden, Funktionen
  - Angeforderte Berechtigungen (Sensoren und Daten)
  - Inhalte
- Genaue Prüftätigkeit nicht bekannt
- Prüfung dauert typischerweise 10 Tage (bevor App im Store verfügbar ist)

Google (Play-Store)

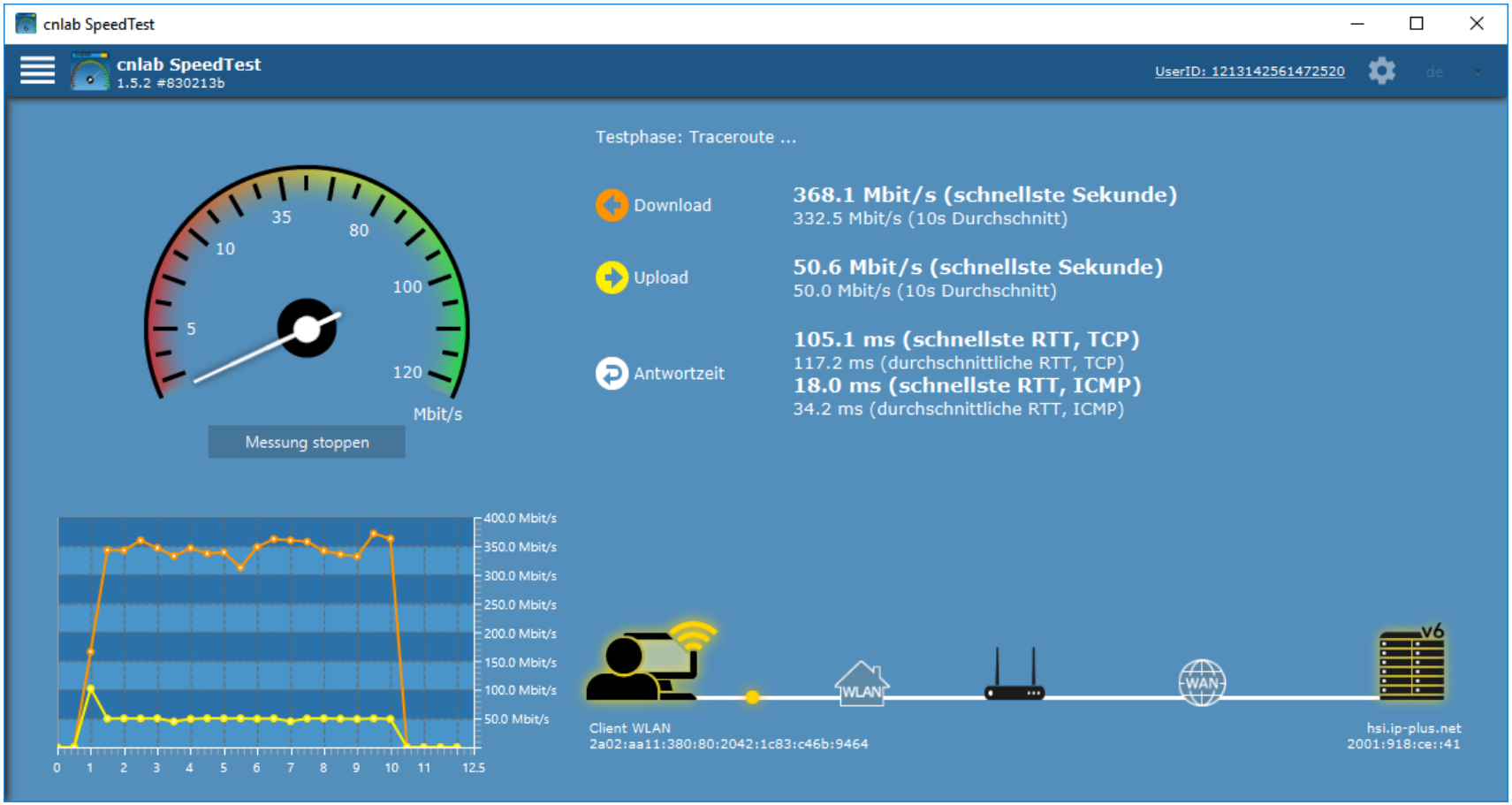
- Automatisierte Prüfung
- Genaue Prüftätigkeit nicht bekannt
- Prüfung dauert typischerweise wenige Stunden (nachdem App im Store verfügbar ist)

Jailbreak/Rooting

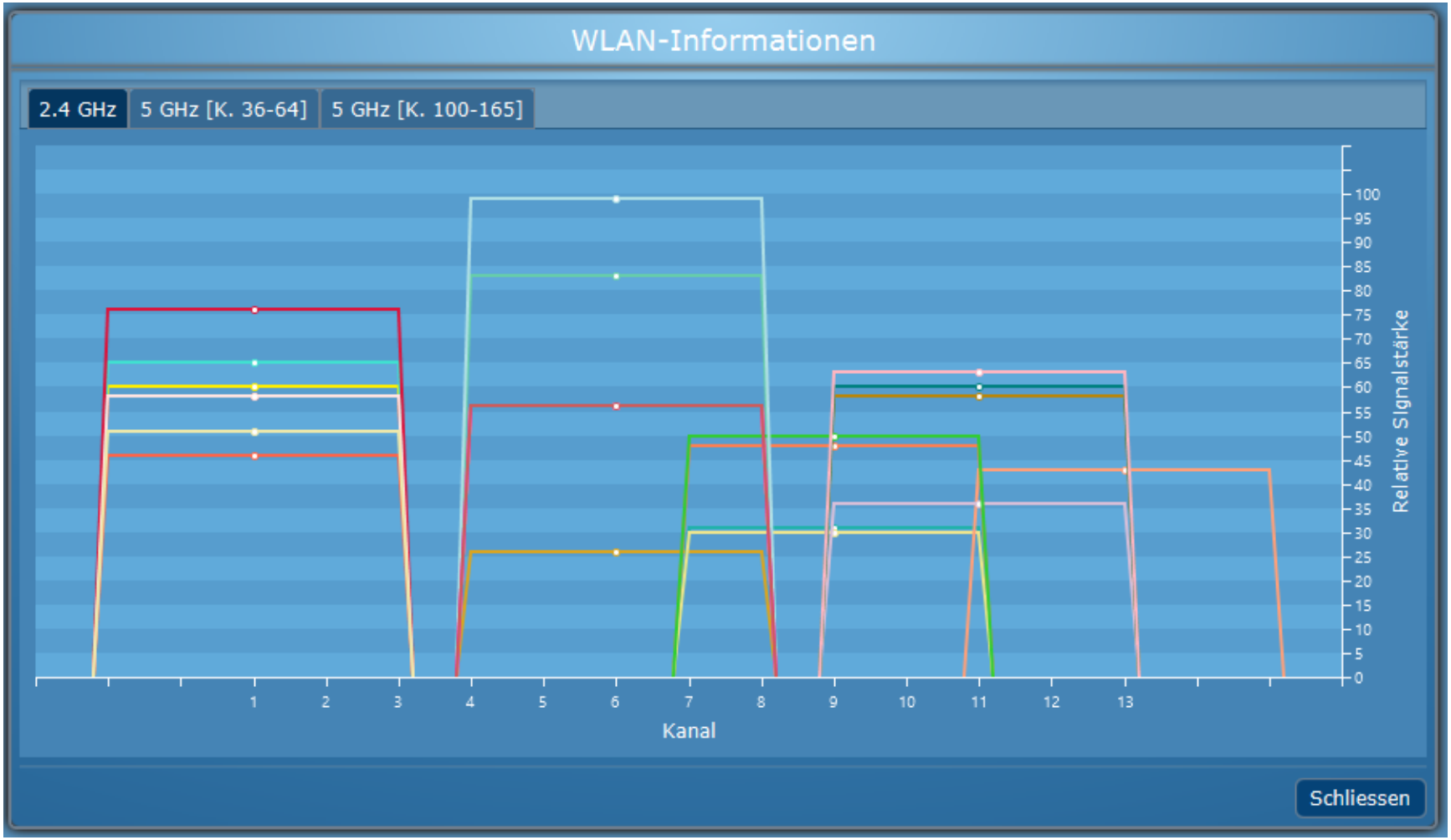
- iOS → Jailbreak, Android → Rooting
- Installation erfolgt meist durch Ausnutzung einer Schwachstelle
- Für aktuelle Geräte verfügbar
- Gespeicherte Daten gehen im Normalfall nicht verloren
- Deaktiviert Sicherheitsmechanismen

CIA
Availability

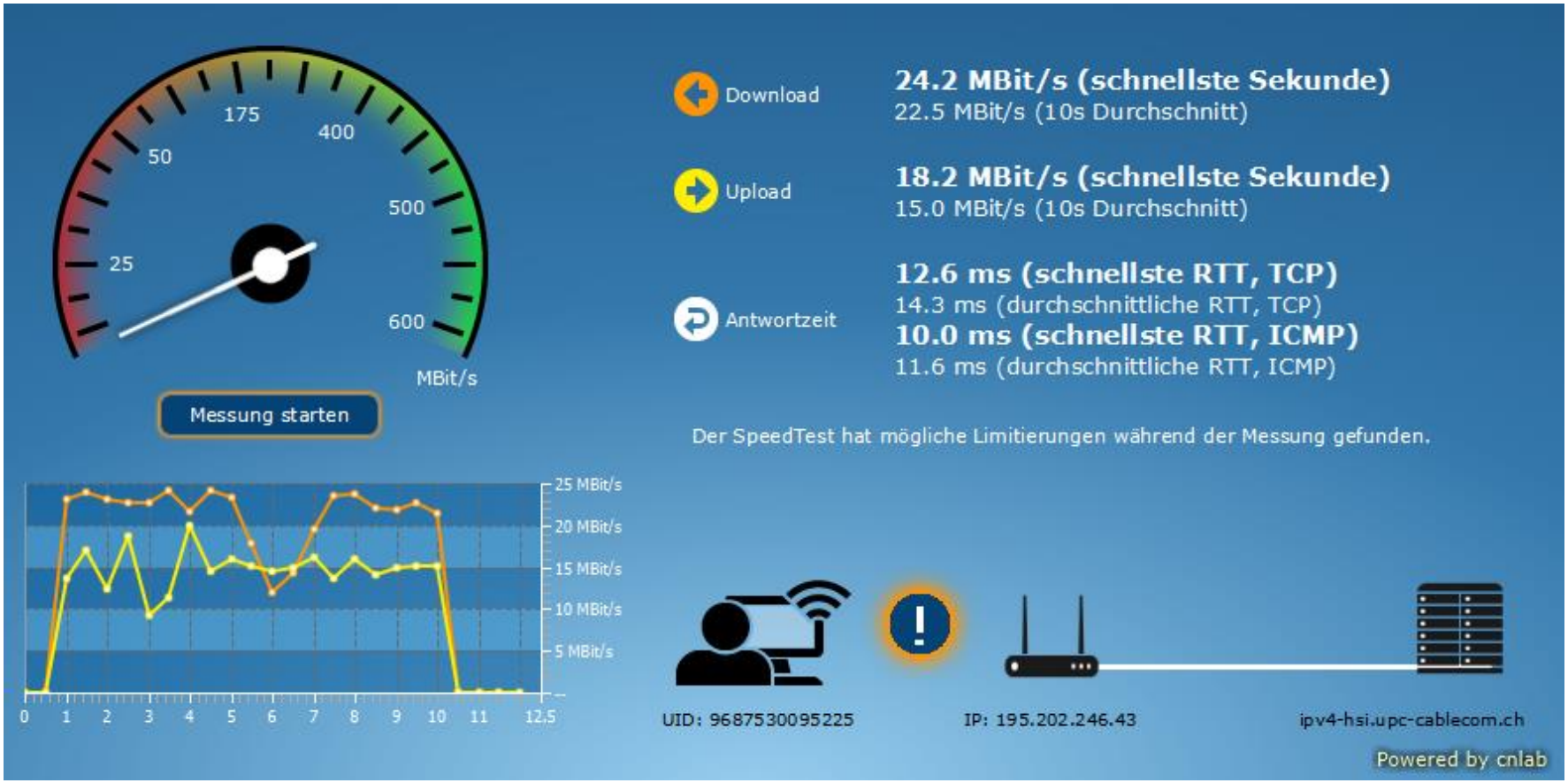
Verfügbarkeit (Availability)



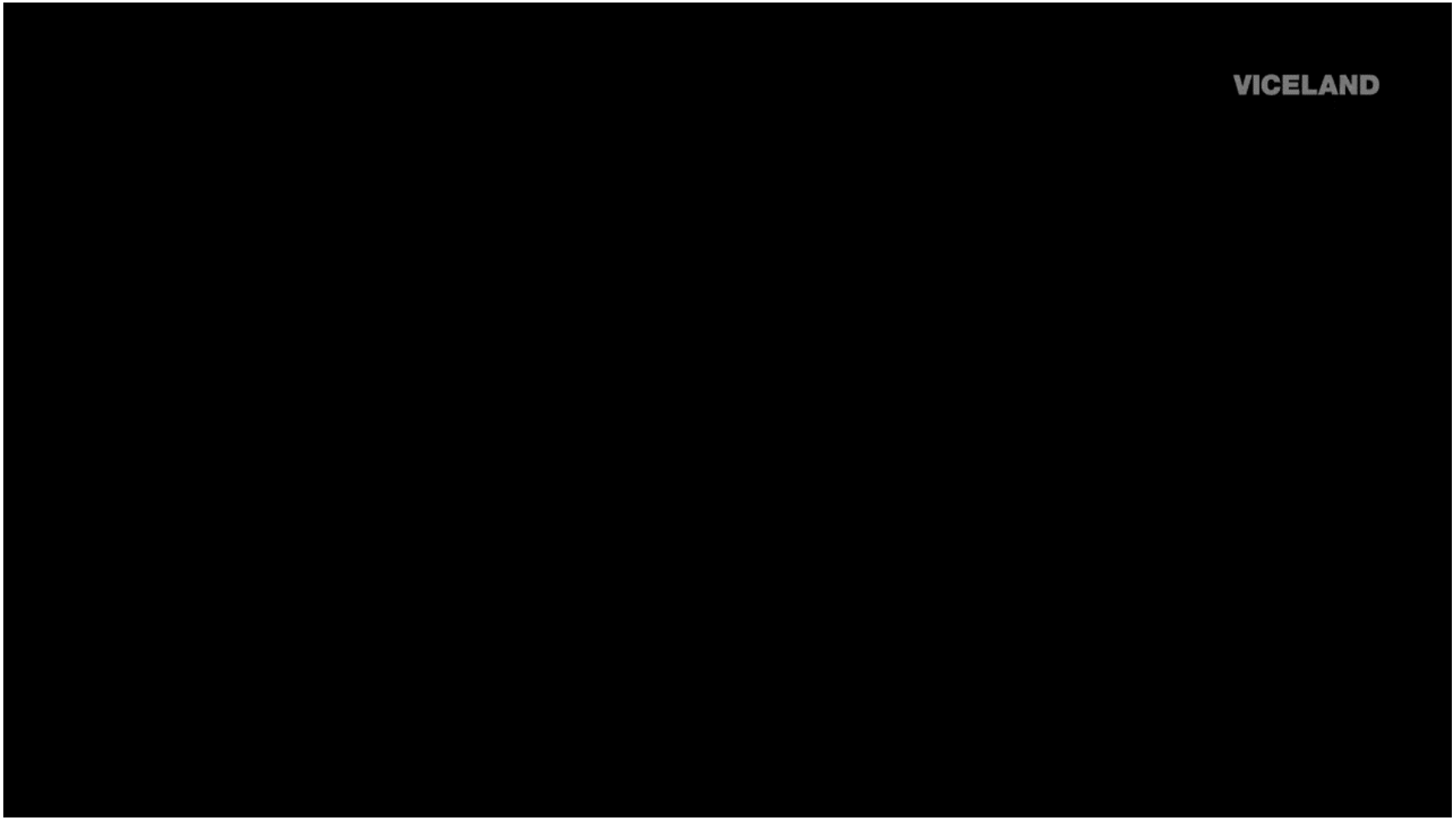
Lokale Netzwerkverbindungen: Ethernet - WLAN



Erkennung von Engpässen



8.7.2016, Hacking a Car with an Ex-NSA Hacker



www.youtube.com/watch?v=MeXfCNwMG64 5m24s

Crowd Sourced Vulnerability Detection (Bug Bounty Programs)

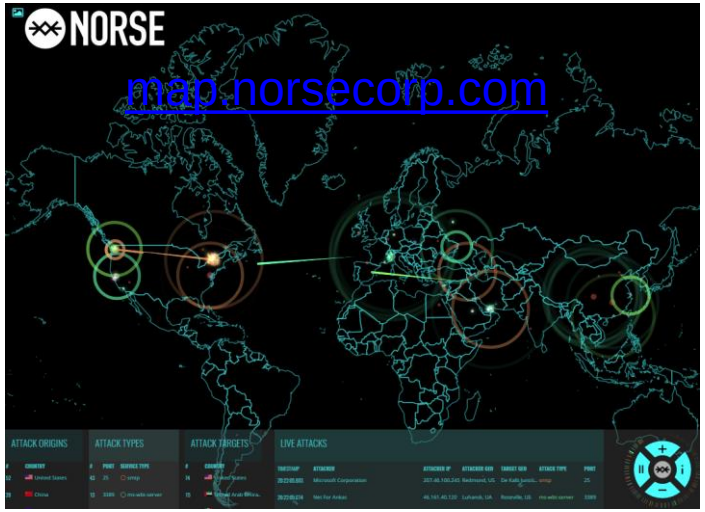
bugcrowd.com

- Private and Public Programs bugcrowd.com/programs
- 7 Myths of Bug Bounty Programs, 7.12.2016 54min

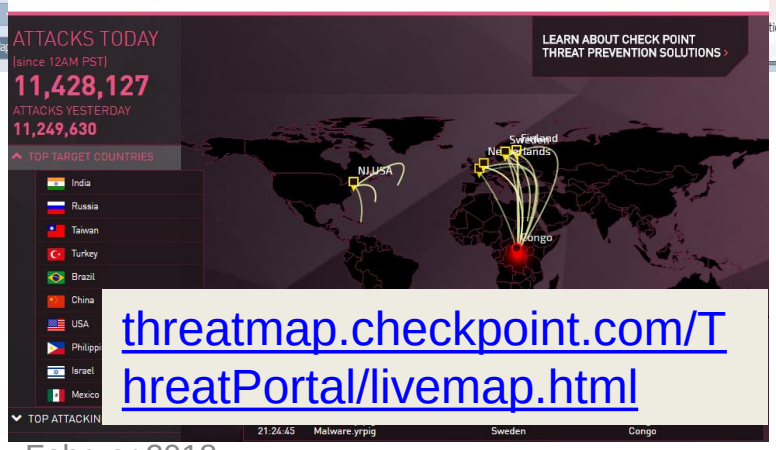
- Crowd Sourcers
  - Okta Bugcrowd bugcrowd.com
  - Vulnerability Lab vulnerability-lab.com
  - Fire Bounty firebounty.com
  - HackerOne www.hackerone.com
- Firmen
  - United Airlines www.united.com/web/en-US/content/Contact/bugbounty.aspx
  - Bitcoin www.bitcoin.de/de/bug-bounty
  - Facebook www.facebook.com/whitehat
  - Microsoft technet.microsoft.com/en-us/security/dn425055.aspx
  - Apple
  - Google Vulnerability Reward Program bughunter.withgoogle.com/

Botnet Übersichtskarten (Command and Control Servers und attackierte Computer)

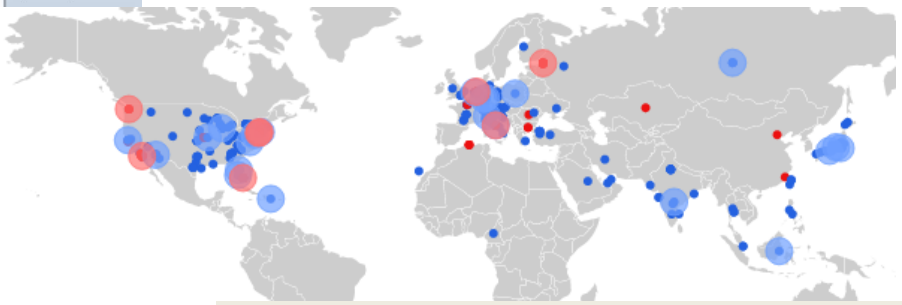
www.digitalattackmap.com



map.norsecorp.com



threatmap.checkpoint.com/ThreatPortal/livemap.html



- C&C-Server
- Gekaperte Computer

www.trendmicro.de/sicherheitsinformationen/aktuelle-bedrohungsaktivitaeten/globale-botnetz-uebersichtskarte

Danke

Christian Birchler
christian.birchler@cnlab.ch
+41 55 214 33 40