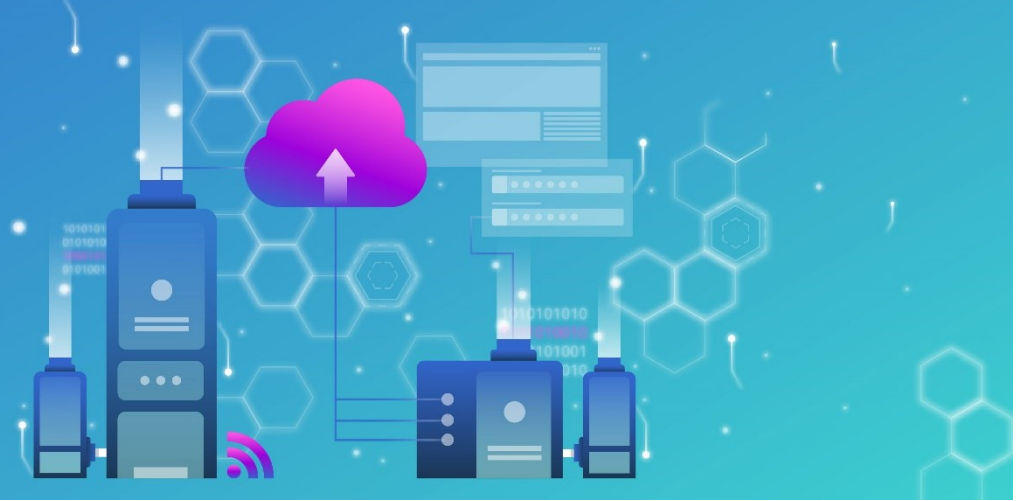




Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS

Herzlich willkommen
beim Bundesamt für Cybersicherheit



Cybersicherheit und das «Situation Picture»

Marc Henauer, BACS

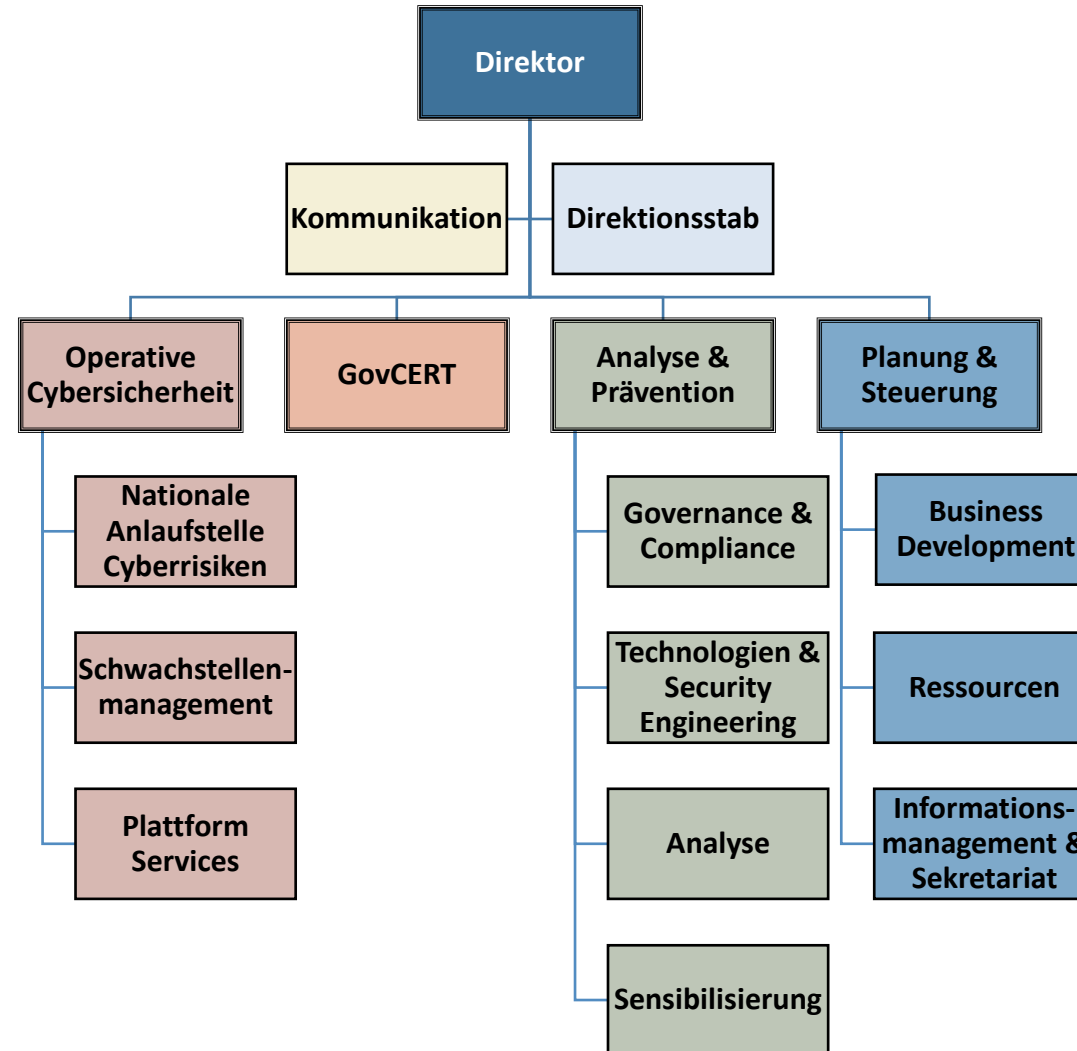
ICT Warrior Academy, 2. September 2024



Das Bundesamt für Cybersicherheit (BACS)



Das BACS - Organigramm





Das BACS – Aufgaben und Grundlagen

- Kompetenzzentrum des Bundes für Cybersicherheit. Erste Anlaufstelle für Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen.
- Verantwortung Umsetzung der Nationalen Cyberstrategie (NCS) [Nationale Cyberstrategie NCS \(admin.ch\)](#)
- Grundlage bildet das Informationssicherheitsgesetz (ISG) und die Informationssicherheitsverordnung (ISV)
- Meldeformular für Cybervorfälle: www.bacs.admin.ch



Cybersicherheit und Risikomanagement



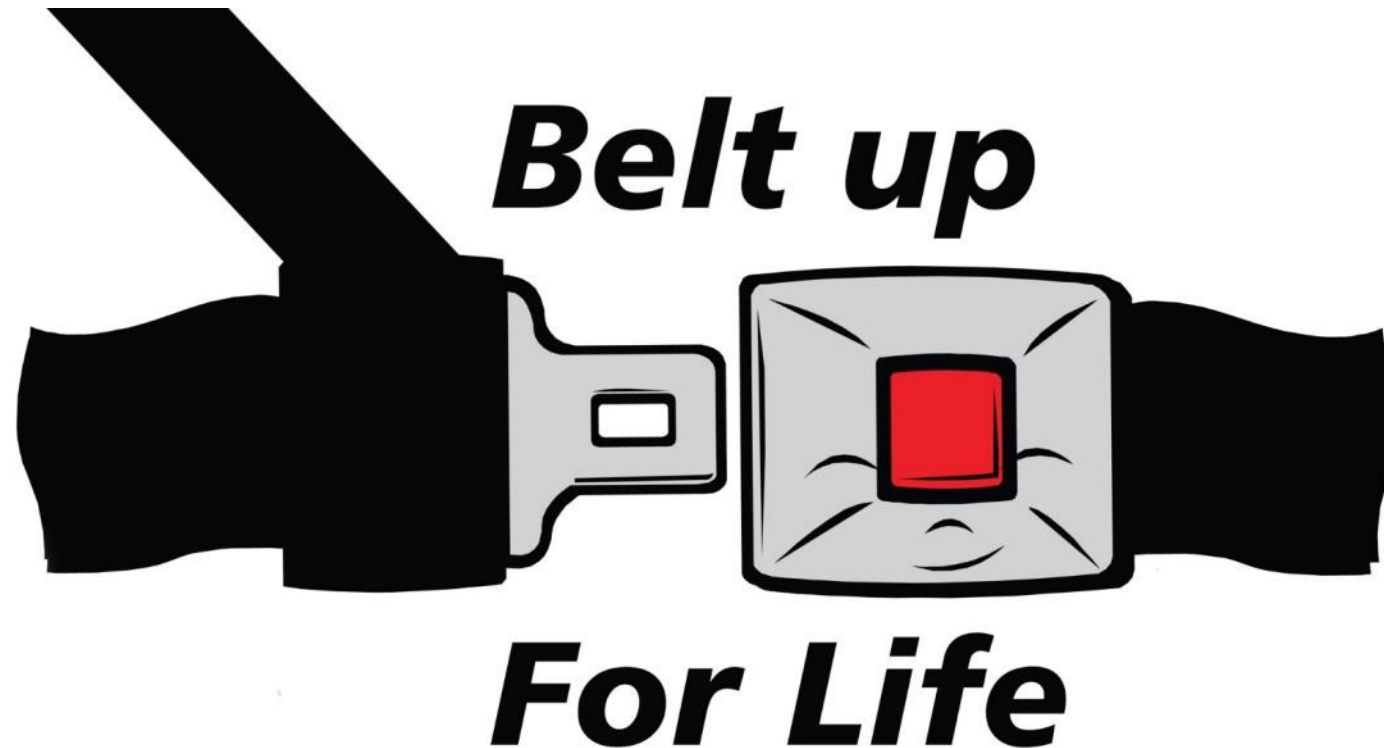
Das Spannungsfeld

- Zunahme der Bedeutung der Informationstechnologie für Geschäftsprozesse und Finanztransaktionen
- Zunahme der Teilnehmer an diesen Prozessen, zunehmende Vernetzung
- Zugang zu immer mehr wertvoller Information wird möglich
- Zunahme der Möglichkeiten für Betrug, Spionage, Erpressung, Sabotage
- Auftreten neuer Akteure (z.B. Organisierte Kriminalität, Staaten)
- Anpassung der Motive und Methoden bestehender Akteure: kommerzieller Gewinn, Know-how Transfer, politische Motive



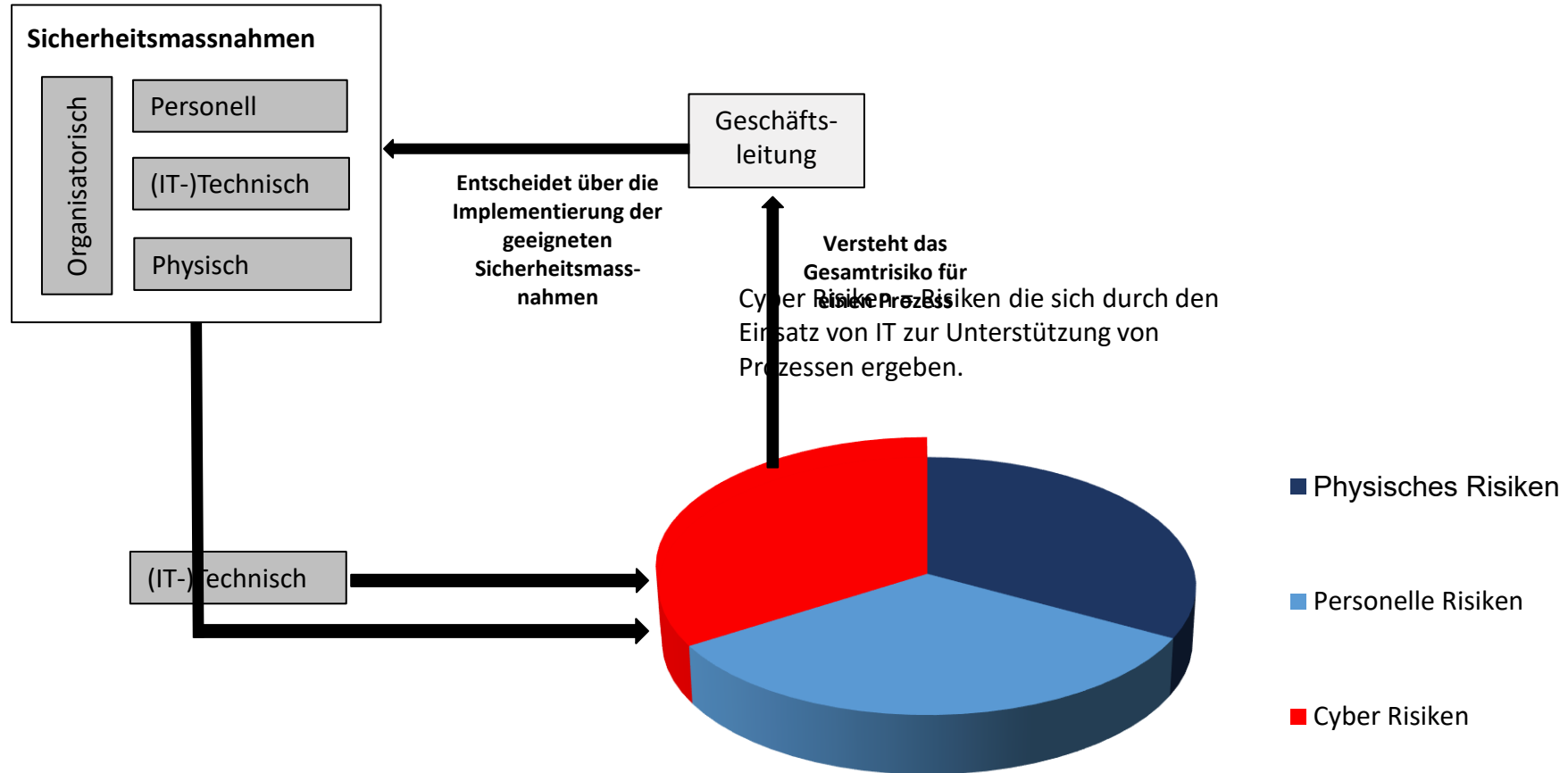
Sicherheit vs. Risiko

“Seat belts reduce serious crash-related injuries and deaths by about half.” *(National Highway Traffic Safety Administration)*





Cyberisiken als Geschäftsrisiko





Das «Situation Picture»



Bedrohungslandschaft – Bad Stuff aber relevant?

Täter

Script-Kiddies



Hacktivisten



Cyberkriminelle



Staaten
*Advanced
Persistent
Threat*



Typen



Menschlicher "Fehler" /
technisches Versagen



Betrug



Phishing



Malware



DDoS



Ransomware



Beeinflussung



Sabotage



Spionage

Ziele





Von Risiko und Bedrohung

$$V \times B \times S = R$$



$$1 \times 0.1 \times 1 = 1$$



$$1 \times 0.9 \times 1 = 1$$



«Reduktion der real existierenden Komplexität»



Militärische Lage

Willkommen zu MELANI-Net

Bitte geben Sie unten Ihren Benutzernamen und Ihr Passwort ein. Die Daten werden verschlüsselt übermittelt.

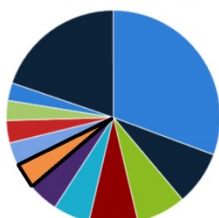
Benutzername

Passwort



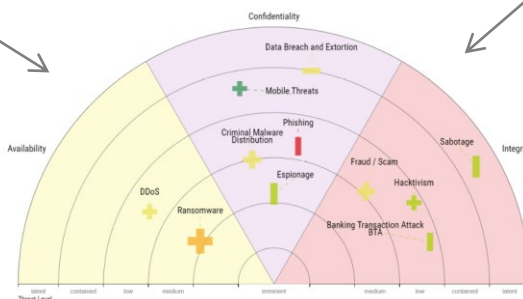
Internationale Partner

Infections per Malware Family



Technische Lage in den Netzen

PPP mit kritischen
Infrastrukturen



Polizei-Lage

Melden Sie uns



einen
Cybervorfall



eine
Schwachstelle

Sicherheitspolitische Lage



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Federal Department of Foreign Affairs FDFA

New banking malware 'Dyre' targets Bank of America, CitiGroup accounts

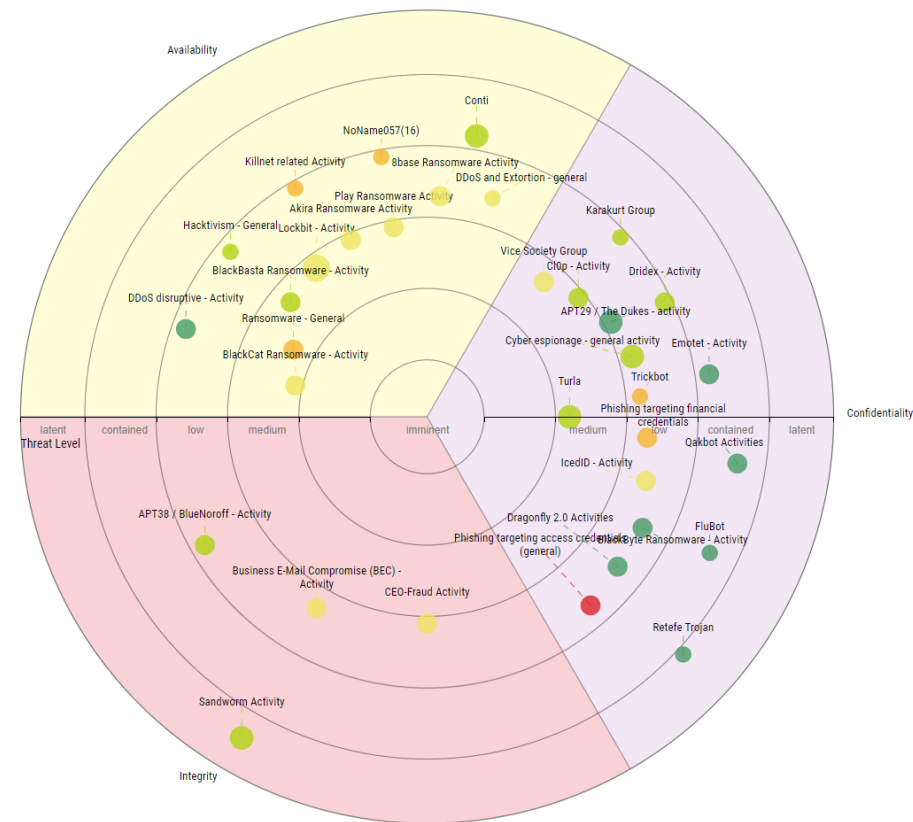
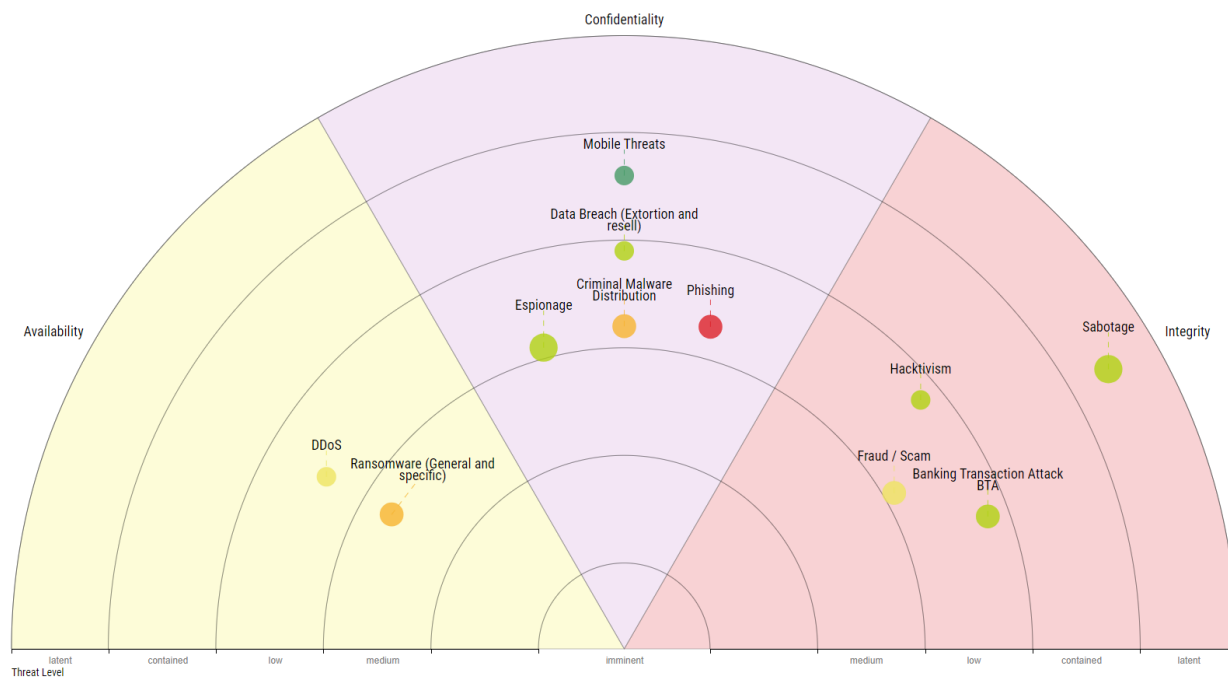
BY ALAN MARTIN POSTED 18 JUN 2014 - 10:12AM

BANKING 0

Open Source



Aktuelle Bedrohungslage





Und Jetzt?





Threat Level

W | CIIP-Threat Landscape > P | CIIP-Threatradar > M | Threat Assessment

ALPHV, NODERUS

General Modus Operandi

Besides the common double-extortion tactic in which sensitive data is stolen prior to encryption and the victim threatened with its public release, BlackCat affiliates were also observed applying triple-extortion tactics, menacing victims in chats with the threat of a distributed denial-of-service (DDoS) attack if the ransomware group's demands aren't met.

Technical capabilities

According to its developers' claims, it can infect various Windows and Linux operating system versions. This ransomware is highly customizable and heavily human-operated, which is especially important as it is primarily used to target large entities (e.g., companies, corporations, organizations, etc.). ALPHV (BlackCat) malware can employ different encryption routines, use several cryptographic algorithms, proliferate via local networks (i.e., spread between computers), terminate virtual machines, and so on. It can also end running processes and close files that are open during encryption.

related capabilities

-

Target profile

Based on the leaksite, BlackCat activities seem strongly focussed on the US and Europe (each about 40% of its entire activities), Asian organizations seem targeted to a lesser degree. Victims include organizations in the following sectors: construction and engineering, retail, transportation, commercial services, insurance, machinery, professional services, telecommunication, auto components and pharmaceuticals. However, the so-far sporadic spread of the attacks may indicate a somewhat opportunistic approach, as with most contemporary ransomware families.

Attack frequency

Trend

Created

Created

Modified

Modified

Comm

Write

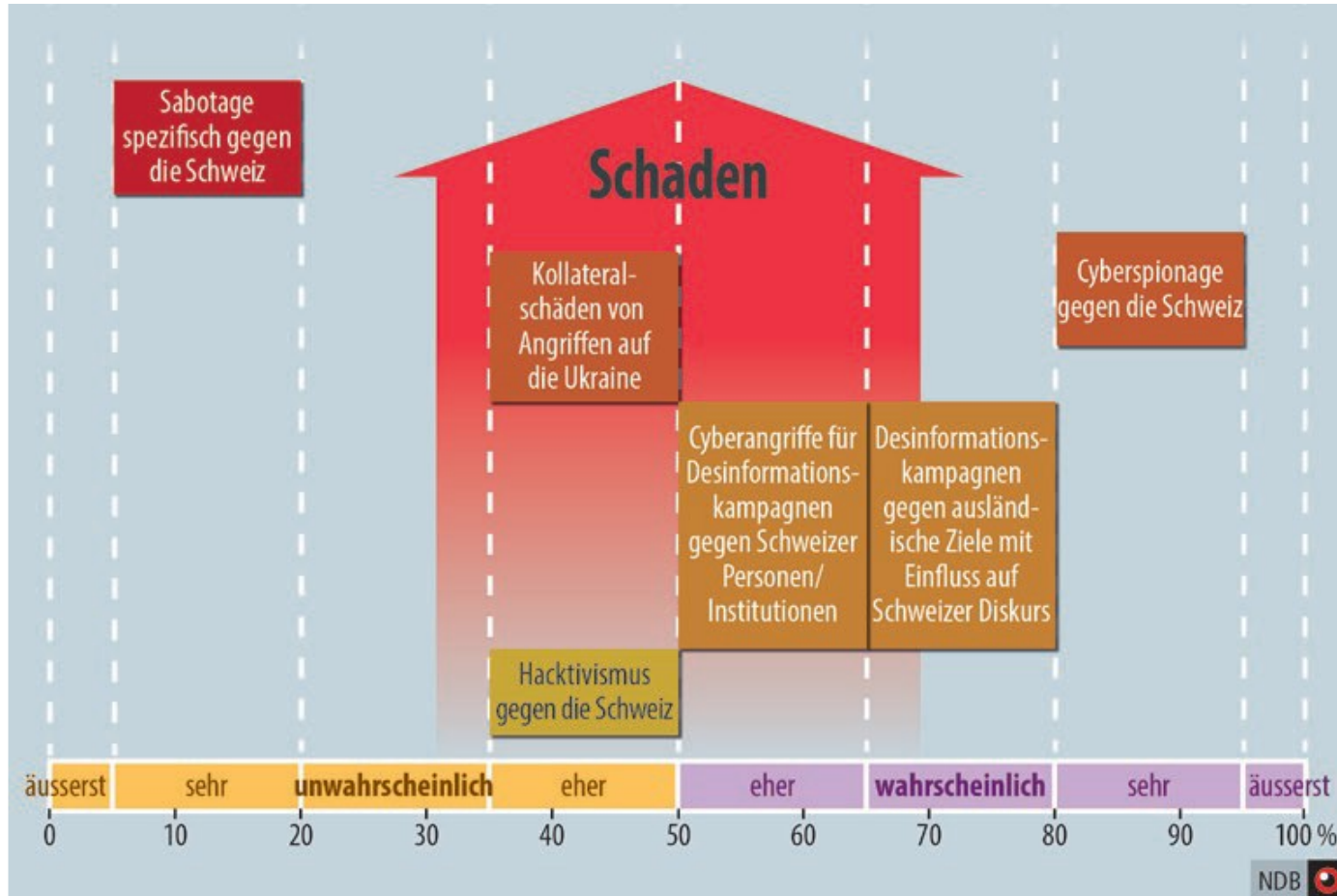
Confidentiality

0 / 2000

Sandworm Activity



Speziallagen – Krieg in der Ukraine



WIRED

BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

MATT BURGESS SECURITY MAR 23, 2022 7:00 AM

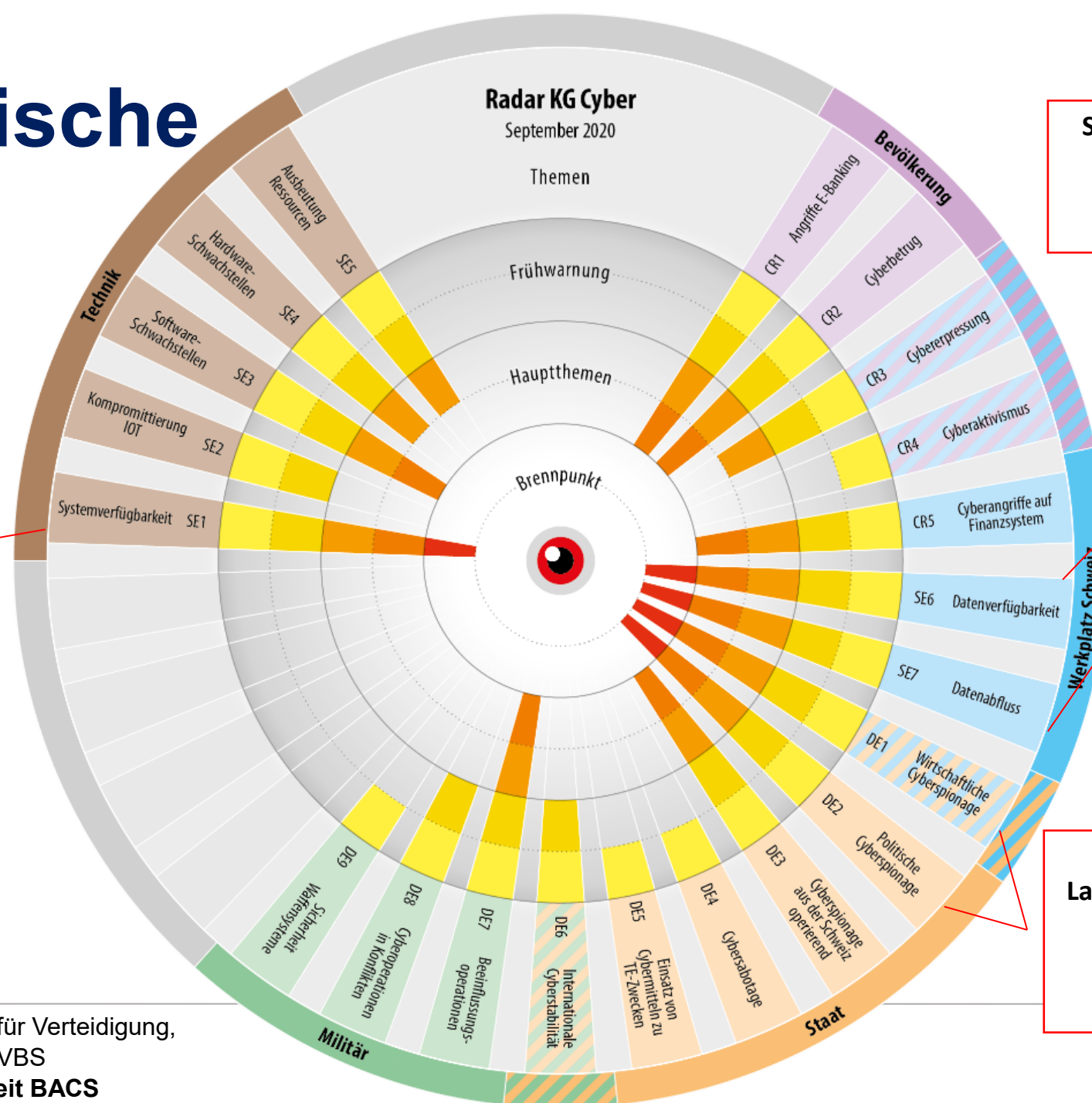
A Mysterious Satellite Hack Has Victims Far Beyond Ukraine

The biggest hack since Russia's war began knocked thousands of people offline. The spillover extends deep into Europe.





Die Politische Lage



**SE 1: DDoS
Blackmailcampaigns**

**SE6/7: Lasting Ransomware
Threat, new waves from
different groups**

**DE1/2:
Lasting Cyberspionage Threat
für CHE Enterprises and
Administration**



Und so weiter...

MELANI_Finance_Threat_Assessment_2020-1.pdf - Adobe Acrobat Reader 2017

Datei Bearbeiten Anzeige Fenster Hilfe

Start Werkzeuge DRUCK_Konferenzb... MELANI_Finance_T... x

Contederaziun svizra

www.melani.admin.ch contact: melani-incidents@ndb.admin.ch

INTERNAL – TLP:AMBER*

01.07.2020

CyberCoronaSituation: **released every Wednesday**

Corona/COVID-19 related and themed Cyberthreats

Overview Situation / Incidents (**new additions in red**):

TLP: AMBER – restricted to your organisation

Important current and ongoing phen	
Malware- & Phishing- E-Mails	Social Engineerir passwords or cre various national l Rarely targeted a
Suspicious online-offers (see also Fraud)	Offers of (mostly Suspected Fraud - (new) web sh

targeted attacks that target financial institutions' networks.

Ransomware

Threat Level: Medium

Suchbegriff hier eingeben

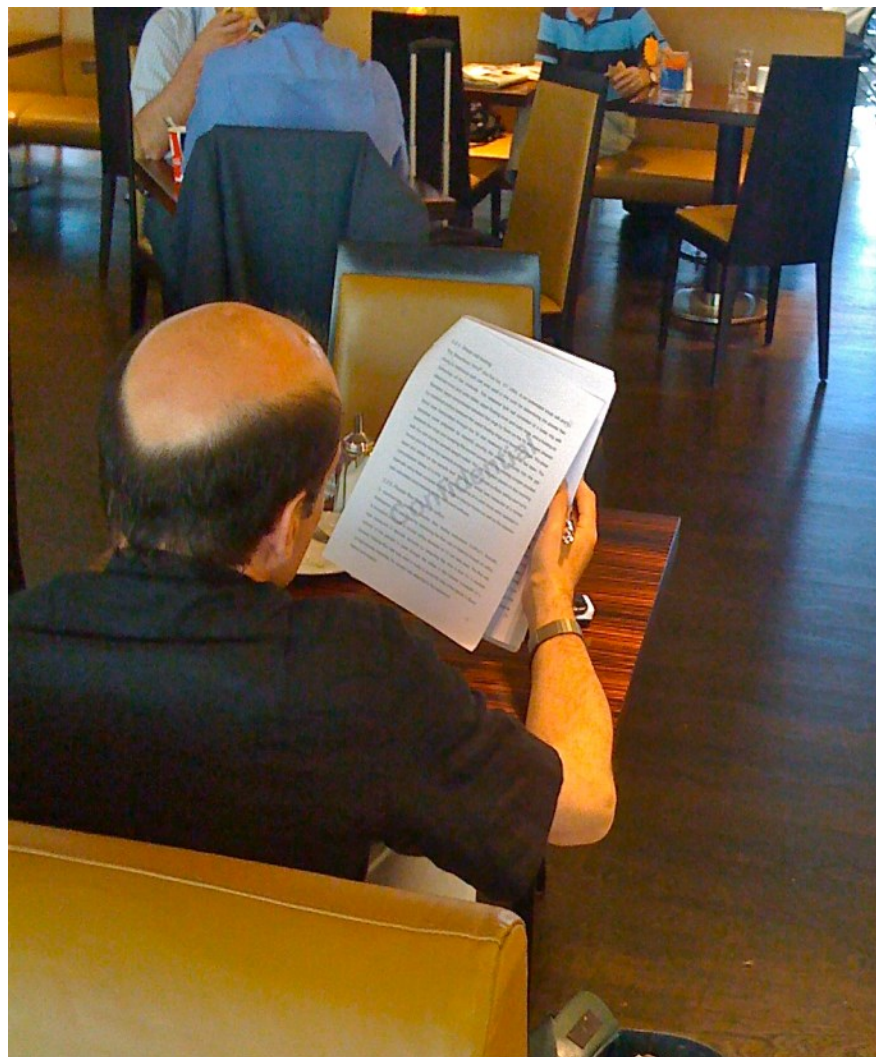
2.1 COVID-19 impact on the health sector's risk profile

The COVID-19 pandemic and the extraordinary situation that started in spring 2020 has had observable effects in cyber space. The uncertainty and insecurity that the new processes produced/created is a window of opportunity in social engineering. While health institutions have been in the focus of cybercrime before³, the pressure on staff and IT-infrastructure have significantly risen during the pandemic.

As outlined in the "CyberCorona Interim Report" published by MELANI⁴, while COVID-19 was



Fragen?





Vielen Dank für Ihre Aufmerksamkeit