Cyber Resilience

SSCC Online Workshop, June 11th, 2024

EPFL Center for Digital Trust

ETH zürich

ZISC Zurich Information Security & Privacy Center

zh aw

Announcement

General Public

Society, Swiss Population,…

NGOs

Humanitarian Aid,…

Industry

Associations, Companies,…

Governmental Bodies

Federal Council, Parliament, Federal/Cantonal Bodies such as NCSC, CYD, SVS,…

Ideas for Collaboration, Requests and Demand, Data and Information, Contacts

Knowledge Transfer, Education/Training Research Projects, Consulting, Expert Committees, Working Groups

= + +

Est. 2020

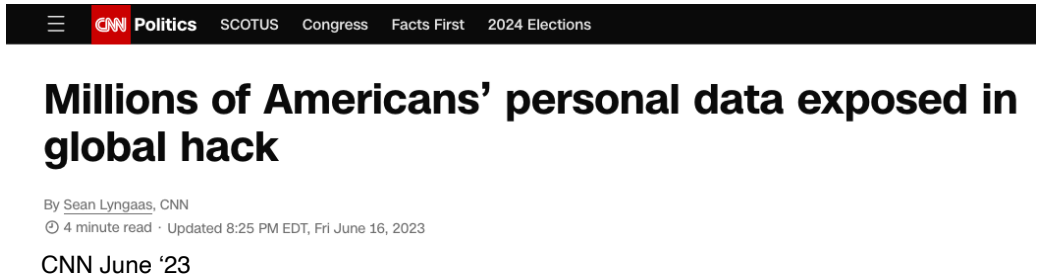
Motivation

- Even the most security sensitive organizations have suffered from cyber incidents.
- Sophisticated threat actors managed to compromise IT infrastructures in ways that allowed them to stay undetected over long periods of time (Advanced Persistent Threats APTs).
- Everyday numerous security vulnerabilities are being published.

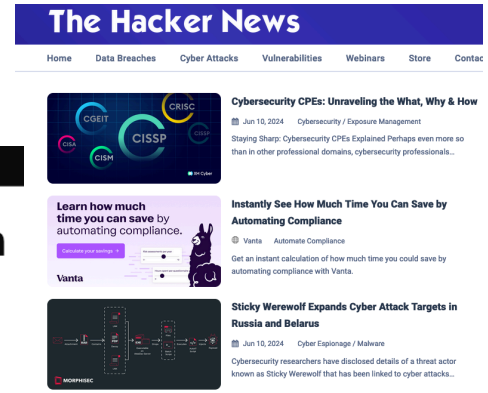
swissinfo June ‘23

The Verge Oct. ‘23

BBC June ‘24



CNN June ‘23



The Hacker News June ‘24

Motivation

- New attack vectors are discovered continuously.
- Our business models strongly depend on IT.
- By dependencies, any organizations depends on IT infrastructure today.

⇒

- It seems impossible to provide a *secure* IT infrastructure.
- Sooner or later any organization will be affected by a cyber incident.

The New York Times

Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack

In Sweden, a grocery chain temporarily closed its doors after the attack. Some companies have been asked for $5 million in ransom.

NYT, July ‘21

Konkurs Fensterhersteller

Offenbar zwang eine Cyberattacke Swisswindows in die Knie

In einem Schreiben an die Geschäftspartner begründet der Verwaltungsrat den Konkurs.

Donnerstag, 27.02.2020, 04:33 Uhr

SRF, Feb ‘20

BBC

Home News Sport Business Innovation Culture Travel Earth Video Live

Cyber-attacks

3 hrs ago

O-type blood donors needed after London cyber-attack

The NHS says last week's cyber-attack means blood cannot be sorted at the same frequency.

London

21 hrs ago

Trainees urged to help hospitals after cyber-attack

Students are asked to act as "floor-runners" to help London hospitals recover from a cyber-attack.

London

BBC, June ‘24

From Cyber Security To Cyber Resilience

SWISS SUPPORT CENTER FOR CYBERSECURITY

- Cyber Security
  - Protection of Internet-connected systems (hardware, software, and data) from cyber threats
  - Protection against unauthorized access to stored data and computerized systems
- Cyber Resilience
  - Preparation for responses to attacks and vulnerabilities
  - Cybersecurity strategy and program for organizations to mitigate damage from attacks (data breaches, vulnerabilities, malware attacks, insider threats, human errors)
- **Goal**: *Align cyber security and cyber resilience plans*

Definitions of Cyber Resilience

- *"Cyber Resilience Engineering Framework"* (MITRE technical report [1]):
  - **Anticipate**: maintain a state of informed preparedness in order to forestall compromises of mission/business functions from adversary attacks,
  - **Withstand**: continue essential mission/business functions despite successful execution of an attack by an adversary,
  - **Recover**: restore mission/business functions to the maximum extent possible subsequent to successful execution of an attack by an adversary, and
  - **Evolve**: to change missions/business functions and/or the supporting cyber capabilities, so as to minimize adverse impacts from actual or predicted adversary attacks.

Definitions of Cyber Resilience

- *“Cyber resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”* NIST publication 800-160, Volume 2 (see [2])
- “*Cyber resilience is an organization's ability to prevent, withstand and recover from cybersecurity incidents.*”, IBM (see [3])
- “*Cyber resilience refers to an organization's ability to identify, respond, and recover swiftly from an IT security incident. Building cyber resilience includes making a risk-focused plan that assumes the business will at some point face a breach or an attack.*”, Cisco Systems (see [4])

Means to Reach Cyber Resilience

SS SWISS SUPPORT CENTER FOR CYBERSECURITY CC

- Technology
  - “Zero Trust Architectures” (see [5])
  - “Cyber Hygiene” (see [6])
  - Defense in Depth
  - ...
- Operations
  - Cyber Trainings (cyber ranges, blue/red teaming)
  - Security Operations Center (detection, incident response)
  - …
- Organization
  - Business Continuity Management (BCM)
  - Crisis Exercises/Drills
  - …

Today’s Speakers

SWISS SUPPORT CENTER FOR CYBERSECURITY

- **Mathias Payer**: "Why fuzz about security? How automated testing saves developer time and improves security"
- **Melanie Knieps**: "CYRENZH - On engaging students and citizens in cyber resilience"
- **Nicolas Frey**: "Small and Medium Organisations : paving the way for effective resilience"
- **Fabien Leimgruber**: "CyberPeace Builders: Partnering with Companies to Enhance Cyber Resilience in Nonprofits"
- **Monica Ratte**: "How can the NCSC help me increase my resilience?"

References

- [1]: Mitre Cyber-Resilience Engineering Framework, Technical Report, Deborah Bodeau and Richard Graubart, 2011, https://www.mitre.org/sites/default/files/media/publication/11_4436_2.pdf
- [2]“Developing Cyber Resilient Systems, A System Security Engineering Approach”, NIST Special Publication 800-160, Volume 2, 2021, https://doi.org/10.6028/NIST.SP.800-160v2r1
- [3]: “What is Cyber Resilience?”, IBM online resource, https://www.ibm.com/topics/cyber-resilience
- [4]: “What is Cyber Resilience?”, Cisco Systems online resource, https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-cyber-resilience.html

References

- [5]: “Zero Trust Architecture”, NIST Special Publication 800-207, 2020, https://doi.org/10.6028/NIST.SP.800-207
- [6]: Microsoft Defense Report 2023 (MDDR), online resource, https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023