Gesetzliche Grundlagen für digitale Sicherheit

Digitale Gesellschaft, Stammtisch vom 19.11.2020

Wir machen Infrastrukturen und Menschen digital sicher

www.electrosuisse.ch/cybersecurity

Electrosuisse

- 1889 gegründet als Schweizerischer Elektrotechnischer Verein (SEV).
- 2002 Neupositionierung als Electrosuisse, Fachverband für Elektro-, Energie- und Informationstechnik.

- Hauptsitz in Fehraltorf, 230 Mitarbeitende.
- Mitglieder: 4500 Fachleute und mehr als 2000 Firmen.
- Akkreditierte und neutrale Fachstelle mit Angeboten zu Normung, Inspektion/Prüfung, Zertifizierung, Beratung und Weiterbildung.

- Seit über 130 Jahren engagiert für Sicherheit in der Elektrotechnik.
- Seit 2018 auch **engagiert für Cybersicherheit.**

Das Cybersecurity Grundproblem

Drittes newtonsches Axiom im Cyberspace?

ACTIO:

- Unreife Software auf löchriger Hardware (Bananaware & Crapware)
- Sicherheitsgefährdende Geschäftsmodelle
- Malware & Stalkerware
- Cyber-Kriminalität
- Fehlende Sicherheitsvorschriften

REACTIO:

- Security Patches
- Security Tools
- Threat Intelligence
- Nutzungsrichtlinien
- Awareness Training
- Notfallvorbereitung
- Empfehlungen

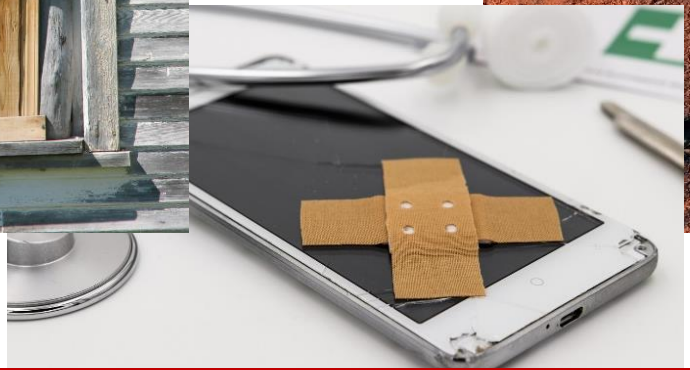
Reagieren wir richtig auf die Probleme?

Security Patches

Läufst Du auch jeden Abend um Dein Haus und flickst Löcher in der Mauer?

Er schon.

Aktuelle Sicherheitslösungen sind ein Flickwerk zur Symptombekämpfung



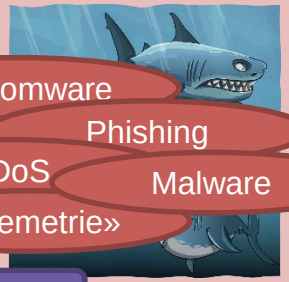
… und vergrössern womöglich die Angriffsfläche

Aktuelle Bemühungen

**Wie sinnvoll ist es, nur den Leuten beizubringen,
mit solchen Fahrzeugen sicher zu fahren?**

Cybersecurity Status Quo und Quo Vadis?

Problembereich



Ransomware
Phishing
DDoS
Malware
«Telemetrie»

Nachlässigkeit
Awareness

Unwissen
Das schwächste Glied

Komplexität
Schwachstellen

Cloud
IoT

Ignoranz
Fachkräftemangel

Empfehlung 957
Empfehlung 1

amazon
facebook
Google
Microsoft
Tencent 腾讯
Alibaba Group 阿里巴巴集团
百度

Smart Everything
Big Data

Gesetz des Stärkeren

?

Lösungsbereich

- Gesetze
- Normen
- Prüfung & Zertifizierung
- Anreize & Belohnung
- Sanktionierung
- Bildung
- Sponsoring

Gleiche Regeln für alle

Vergleich verbindlicher Sicherheit beim Strassenverkehr und Datenverkehr

Strassenverkehr

Produkte & Hersteller	Anwender
Technische Normen	Strassenverkehrsgesetz Verkehrsregeln
Sicherheitsvorschriften für Hersteller	Halterhaftpflicht-Versicherung
Produkthaftung	Verkehrszulassung
Typenprüfung	Fahrprüfung
Periodische Fahrzeugkontrolle	Verkehrskontrollen

Datenverkehr / ICT

ISO/IEC 27xxx, IEC 62443, …

Datenschutzgesetz

Governance & Compliance (implizit)

?

Digitaler Wilder Westen

→ Laws & Marshals!!!

Welchen Toaster würdest Du wählen?

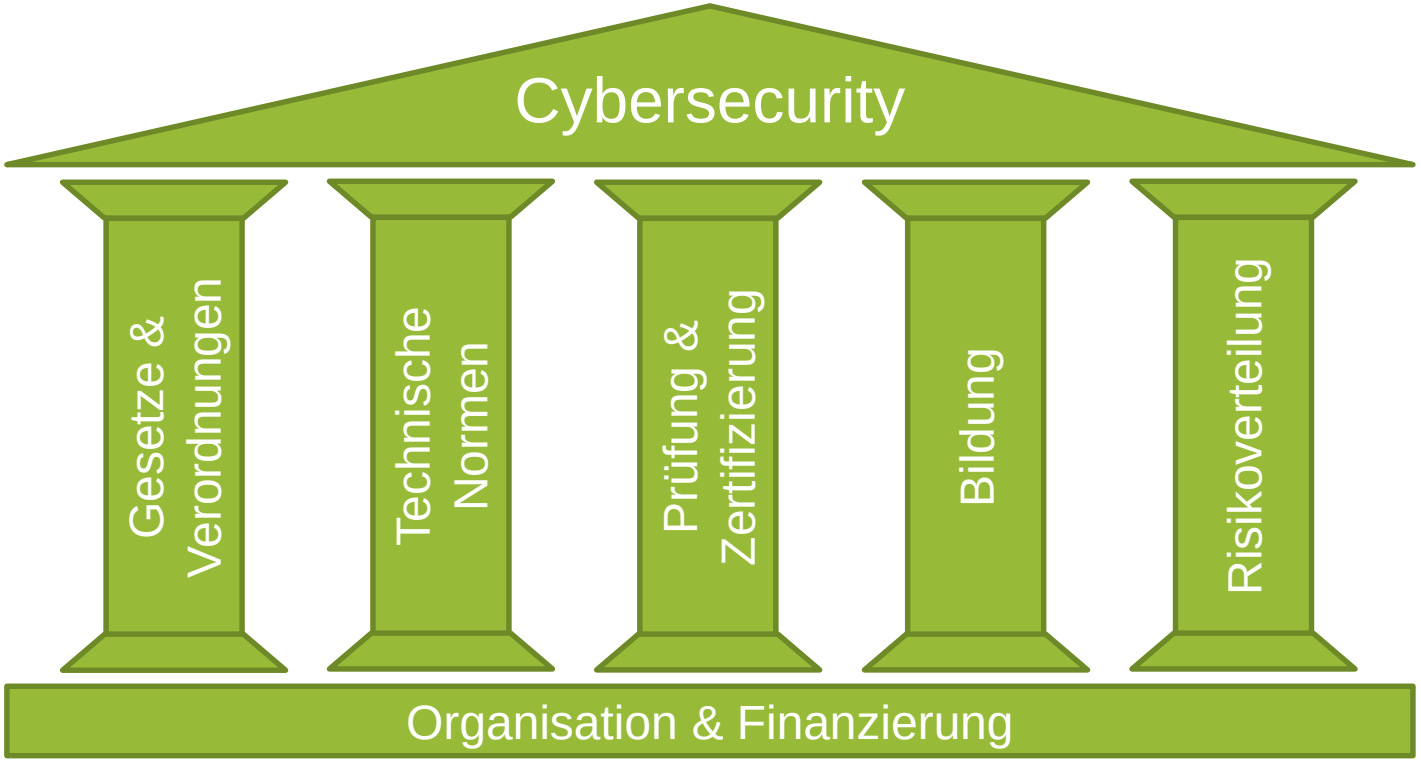
Toaster gestern

Toaster heute

ICT & IoT heute

ICT & IoT morgen?

Cybersecurity Pfeiler



Problemstellung

- **Aktuelle Standards** sind in verschiedener Hinsicht **ungenügend**, nicht einfach umsetzbar, nicht skalierbar und unverbindlich.
- Wildwuchs an Initiativen und **Empfehlungen** für Anwender mit **dürftigem Erfolg**.
- Hersteller und Anbieter als primäre Gefahrenverursacher vernachlässigt → **Symptombekämpfung**.
- **Fehlende Transparenz** bezüglich Risiken.
- **Fehlende Souveränität** der Systemeigner über ihre Systeme und der Benutzer über ihre Daten.
- Fehlende gesetzliche **Mindestsicherheitsstandards**.

Regulierung der digitalen Sicherheit

- Cybersecurity ist eine gemeinschaftliche Aufgabe von Bund, Kantonen, Wissenschaft, Wirtschaft und Gesellschaft.
- Sicherheit braucht Regeln (gesetzliche Grundlagen):
  - **a)** **Gesetzliche Vorschriften** für Herstellung, Inverkehrbringung, Wartung und Betrieb informationstechnischer Produkte/Systeme über deren gesamten Lebenszyklus.
  - **b)** **Verordnung** dazu verweist auf Norm(en) als «anerkannte Regeln der Technik».
  - c) Gesellschaftliche Verhaltensregeln, Haftungs- und Strafbestimmungen.
  - **d)** **Cybersecurity Label** für Produkte und Dienste als Orientierungshilfe für Kunden und eine **Prüf- und Zertifizierungsorganisation** dazu.
  - **e)** **Umsetzungsnorm** (analog Niederspannungs-Installationsnorm NIN).

Cybersecurity-Regulierungsrahmen

Gesetz und Verordnung
- Allgemeine Bestimmungen
- Vorschriften für Hersteller und Dienstanbieter
- Vorschriften für Händler und Lieferanten
- Vorschriften für Betreiber und Integratoren
- Haftungs- und Strafbestimmungen
- Volle System- und Datensouveränität
- Volle Transparenz bezüglich Risiken

Umsetzungsnorm («anerkannte Regeln der Technik»)
- Hersteller und Dienstanbieter
- Systembetreiber und -integratoren

Bildung und Zulassung
- «Internet-Führerschein»
- Integrator-Konzession

Cybersecurity Label
- Selbstdeklaration
- Geprüfte Cybersecurity

Zertifizierung und Inspektion
- Label-Zertifizierung
- Periodische Installationskontrolle

Cybersecurity Label für Produkte & Dienste

Aspekte

- Umsetzung von Sicherheitsgrundsätzen (Security by Design & Default)
- Normenkonformität
- Transparenz bezüglich Risiken
- Systemsouveränität für Systemeigner
- Datensouveränität für Benutzer
- Keine bekannte Schwachstellen
- Security Support

Trust Level

Selbstdeklaration

obligatorisch

- durch Hersteller oder Dienstanbieter

Zertifizierung

freiwillig

- durch unabh. und akkred. Prüfstelle
- Korrektheit der Selbstdeklaration
- Beurteilung der Umsetzungsqualität

Momentaufnahme

Label-Version | Prüfling-Version | Prüfdatum | Prüfstelle

… soll zu einer eigenen Norm werden

Gesetzliche Anknüpfungspunkte

- Bundesgesetz über die Produktesicherheit (PrSG)
- Verordnung über die Produktesicherheit (PrSV)
- Bundesgesetz über die Produktehaftpflicht (PrHG)

Anpassungsbedarf:

- Definition von «Produkt»
- Definition von «Sicherheit»

Danke für Eure Aufmerksamkeit!

Die Zukunft ist heute schon digital.

Machen wir sie auch sicher!