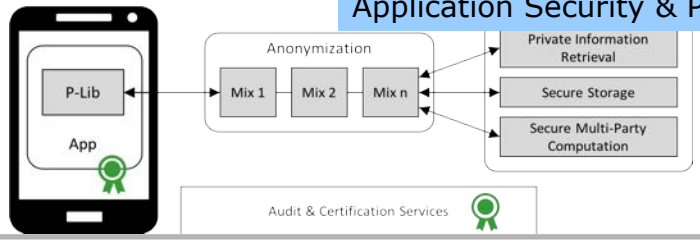
Cybersicherheit – verschärfte Bedrohungslage durch den Ukrainekrieg

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)
http://svs.informatik.uni-hamburg.de

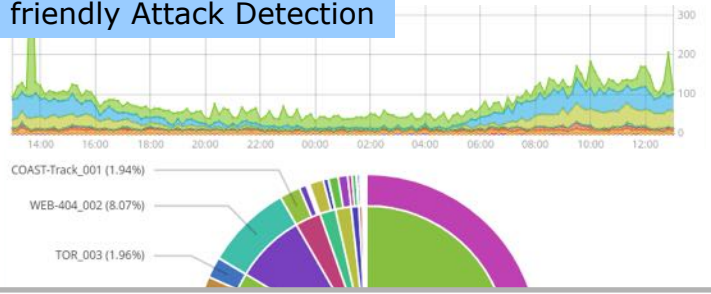
Research: Data Protection and Privacy (Selection)

Privacy Enhancing Technologies

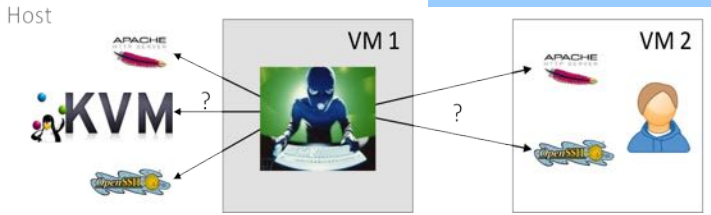
Application Security & Privacy



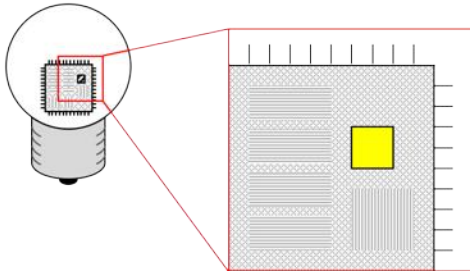
Privacy friendly Attack Detection

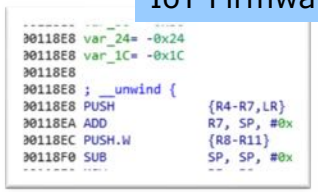


Cloud Security & Privacy



IoT Security & Forensics





IoT Firmware Reverse Engineering

Research: Data Protection and Privacy (Selection)

Privacy Enhancing Technologies

Application Security & Privacy

Drittmittelgeförderte Forschungsprojekte

AppPETs

IDOMENEO | RABATT
A GermanVasc Study

DREI
Datenschutz-respektierende Erkennung von Innentätern

EMPRI-DEVOPS

NEW 4.0
Norddeutsche EnergieWende

AN.ON
NEXT GENERATION

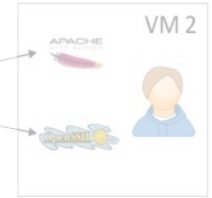
IHATEC
Innovative Hafentechnologien

NRL
Norddeutsches RealLabor

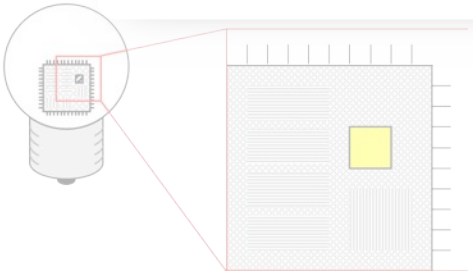
Information Governance Technologies

Privacy friendly Attack Detection

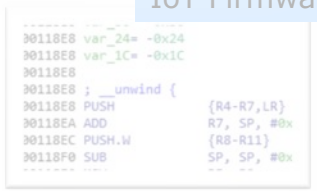
Cloud Security & Privacy

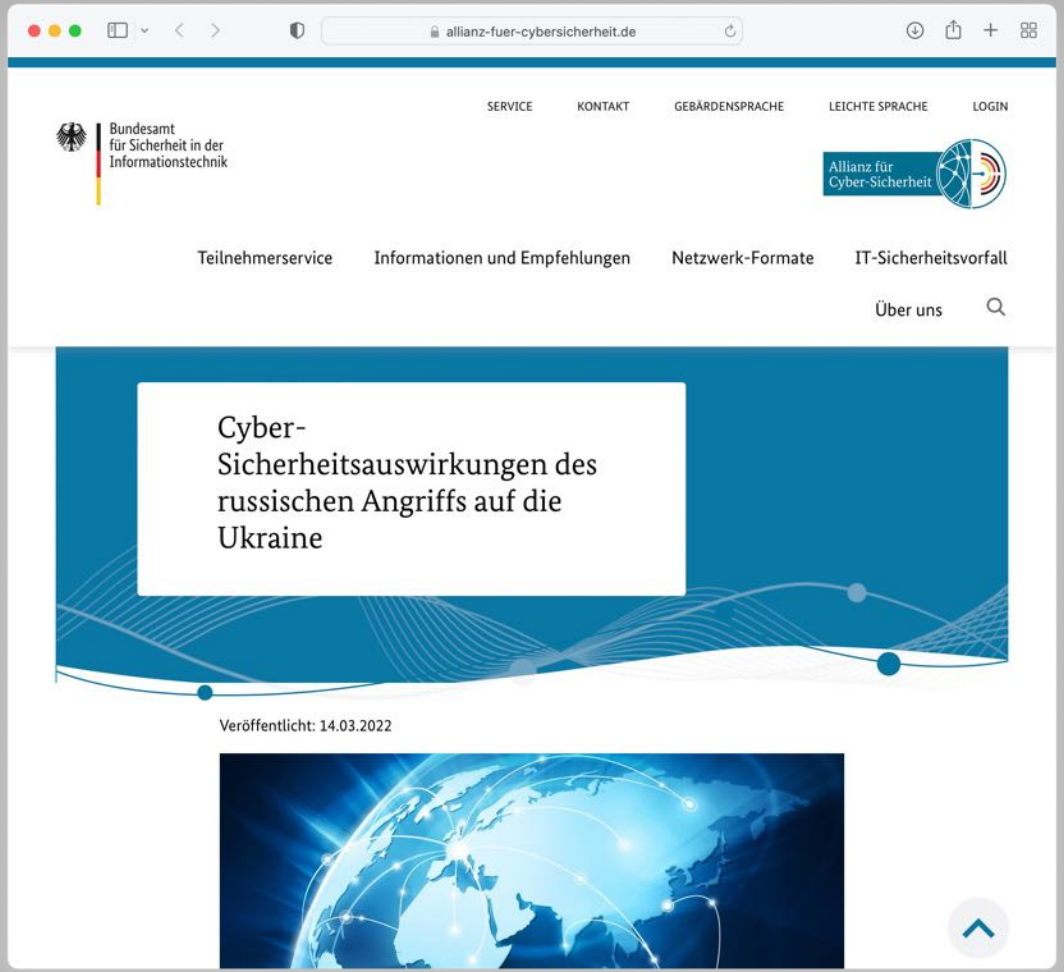


IoT Security & Forensics



IoT Firmware Reverse Engineering





https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Cyber-Sicherheitslage-fuer-die-Wirtschaft/gravierende-Cyber-Risiken/Ukraine_Konflikt/ukraine_konflikt.html

Der russische Angriff auf die Ukraine am 24.02.2022 markiert, so Bundeskanzler Olaf Scholz, eine Zeitenwende. Die Entwicklungen werden mit großer Unruhe betrachtet. Kurz vor und während dem Einmarsch der russischen Truppen in die Ukraine gab es zahlreiche digitale Angriffe auf ukrainische Infrastrukturen und auf regierungsnahe Unternehmen. Nachrichten über Cyber-Angriffe und einen „Krieg im Netz" schüren auch in Deutschland Unsicherheit und Sorge. Was bedeutet die aktuelle Lage für Unternehmen in Deutschland?

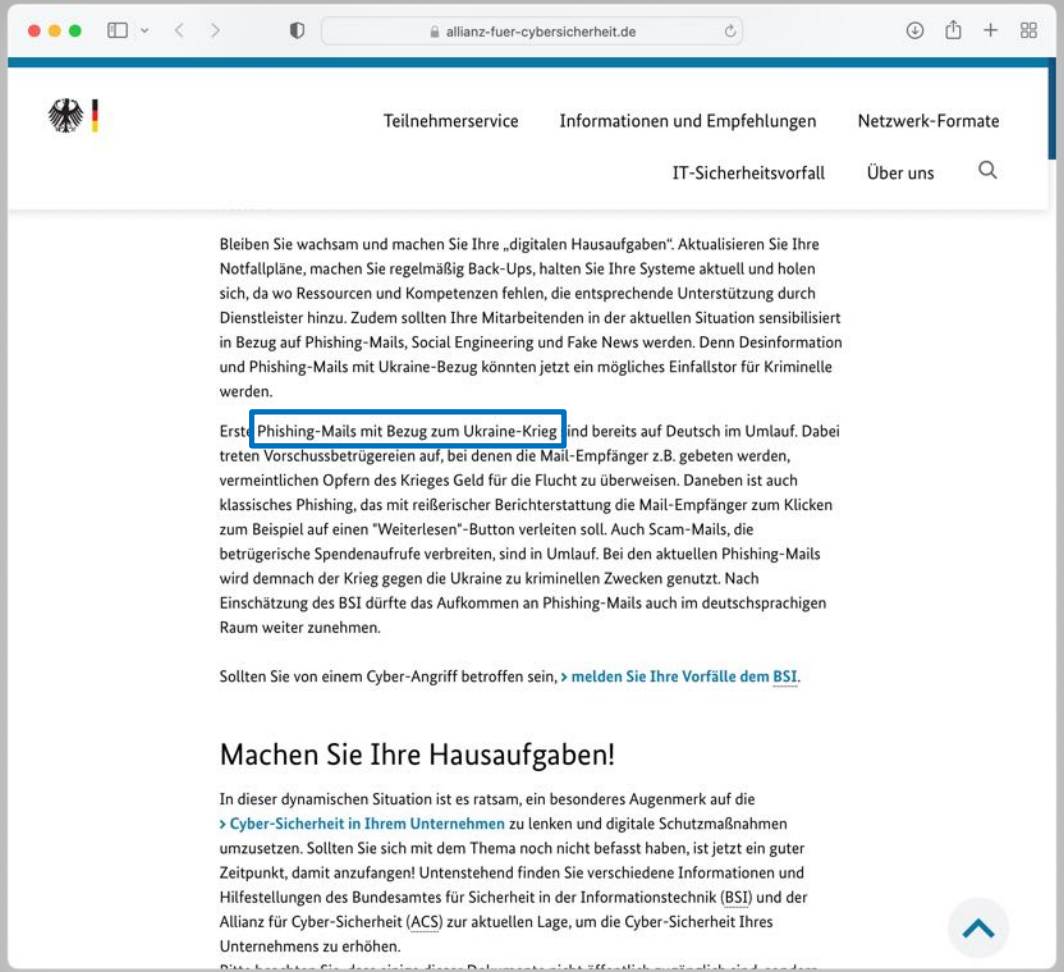
Bleiben Sie ruhig, bleiben Sie wachsam!

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bewertet fortwährend die Lage mit Bezug zur Informationssicherheit und steht in engem Austausch mit dem Bundesministerium des Innern und für Heimat (BMI) sowie zahlreichen nationalen und internationalen Partnerbehörden. Alle Informationen zur Lage mit Bezug zur Informationssicherheit laufen zudem im Nationalen Cyber-Abwehrzentrum in Bonn zusammen und werden dort ausgewertet.

Abstrakt erhöhte Bedrohungslage - Keine akute unmittelbare Gefährdung der Informationssicherheit in Deutschland

Das BSI erkennt eine abstrakt erhöhte Bedrohungslage für Deutschland. Der Konflikt wird weiterhin von verschiedensten Formen von Cyber-Angriffen begleitet.
Der Angriff auf den Betreiber aus der Branche Mineralöl ist der erste schwere direkte Cyber-Angriff in Deutschland, der einen unmittelbaren Bezug zum russischen Angriffskrieg in der

https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Cyber-Sicherheitslage-fuer-die-Wirtschaft/gravierende-Cyber-Risiken/Ukraine_Konflikt/ukraine_konflikt.html



https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Cyber-Sicherheitslage-fuer-die-Wirtschaft/gravierende-Cyber-Risiken/Ukraine_Konflikt/ukraine_konflikt.html

Scamming Mail mit Spendenaufruf

Ukraine Humaniterian Donation

From Ukraine / Україна Govt® on 2022-02-28 15:19

Details Plain text

A donation campaign has been launched to support Ukrain and also help refugees fleeing the conflict in Ukraine
The campaign, organized by the humanitarian organization Act for Peace, is hoping to raise **$9,000,000** to support refugees in the region.

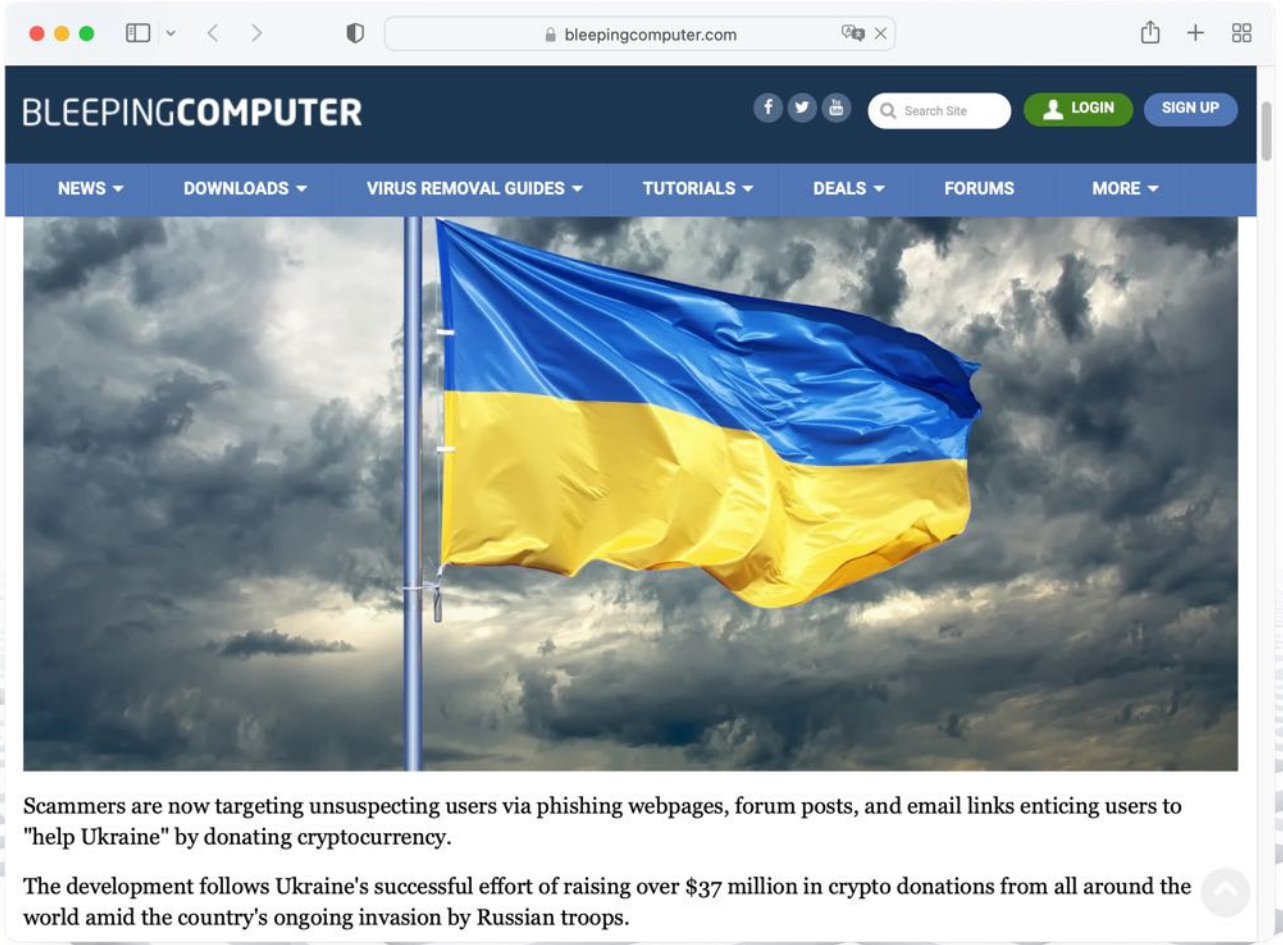
Stand with the people of Ukraine. Now accepting cryptocurrency donations. Bitcoin, Ethereum, USDT and NFT

BTC- bc1qqglytupu8pup07eksh3gd77edkd3ge7ku6809y

ETH- 0x5535480a9D0F39b545F9c14b0a70a8755237b01f

Best Regards
Ukraine
#BeautifulUkraine

https://www.bleepingcomputer.com/news/security/help-ukraine-crypto-scams-emerge-as-ukraine-raises-over-37-million/



https://www.bleepingcomputer.com/news/security/help-ukraine-crypto-scams-emerge-as-ukraine-raises-over-37-million/

handelsblatt.com

Handelsblatt

MEINE NEWS | HOME | POLITIK | UNTERNEHMEN | TECHNOLOGIE | FINANZEN | MOBILITÄT | KARRIERE | ARTS & STYLE | MEINUNG | VIDEO | SERVICE

Industrie | Energie | Handel + Konsumgüter | Dienstleister | Medien | Mittelstand | Management | Nachhaltigkeit

Handelsblatt > Unternehmen > Energie > BSI: Warnung vor weiteren Angriffen nach Hackerangriff auf Ölkonzern Rosneft

Suchbegriff, WKN, ISIN

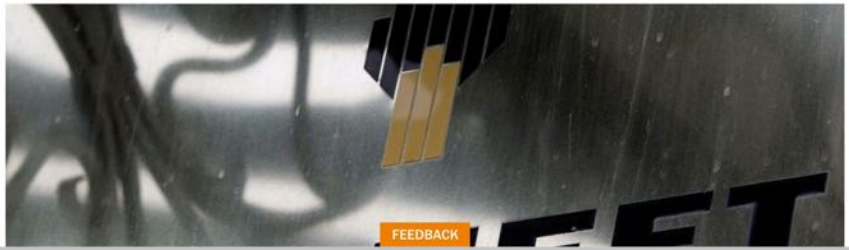
IT-SICHERHEIT

Nach Cyberangriff auf Rosneft: BSI warnt Mineralölwirtschaft vor weiteren Angriffen

Das Hackerkollektiv Anonymous hat angeblich große Datenmengen kopiert. Der Angriff kam wohl über die Druckersteuerung – die Staatsanwaltschaft ermittelt.

Christof Kerkmann, Lars-Marten Nagel, Claudia Scholz, Klaus Stratmann, Kathrin Witsch

14.03.2022 • Update: 14.03.2022 - 15:07 Uhr • Kommentieren • 1 x geteilt



https://www.handelsblatt.com/unternehmen/energie/it-sicherheit-nach-cyberangriff-auf-rosneft-bsi-warnt-mineraloelwirtschaft-vor-weiteren-angriffen-/28160768.html

handelsblatt.com

Rosneft

Der Konzern ist Russlands größter Ölproduzent.
(Foto: Reuters)

Berlin. Ein Cyberangriff auf die deutsche Tochter des russischen Mineralölkonzerns Rosneft hat zu einem massiven Datenverlust geführt. Die Hacker haben offenbar auch noch andere Unternehmen der Branche im Visier: Wie das Handelsblatt aus IT-Sicherheitskreisen erfahren hat, gab es Zugriffsversuche über Fernwartungszugänge. Diese seien jedoch von den Betreibern durch Trennen der Verbindung unterbunden worden.

Der Hackerangriff der Gruppe Anonymous war am Wochenende durch übereinstimmende Medienberichte in „Spiegel“ und „Welt“ bekannt geworden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bestätigte am Montag, dass das Unternehmen in der Nacht zu Samstag einen IT-Sicherheitsvorfall gemeldet habe. Dazu ist es verpflichtet, weil es eine „kritische Infrastruktur“ betreibt.

Auswirkungen auf die Versorgung seien bisher nicht offenbar geworden, schrieb das BSI. Der Betreiber und die Behörden seien in stetigem Austausch. „Das BSI hat zudem eine entsprechende Cybersicherheitswarnung an andere Unternehmen und Organisationen der Mineralölwirtschaft herausgegeben.“ Der Vorfall bestätige die Einschätzung der Behörde zur verschärften Sicherheitslage im Cyberraum kurz nach Beginn des russischen Angriffs auf die Ukraine.

FEEDBACK

https://www.handelsblatt.com/unternehmen/energie/it-sicherheit-nach-cyberangriff-auf-rosneft-bsi-warnt-mineraloelwirtschaft-vor-weiteren-angriffen-/28160768.html

enercon.de

Aktuell | Ukraine-Krieg: Satellitenverbindung KA-SAT ausgefallen - Golem.de

ENERCON
ENERGIE FÜR DIE WELT

Aktuell | Download-Portal | Karriere-Portal | Aloys Wobben Stiftung | Language: Deutsch

Produkte | Technologie | Service | Dienstleistungen | Unternehmen | Referenzen | Kontakt

Aktuelle Themen & Trends

☑ Alle Artikel ☐ Unternehmen ☐ Messen ☐ Produkte & Technologie ☐ Service

ENERCON-Installationen übertreffen in Deutschland 25 Gigawatt

Meilenstein im Bürgerwindpark Ebersdorf/Niedersachsen erreicht – gemeinsam mit Kunden weiterer forcierter Windenergie-Ausbau angestrebt

Artikel lesen

Störung der Satellitenverbindung zu Windenergieanlagen

Durch die Störung ist lediglich der Kommunikationskanal des Service zu den Anlagen beeinträchtigt.

Artikel lesen

ENERCON erhält Auftrag von Ørsted in Nordirland

ENERCON installiert 16 MW im Rahmen eines Corporate Power Purchase Agreement in Ballykeel in Nordirland

Artikel lesen

ENERCON stellt sich bei zweitem virtuellen Betreiberforum Kundenfragen

Konstruktiver Austausch auch in Pandemiezeiten – mehr als 100 Teilnehmer

Artikel lesen

ENERCON

Alterric

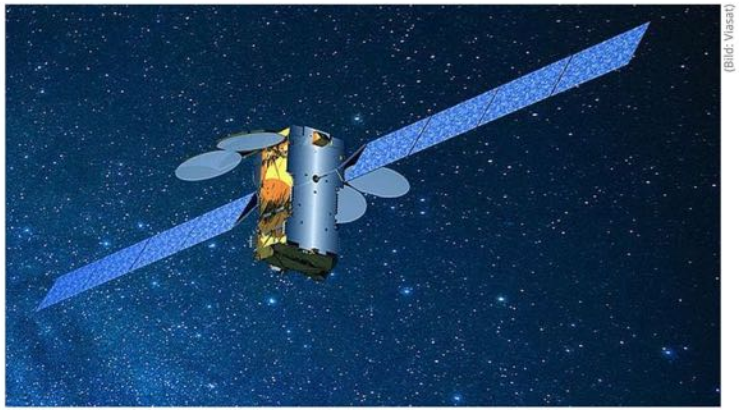
https://www.enercon.de/de/aktuelles/stoerung-der-satellitenverbindung-zu-windenergieanlagen/

UKRAINE-KRIEG

Satelliteninternet KA-SAT ausgefallen

Beginnend mit dem Krieg in der Ukraine begann ein Ausfall des KA-SAT-Satellitennetzwerks. Elon Musk bringt mit Starlink Satelliteninternet.

27. Februar 2022, 12:59 Uhr, Achim Sawall



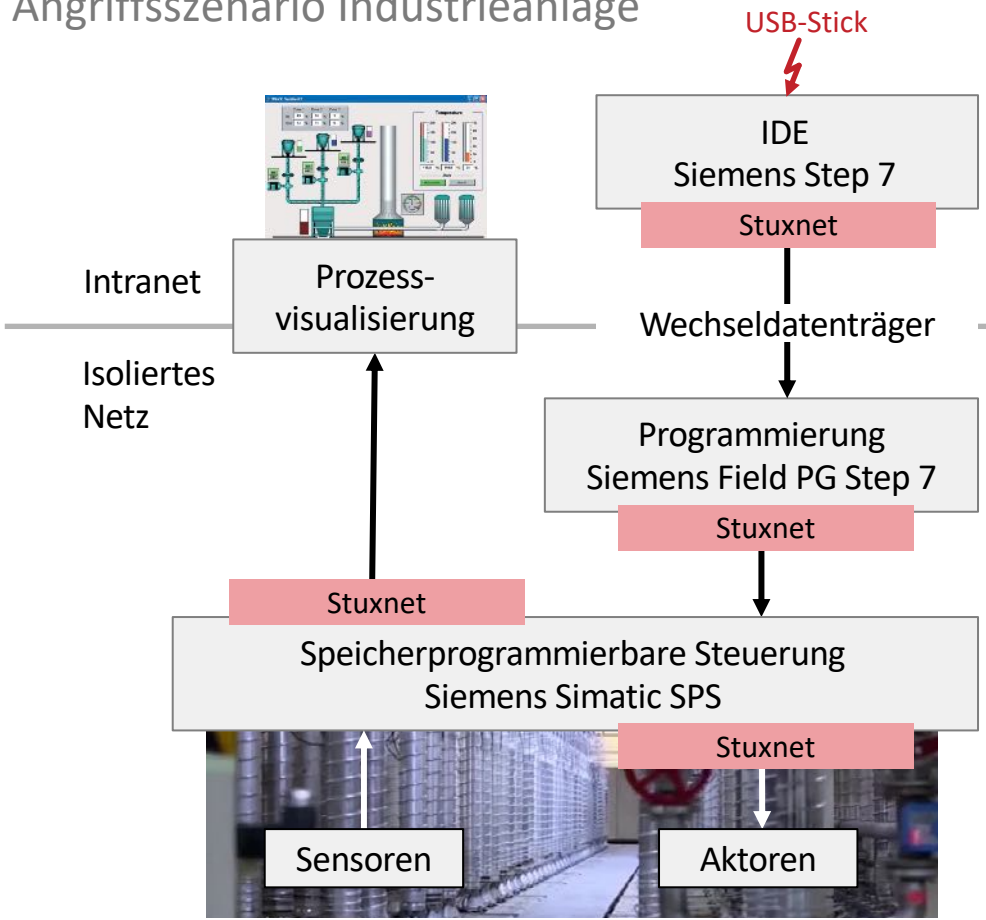
(Bild: Viasat)

KA-SAT-Satellit

Der Dienst des KA-SAT-Satellitennetzwerks über Europa ist weitgehend ausgefallen. Wie aus einer E-Mail des US-Betreibers Viasat an seine Partner hervorgeht, die Golem.de vorliegt, begann das Problem in der Ukraine. *"Dies scheint zunächst mit dem KA-SAT-Dienst in der Ukraine begonnen zu haben und sich anschließend über fast die gesamte KA-SAT-Ausleuchtzone ausgebreitet zu haben"*, heißt es. Viasat betreibt auch verschlüsselte Kommunikationsdienste für das US-Militär.

https://www.golem.de/news/ukraine-krieg-satelliteninternet-ka-sat-ausgefallen-2202-163468.html

Stuxnet:
Angriffsszenario Industrieanlage



Treiber mit gestohlenen Zertifikaten (Realtek, JMicron) signiert

Manipulation Step-7-IO-Treiber und -Projektdateien

Vermutlich genaue Kenntnis der Anlagen vorhanden gewesen

Stuxnet überprüft Konfiguration der SPS und befällt nur bestimmte Systeme

Transitives trojanisches Pferd, da zunächst die IDE befallen wird, um anschließend die SPS zu manipulieren.

Mechanische Zerstörung (Drehzahlmanipulation) der Zentrifugen

Angreifer kann alle drei Schutzziele verletzen:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

- Mögliche Schadfunktionen:
  - Spionagesoftware, Sabotage (Stuxnet)
  - Ransomware (Erpressungstrojaner)
  - Sleeping Time Bombs (Kill Switch)

Bild: WannaCry Ransomware

Typische Angriffsfolge

1. Informationsgewinnung
   - IP-Adressen, Passwörter, Eindringpunkte

Beispiele: Social Engineering, Security Scanner, Port Scanner

2. Angriff (über das Netz)
   - Ausnutzen von Schwächen, Missbrauch von Daten

3. Erweiterung der Rechte
   - insb. Schaffen einer unauffälligen Hintertür

4. Spuren verwischen
   - Löschen oder Manipulieren von Log-Dateien

Schutz z.B. TrueWORM – Write Once Read Multiple mittels CD-R, DVD±R, »Datendiode«

Angriffsfolge nach der Lockheed Martin Cyber Kill Chain

Lockheed Martin, 2015

1. Informationsgewinnung
   - IP-Adressen, Passwörter, Eindringpunkte

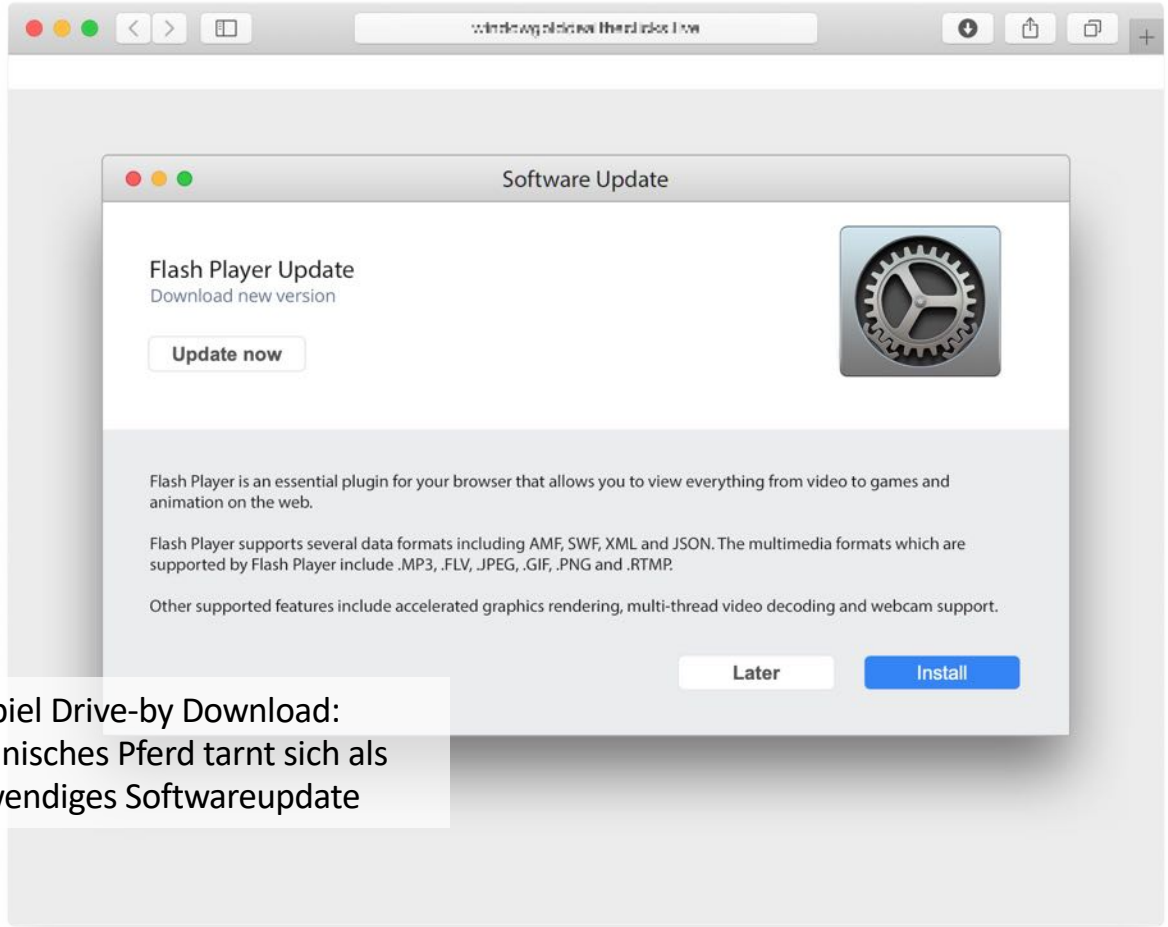
2. Angriff (über das Netz)
   - Ausnutzen von Schwächen, Missbrauch von Daten

3. Erweiterung der Rechte
   - insb. Schaffen einer unauffälligen Hintertür

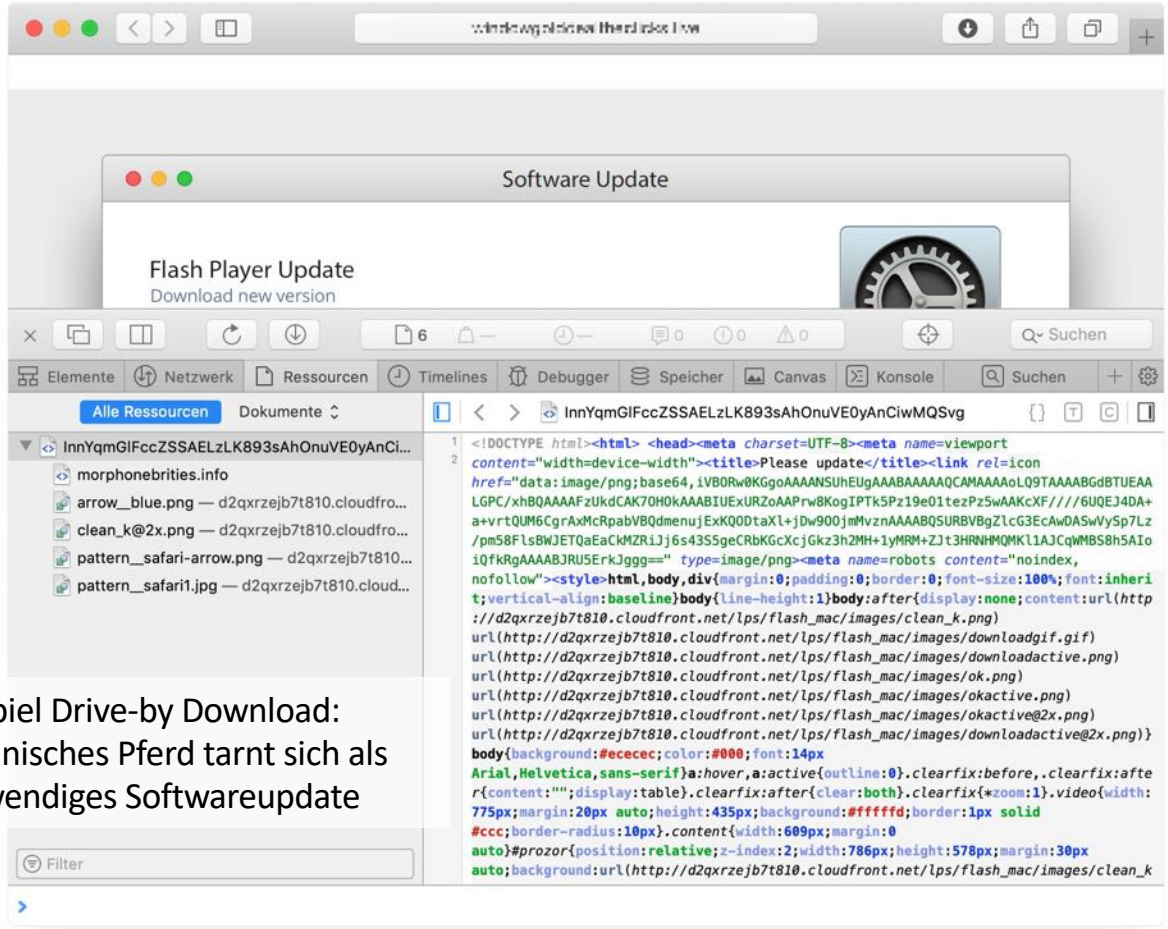
4. Spuren verwischen
   - Löschen oder Manipulieren von Log-Dateien

1. Reconnaissance: Auskundschaften des Ziels
2. Weaponization: Vorbereitung zur Übertragung der Malware
3. Delivery: Übertragung der Malware (E-Mail, USB-Speicher)
4. Exploitation: Initialen Zugang zum Opfer herstellen, Ausnutzen der Schwachstelle beim Opfer
5. Installation: permanenten Zugang zum Opfersystem schaffen (z.B. Backdoors)
6. Command and Control: Fernsteuern des Opfersystems
7. Actions on Objective: (Massenhafte) Angriffe im Netz ausführen (z.B. mittels Botnetz)

Cyber Kill Chain



Beispiel Drive-by Download:
Trojanisches Pferd tarnt sich als notwendiges Softwareupdate



Beispiel Drive-by Download:
Trojanisches Pferd tarnt sich als notwendiges Softwareupdate

MITRE ATT&CK Matrix

https://attack.mitre.org

1. Informationsgewinnung	1. Reconnaissance: Auskundschaften 2. Weaponization: Vorbereitung	
2. Angriff (über das Netz)	3. Delivery: Übertragung Malware 4. Exploitation: Initialer Zugang	
3. Erweiterung der Rechte	5. Installation: Backdoors 6. Command and Control: Fernsteuern 7. Actions on Objective: Angriffe im Netz	
4. Spuren verwischen		

Anzahl der gelisteten Angriffstechniken	
Reconnaissance	10
Resource Development	7
Initial Access	9
Execution	12
Persistence	19
Privilege Escalation	13
Defense Evasion	39
Credential Access	15
Discovery	27
Lateral Movement	9
Collection	17
Command and Control	16
Exfiltration	9
Impact	13

MITRE ATT&CK Matrix

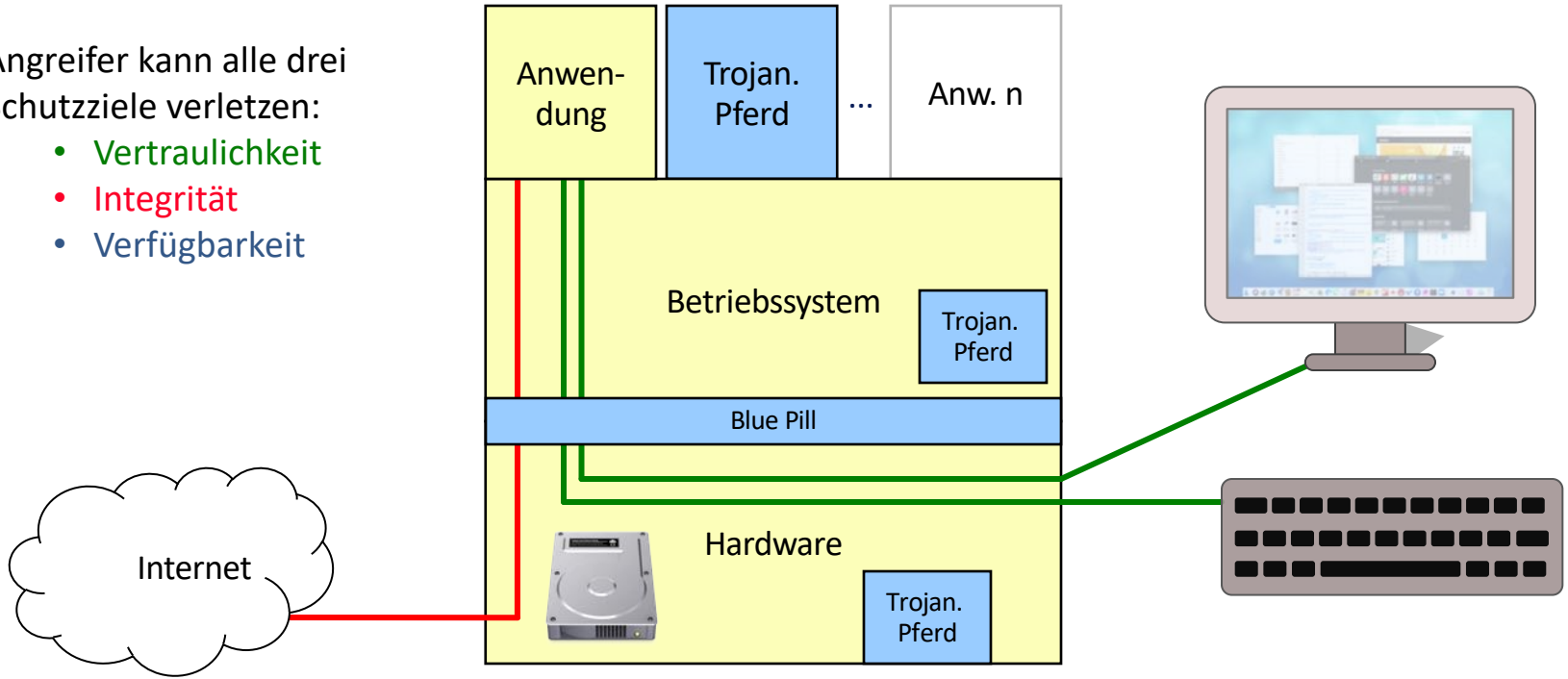
MITRE | ATT&CK®

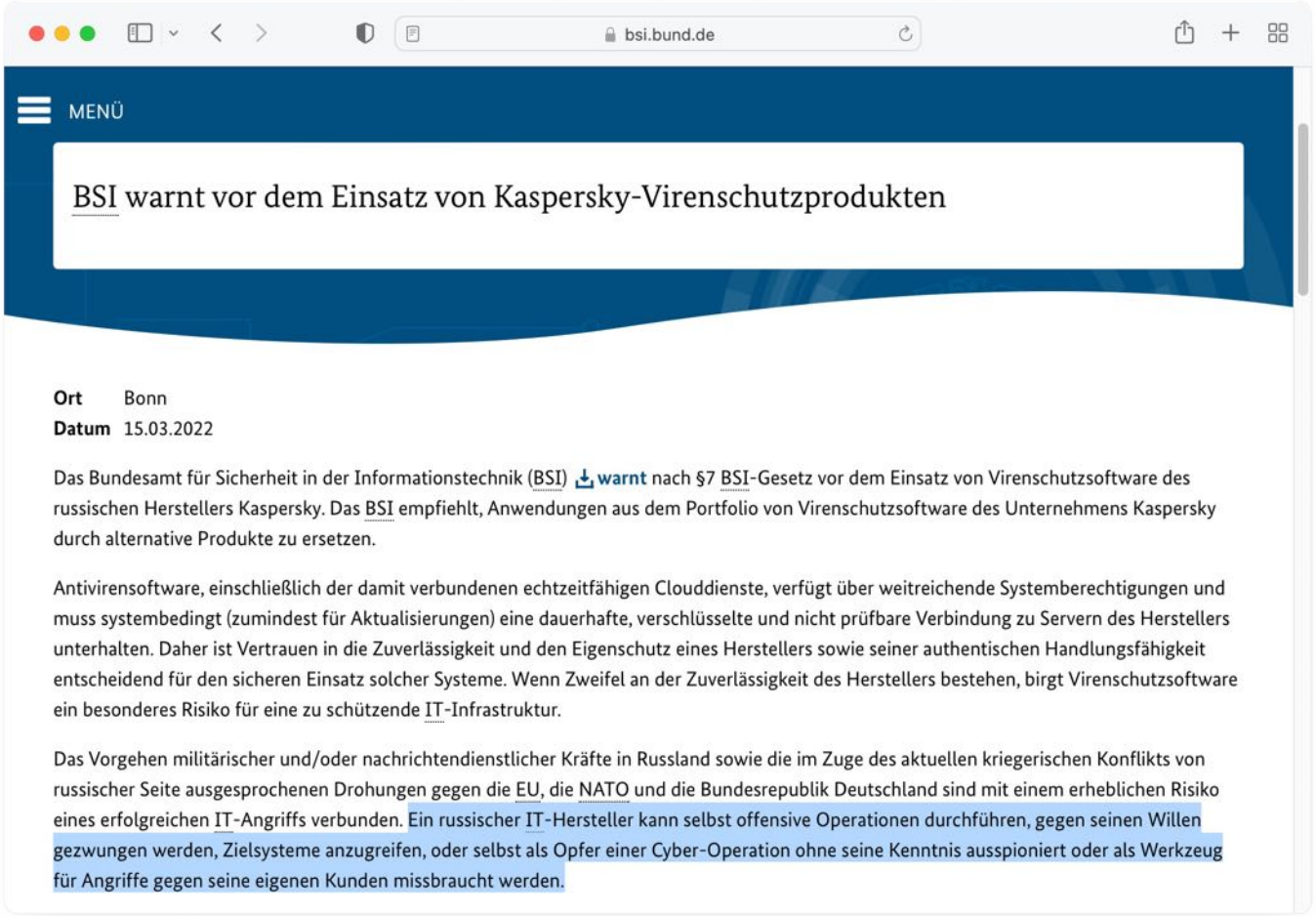
Angriffspunkte für Malware

Angriffspunkte für Malware

Angreifer kann alle drei Schutzziele verletzen:

- Vertraulichkeit
- Integrität
- Verfügbarkeit





https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html

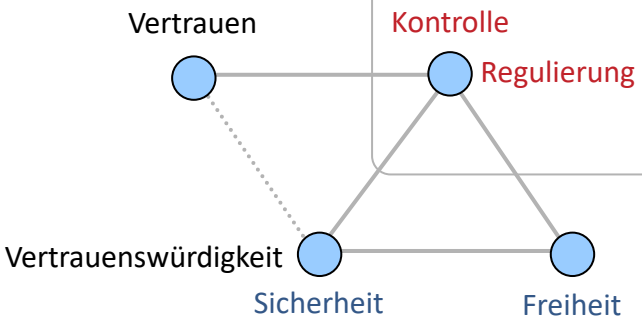
Digitale Souveränität als Schutz

- Aufgabe des Staats, geeignete Rahmenbedingungen zu schaffen

Anreize: Beschäftigungs- und Strukturpolitik für Hitech in Europa
- Forschungs- und Rahmenprogramme
- Zertifizierungen und Gütesiegel von geeigneten Produkten

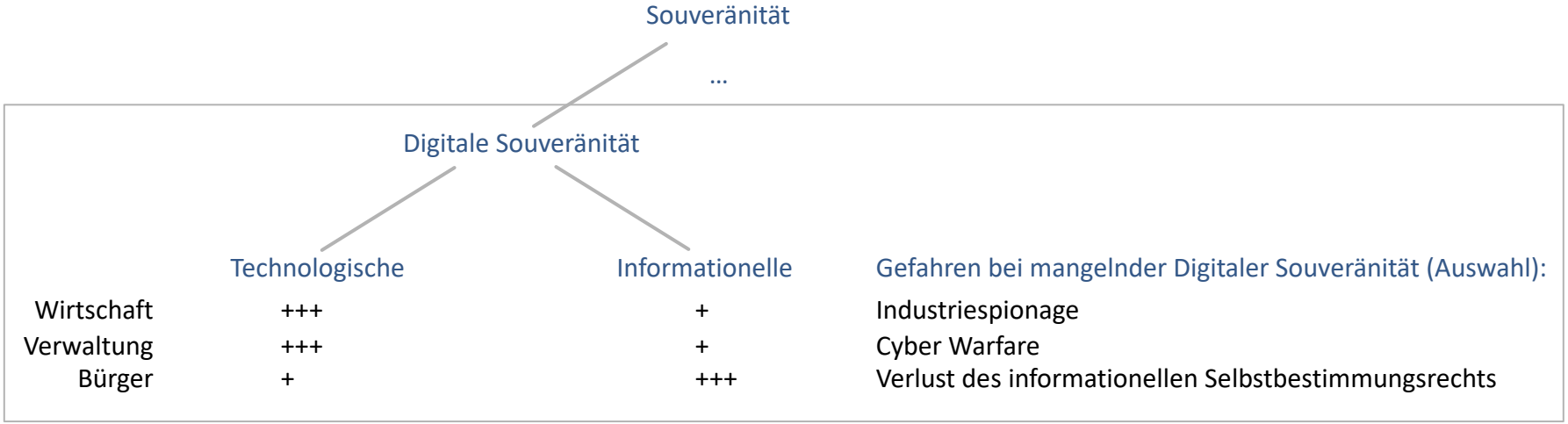
Regulierung: Technologieorientierte Gesetzgebung
- Offenlegungs-, Nachweis- und Kontrollpflichten
- Rechtssicherheit für Technologieanbieter
- Digitale Steuern und Steuererleichterungen für souveräne Technologie

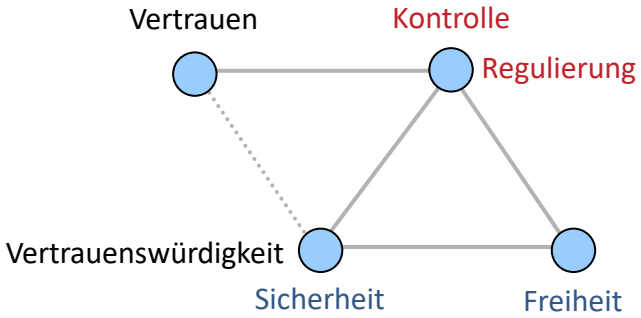
Sanktionen: nur als letztes Mittel
- Einfuhrverbote



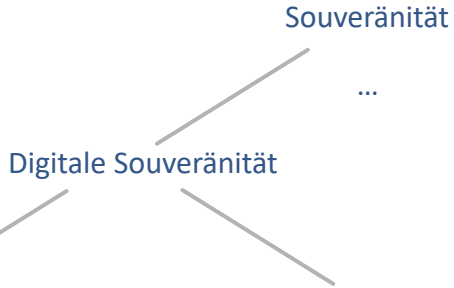
Technologische Souveränität:
- Fähigkeit des Staats, die Kontrolle über Technologien behalten zu können
- Aufgabe des Staats, dafür *geeignete Rahmenbedingungen* zu schaffen

Digitale Souveränität als Schutz





Digitale Souveränität als Schutz



Wirtschaft	+++	+
Verwaltung	+++	+
Bürger	+	+++

Gefahren bei mangelnder Digitaler Souveränität (Auswahl):

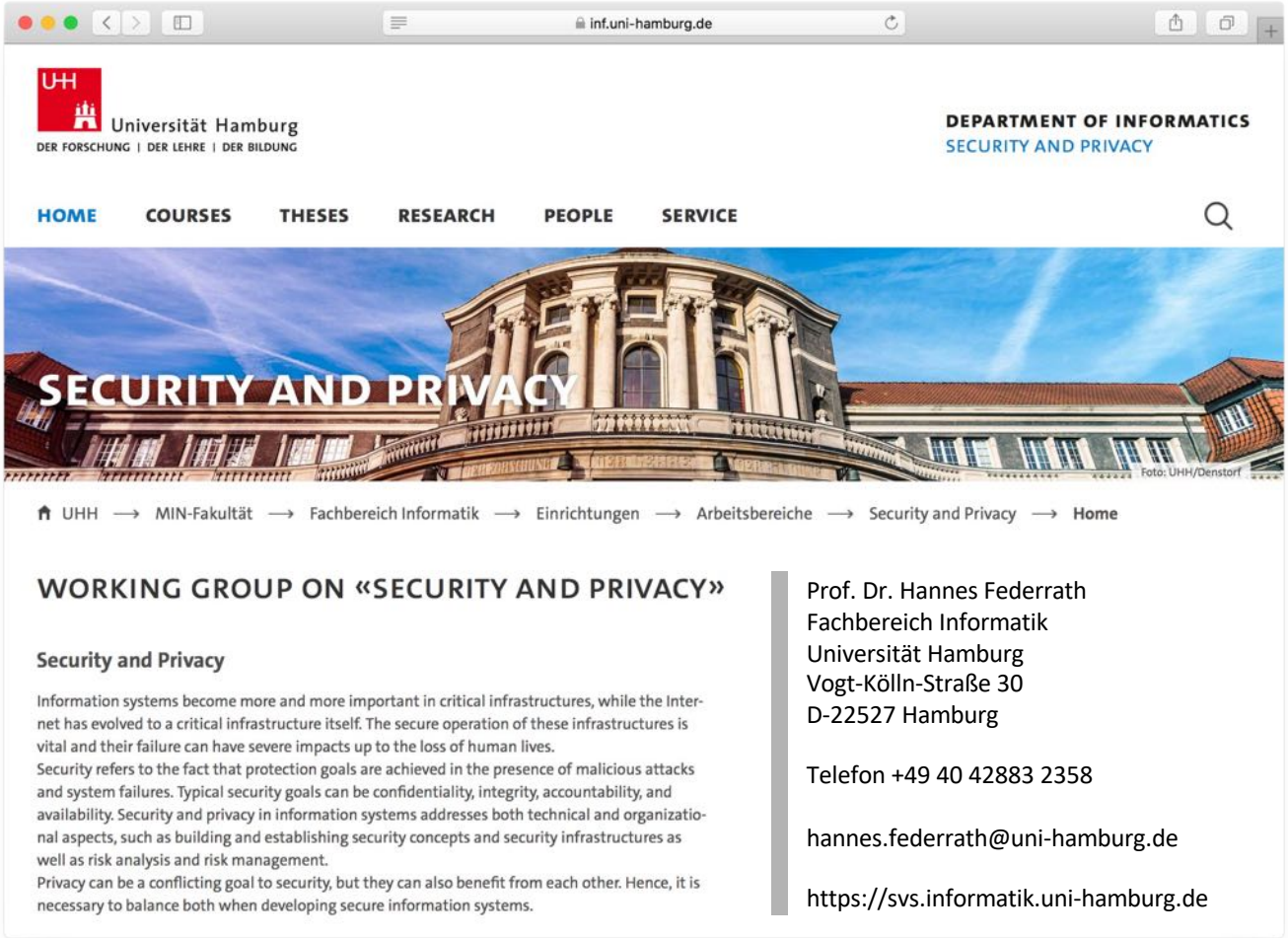
- Industriespionage
- Cyber Warfare
- Verlust des informationellen Selbstbestimmungsrechts

Auswege zur Verbesserung der Digitalen Souveränität:

- Diversität
- Heterogenität
- Offenheit/Offenlegung
- Standardisierung

Folgen mangelnder Digitaler Souveränität:

- Kein Schutz vor verdeckter Fehlerausbreitung
- Lock-in-Effekte
- Abhängigkeit
- Monopole


inf.uni-hamburg.de
UHH
Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG
DEPARTMENT OF INFORMATICS
SECURITY AND PRIVACY
HOME
COURSES
THESES
RESEARCH
PEOPLE
SERVICE
SECURITY AND PRIVACY
Foto: UHH/Denstorf
UHH → MIN-Fakultät → Fachbereich Informatik → Einrichtungen → Arbeitsbereiche → Security and Privacy → Home
WORKING GROUP ON «SECURITY AND PRIVACY»
Security and Privacy
Information systems become more and more important in critical infrastructures, while the Internet has evolved to a critical infrastructure itself. The secure operation of these infrastructures is vital and their failure can have severe impacts up to the loss of human lives.
Security refers to the fact that protection goals are achieved in the presence of malicious attacks and system failures. Typical security goals can be confidentiality, integrity, accountability, and availability. Security and privacy in information systems addresses both technical and organizational aspects, such as building and establishing security concepts and security infrastructures as well as risk analysis and risk management.
Privacy can be a conflicting goal to security, but they can also benefit from each other. Hence, it is necessary to balance both when developing secure information systems.
Prof. Dr. Hannes Federrath
Fachbereich Informatik
Universität Hamburg
Vogt-Kölln-Straße 30
D-22527 Hamburg
Telefon +49 40 42883 2358
hannes.federrath@uni-hamburg.de
https://svs.informatik.uni-hamburg.de