



Cybersicherheit – verschärfte Bedrohungslage durch den Ukrainekrieg

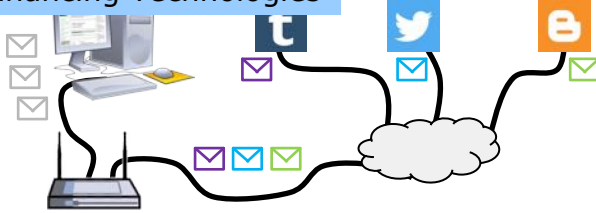
Prof. Dr. Hannes Federrath

Sicherheit in verteilten Systemen (SVS)

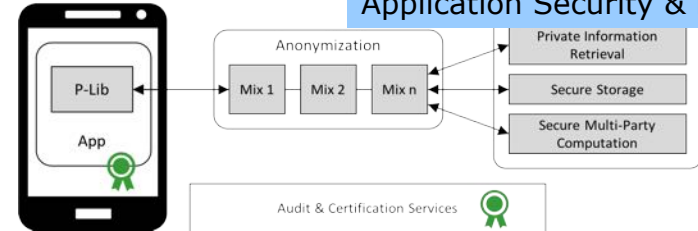
<http://svs.informatik.uni-hamburg.de>

Research: Data Protection and Privacy (Selection)

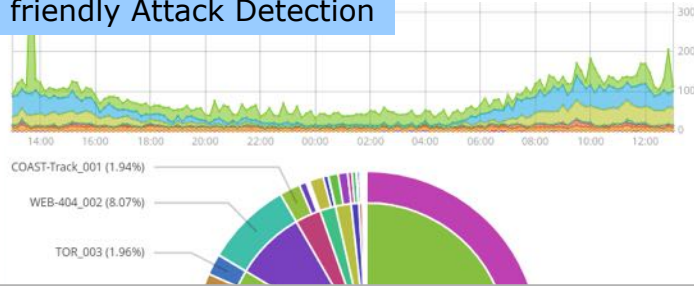
Privacy Enhancing Technologies



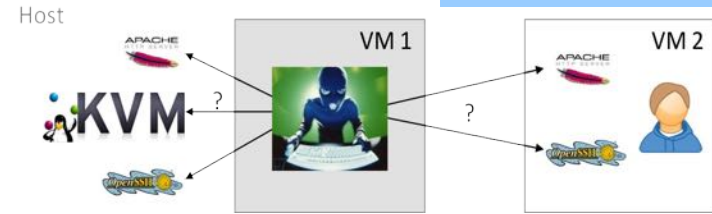
Application Security & Privacy



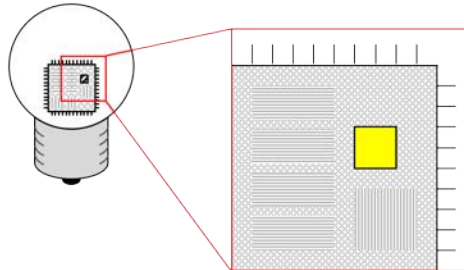
Privacy friendly Attack Detection



Cloud Security & Privacy



IoT Security & Forensics

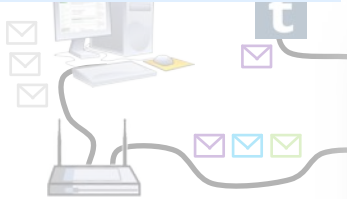


IoT Firmware Reverse Engineering

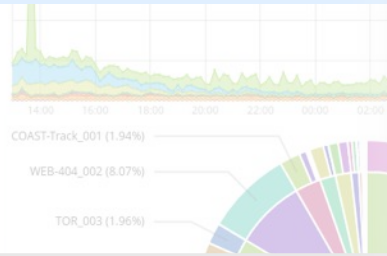
```
00118E8 var_24= -0x24
00118E8 var_1C= -0x1C
00118E8
00118E8 ; __unwind {
00118E8 PUSH      {R4-R7,LR}
00118EA ADD     R7, SP, #0x
00118EC PUSH.W  {R8-R11}
00118F0 SUB     SP, SP, #0x
.....
```

Research: Data Protection and Privacy (Selection)

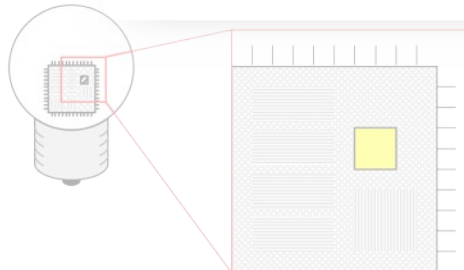
Privacy Enhancing Technologies



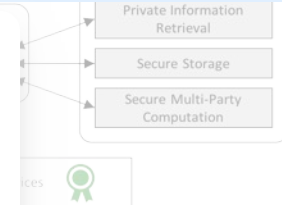
Privacy friendly Attack Detection



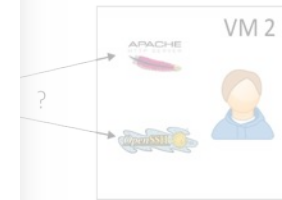
IoT Security & Forensics



Application Security & Privacy



Cloud Security & Privacy



IoT Firmware Reverse Engineering

```
00118E8 var_24= -0x24
00118E8 var_1C= -0x1C
00118E8
00118E8 ; _unwind {
00118E8 PUSH      {R4-R7,LR}
00118EA ADD     R7, SP, #0x
00118EC PUSH.W  {R8-R11}
00118F0 SUB     SP, SP, #0x
```

allianz-fuer-cybersicherheit.de

SERVICE KONTAKT GEBÄRDENSPRACHE LEICHTE SPRACHE LOGIN

Bundesamt für Sicherheit in der Informationstechnik

Allianz für Cyber-Sicherheit

Teilnehmerservice Informationen und Empfehlungen Netzwerk-Formate IT-Sicherheitsvorfall

Über uns

Cyber-Sicherheitsauswirkungen des russischen Angriffs auf die Ukraine

Veröffentlicht: 14.03.2022



Upward arrow icon

allianz-fuer-cybersicherheit.de

 [Teilnehmerservice](#) [Informationen und Empfehlungen](#) [Netzwerk-Formate](#)

[IT-Sicherheitsvorfall](#) [Über uns](#) 



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



allianz-fuer-cybersicherheit.de

 Teilnehmerservice Informationen und Empfehlungen Netzwerk-Formate

IT-Sicherheitsvorfall Über uns

Bleiben Sie wachsam und machen Sie Ihre „digitalen Hausaufgaben“. Aktualisieren Sie Ihre Notfallpläne, machen Sie regelmäßig Back-Ups, halten Sie Ihre Systeme aktuell und holen sich, da wo Ressourcen und Kompetenzen fehlen, die entsprechende Unterstützung durch Dienstleister hinzu. Zudem sollten Ihre Mitarbeitenden in der aktuellen Situation sensibilisiert in Bezug auf Phishing-Mails, Social Engineering und Fake News werden. Denn Desinformation und Phishing-Mails mit Ukraine-Bezug könnten jetzt ein mögliches Einfallstor für Kriminelle werden.

Erste **Phishing-Mails mit Bezug zum Ukraine-Krieg** sind bereits auf Deutsch im Umlauf. Dabei treten Vorschussbetrügereien auf, bei denen die Mail-Empfänger z.B. gebeten werden, vermeintlichen Opfern des Krieges Geld für die Flucht zu überweisen. Daneben ist auch klassisches Phishing, das mit reißerischer Berichterstattung die Mail-Empfänger zum Klicken zum Beispiel auf einen "Weiterlesen"-Button verleiten soll. Auch Scam-Mails, die betrügerische Spendenaufrufe verbreiten, sind in Umlauf. Bei den aktuellen Phishing-Mails wird demnach der Krieg gegen die Ukraine zu kriminellen Zwecken genutzt. Nach Einschätzung des BSI dürfte das Aufkommen an Phishing-Mails auch im deutschsprachigen Raum weiter zunehmen.

Sollten Sie von einem Cyber-Angriff betroffen sein, > [melden Sie Ihre Vorfälle dem BSI](#).

Machen Sie Ihre Hausaufgaben!

In dieser dynamischen Situation ist es ratsam, ein besonderes Augenmerk auf die > [Cyber-Sicherheit in Ihrem Unternehmen](#) zu lenken und digitale Schutzmaßnahmen umzusetzen. Sollten Sie sich mit dem Thema noch nicht befasst haben, ist jetzt ein guter Zeitpunkt, damit anzufangen! Untenstehend finden Sie verschiedene Informationen und Hilfestellungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der Allianz für Cyber-Sicherheit (ACS) zur aktuellen Lage, um die Cyber-Sicherheit Ihres Unternehmens zu erhöhen.

Bitte beachten Sie, dass einige dieser Dokumente nicht öffentlich zugänglich sind und dass

Scamming Mail mit Spendenaufruf

Ukraine Humanitarian 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



bleepingcomputer.com

BLEEPINGCOMPUTER

f t

Search Site

LOGIN

SIGN UP

NEWS ▾DOWNLOADS ▾VIRUS REMOVAL GUIDES ▾TUTORIALS ▾DEALS ▾FORUMS▾MORE ▾



Scammers are now targeting unsuspecting users via phishing webpages, forum posts, and email links enticing users to "help Ukraine" by donating cryptocurrency.

The development follows Ukraine's successful effort of raising over \$37 million in crypto donations from all around the world amid the country's ongoing invasion by Russian troops.

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 🔍

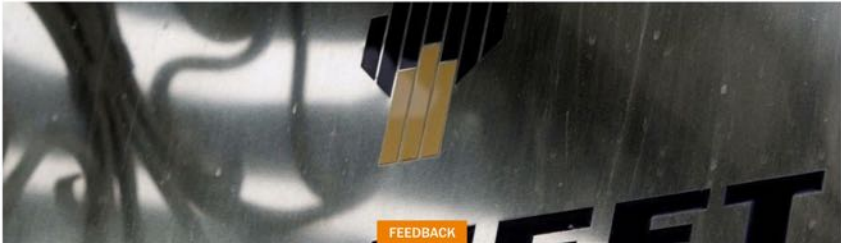
IT-SICHERHEIT

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](#)



FEEDBACK

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

enercon.de

Aktuell

Ukraine-Krieg: Satelliteninternet 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.de

Aktuelles Detail

Ukraine-Krieg: Satelliteninternet KA-SAT ausgefallen - Golem.de



01. März 2022

Störung der Satellitenverbindung zu Windenergieanlagen

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

Aufgrund einer massiven Störung der Satellitenverbindung in Europa ist derzeit die Fernüberwachung und -steuerung von tausenden ENERCON Windenergieanlagen (WEA) nur eingeschränkt möglich. Betroffen von dem Verbindungsausfall sind seit Donnerstag (24. Februar) insgesamt 5.800 WEA in Zentraleuropa mit einer Gesamtleistung von 11 Gigawatt. Eine Gefahr für die WEA besteht nicht. Die betroffenen WEA befinden sich weiterhin in Betrieb und produzieren saubere erneuerbare Energie. Sie laufen bis zu einer Lösung des Problems im Automatikmodus und können sich grundsätzlich autark und selbstständig regulieren.

golem.de

Aktuelles Detail

Ukraine-Krieg: Satelliteninternet KA-SAT ausgefallen - Golem.de

HOME

TICKER

VIDEOS

VORGELESEN

FORUM

KARRIEREWELT

JOBS

IT-FACHTRAININGS

COACHINGS

SPRACHKURSE

GEHALTSHECK

GOLEM-PC

PRODUKTVERGLEICH

TOP-ANGEBOTE

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](#).

In Pocket speichern

merken

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

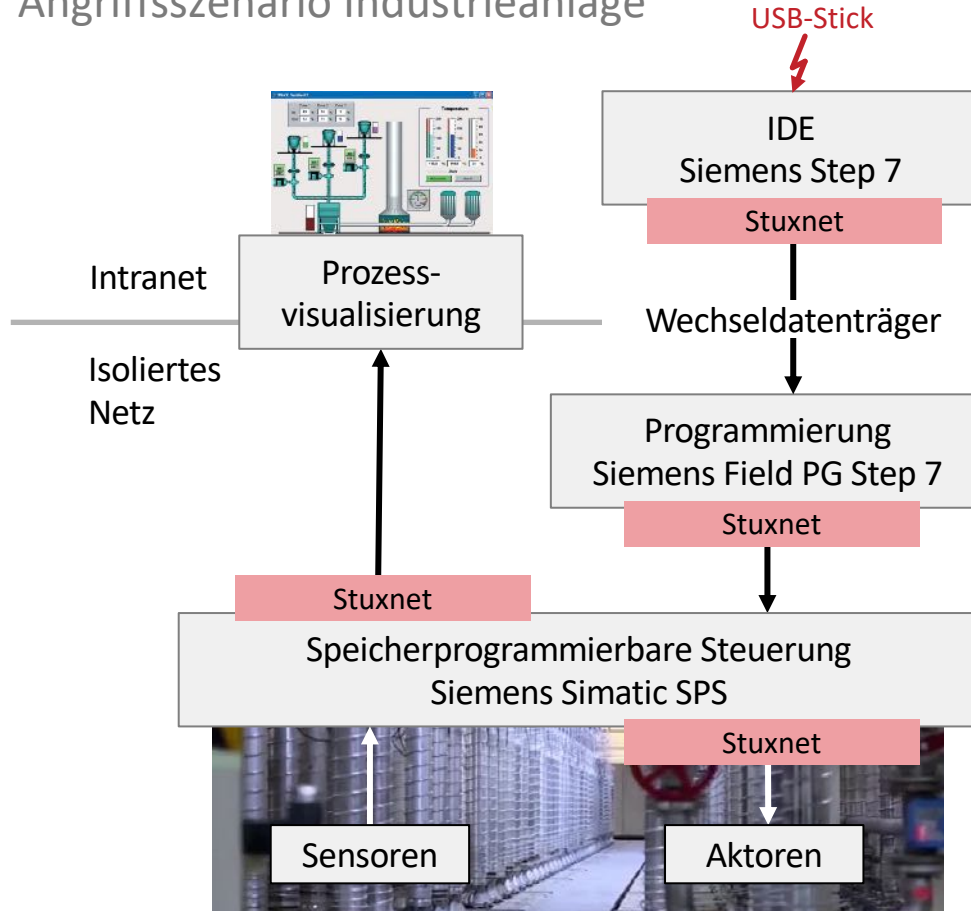


(Bild: Viasat)

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.

Stuxnet: Angriffsszenario Industrieanlage



Treiber mit gestohlenen Zertifikaten
(Realtek, JMicon) 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

Malware

Angreifer kann alle drei
Schutzziele verletzen:

- Vertraulichkeit
- Integrität
- Verfügbarkeit



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



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

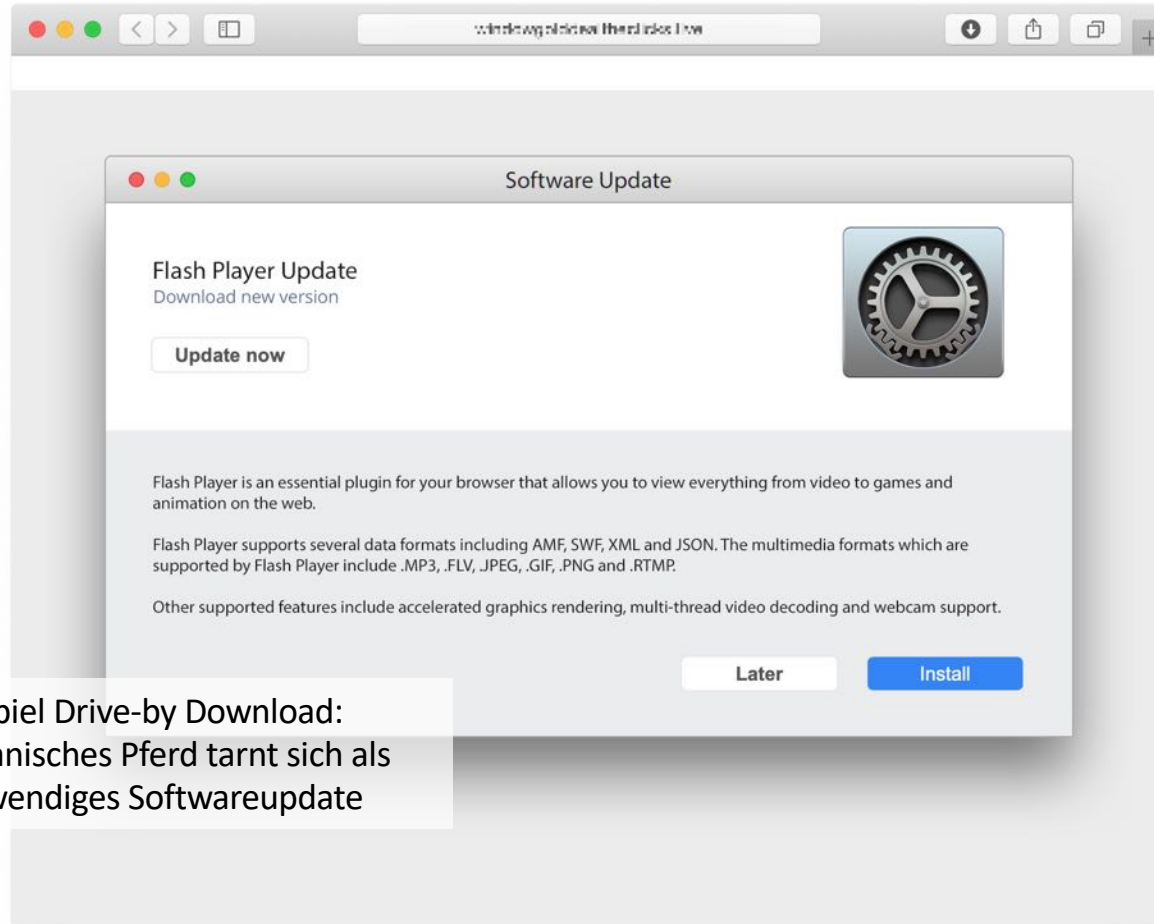
1. Reconnaissance: Auskundschaften des Ziels
2. Weaponization: Vorbereitung zur Übertragung der Malware

3. Delivery: Übertragung der Malware (E-Mail, USB-Speicher)
4. Exploitation: Initialen Zugang zum Opfer herstellen, Ausnutzen der Schwachstelle beim Opfer

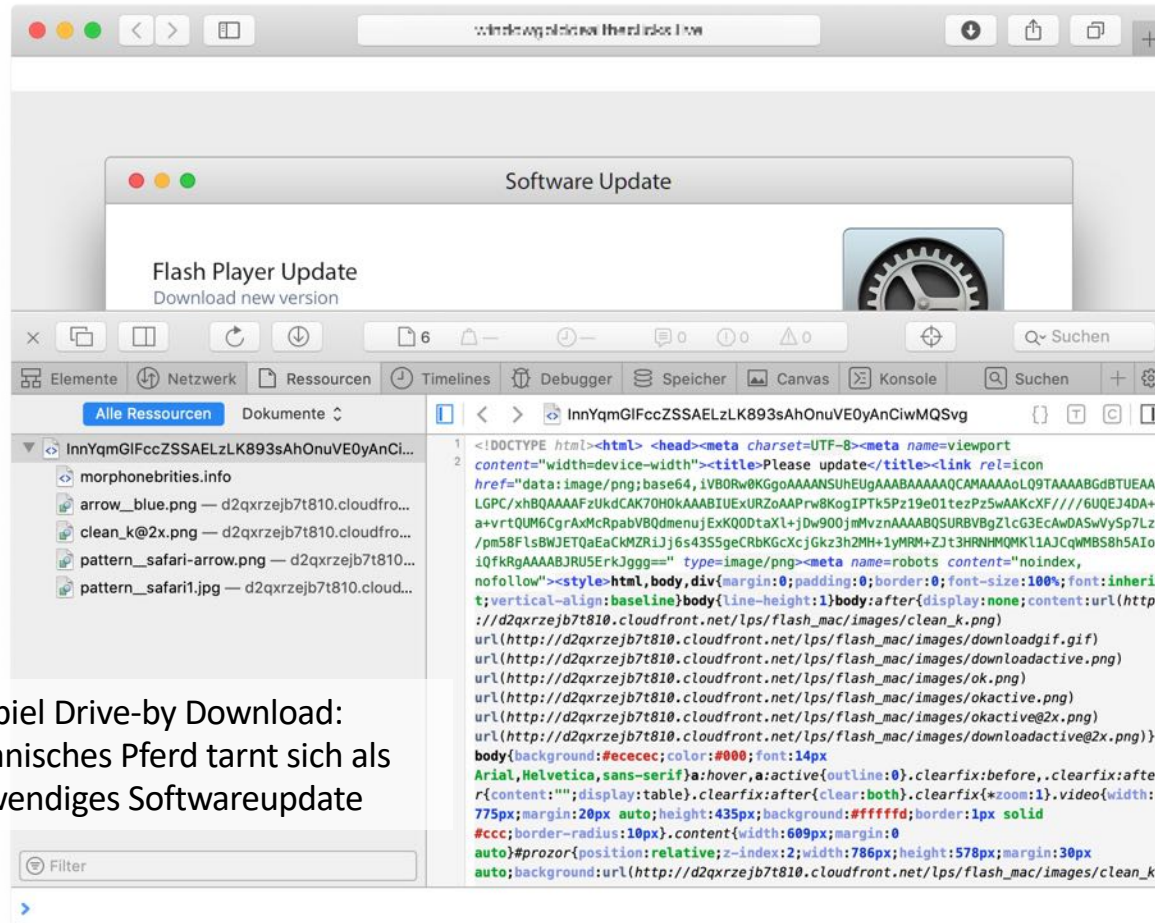
5. Installation: permanenten Zugang zum Opfersystem schaffen (z.B. Backdoors)
6. Command and Control: Fernsteuern des Opfersystems
7. Actions on Objective: (Massenhafte) Angriffe im Netz ausführen (z.B. mittels Botnetz)

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	Reconnaissance	10	Anzahl der gelisteten Angriffstechniken
	2. Weaponization: Vorbereitung	Resource Development	7	
2. Angriff (über das Netz)	3. Delivery: Übertragung Malware	Initial Access	9	
		Execution	12	
		Persistence	19	
		Privilege Escalation	13	
3. Erweiterung der Rechte	4. Exploitation: Initialer Zugang	Defense Evasion	39	
		Credential Access	15	
		Discovery	27	
		Lateral Movement	9	
		Collection	17	
		Command and Control	16	
		Exfiltration	9	
4. Spuren verwischen	5. Installation: Backdoors	Impact	13	
	6. Command and Control: Fernsteuern			
	7. Actions on Objective: Angriffe im Netz			

4. Spuren verwischen

Cyber Kill Chain



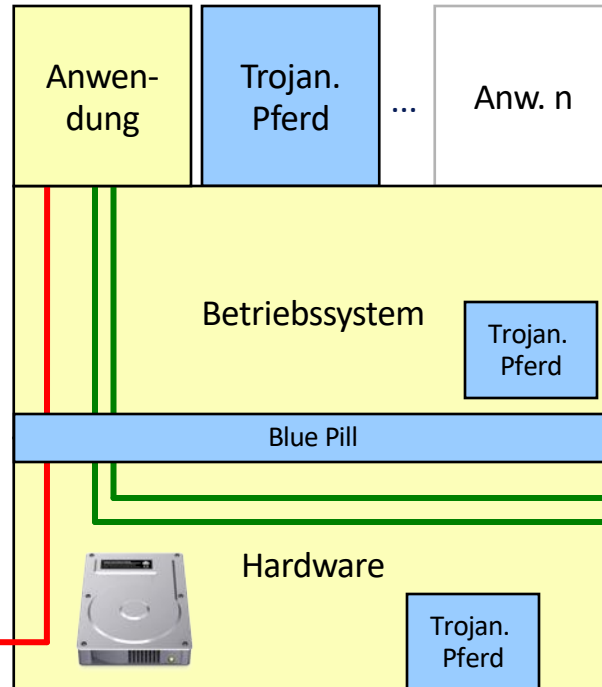
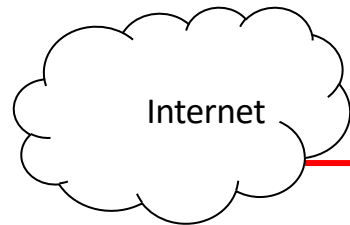
MITRE ATT&CK Matrix

MITRE | ATT&CK®

Angriffspunkte für Malware

Angreifer kann alle drei
Schutzziele verletzen:

- Vertraulichkeit
- Integrität
- Verfügbarkeit



Angriffspunkte für Malware



bsi.bund.de

MENÜ

BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten

Ort Bonn
Datum 15.03.2022

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) [↓ warnt](#) nach §7 BSI-Gesetz vor dem Einsatz von Virenschutzsoftware des russischen Herstellers Kaspersky. Das BSI empfiehlt, Anwendungen aus dem Portfolio von Virenschutzsoftware des Unternehmens Kaspersky durch alternative Produkte zu ersetzen.

Antivirensoftware, einschließlich der damit verbundenen echtzeitfähigen Clouddienste, verfügt über weitreichende Systemberechtigungen und muss systembedingt (zumindest für Aktualisierungen) eine dauerhafte, verschlüsselte und nicht prüfbare Verbindung zu Servern des Herstellers unterhalten. Daher ist Vertrauen in die Zuverlässigkeit und den Eigenschutz eines Herstellers sowie seiner authentischen Handlungsfähigkeit entscheidend für den sicheren Einsatz solcher Systeme. Wenn Zweifel an der Zuverlässigkeit des Herstellers bestehen, birgt Virenschutzsoftware ein besonderes Risiko für eine zu schützende IT-Infrastruktur.

Das Vorgehen militärischer und/oder nachrichtendienstlicher Kräfte in Russland sowie die im Zuge des aktuellen kriegerischen Konflikts von russischer Seite ausgesprochenen Drohungen gegen die EU, die NATO und die Bundesrepublik Deutschland sind mit einem erheblichen Risiko eines erfolgreichen IT-Angriffs verbunden. Ein russischer IT-Hersteller kann selbst offensive Operationen durchführen, gegen seinen Willen gezwungen werden, Zielsysteme anzugreifen, oder selbst als Opfer einer Cyber-Operation ohne seine Kenntnis ausspioniert oder als Werkzeug für Angriffe gegen seine eigenen Kunden missbraucht werden.

Digitale Souveränität als Schutz

- Aufgabe des Staats, geeignete Rahmenbedingungen zu schaffen

Anreize: Beschäftigungs- und Strukturpolitik für Hitech in Europa

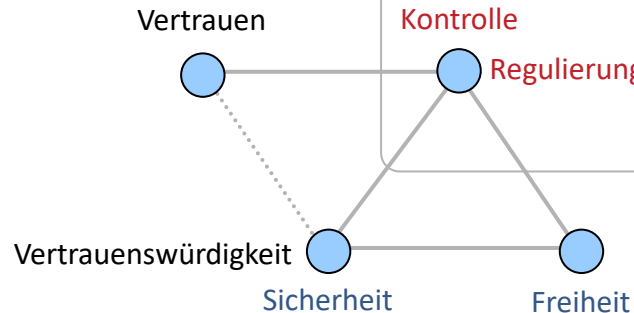
- Forschungs- und Rahmenprogramme
- Zertifizierungen und Gütesiegel von geeigneten Produkten

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

Souveränität

...

Digitale Souveränität

Technologische

Informationelle

Gefahren bei mangelnder Digitaler Souveränität (Auswahl):

Wirtschaft
Verwaltung
Bürger

+++
+++
+

+
+
+++

Industriespionage
Cyber Warfare
Verlust des informationellen Selbstbestimmungsrechts

Vertrauen

Kontrolle

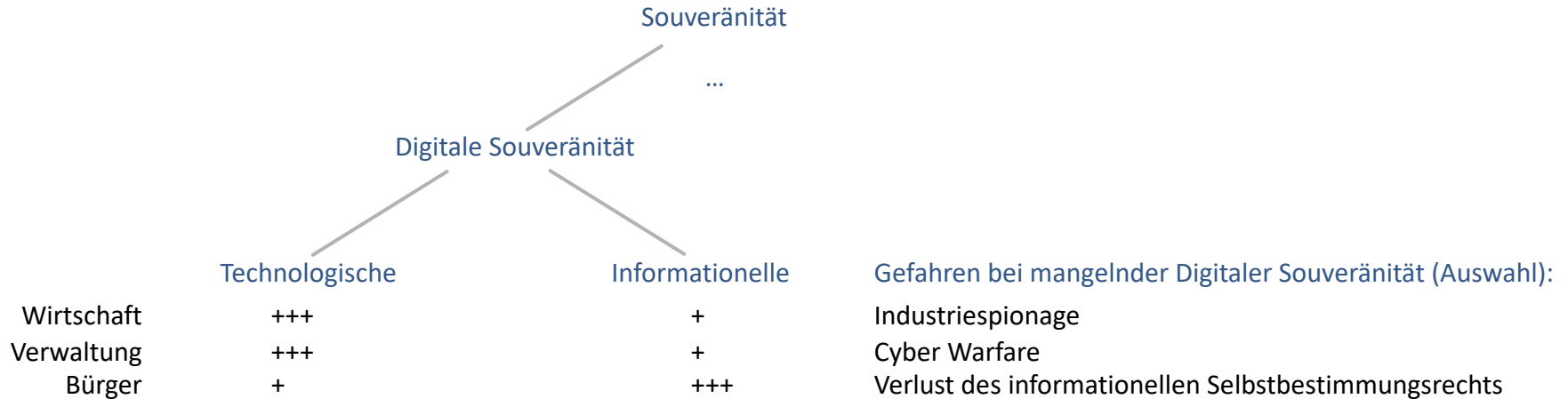
Regulierung

Vertrauenswürdigkeit

Sicherheit

Freiheit

Digitale Souveränität als Schutz



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



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>