

The State of Cyber





Cyber ist die fünfte Dimension

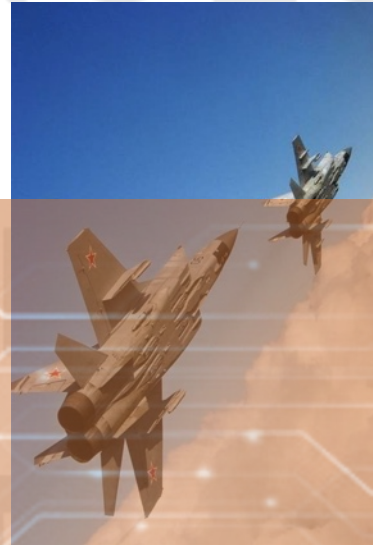
LAND



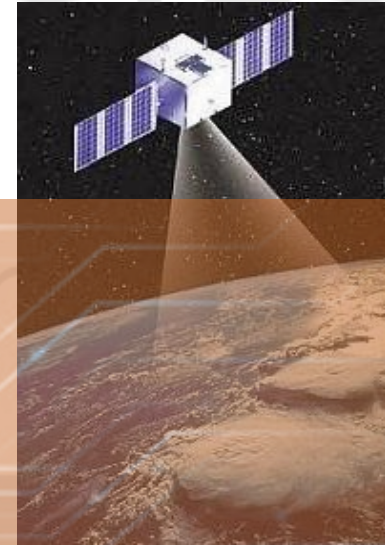
SEE



LUFT



WELTALL

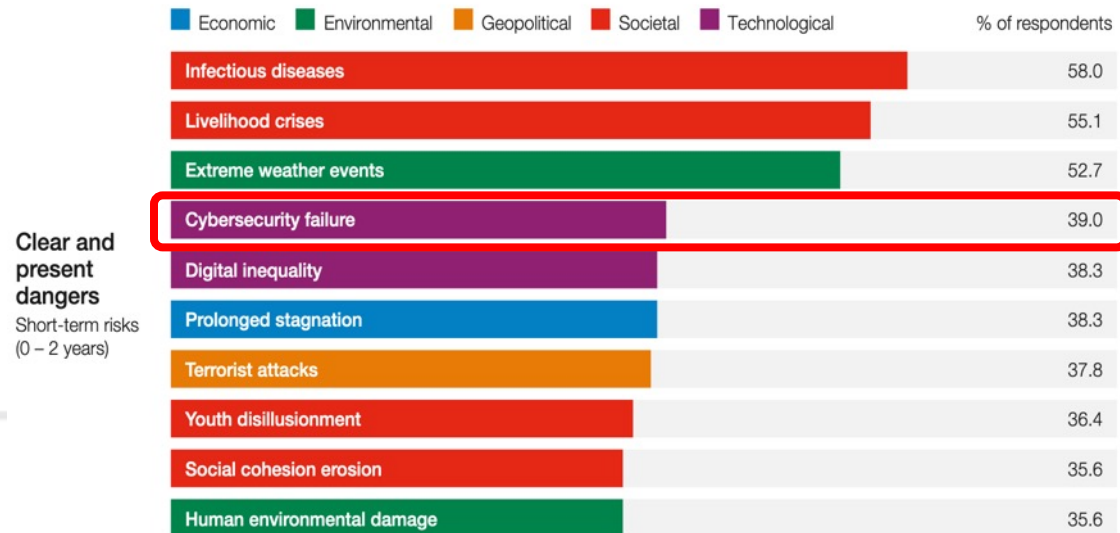


CYBER

Cyber Security Risiken sind globale Spitzenreiter

FIGURE I
Global Risks Horizon

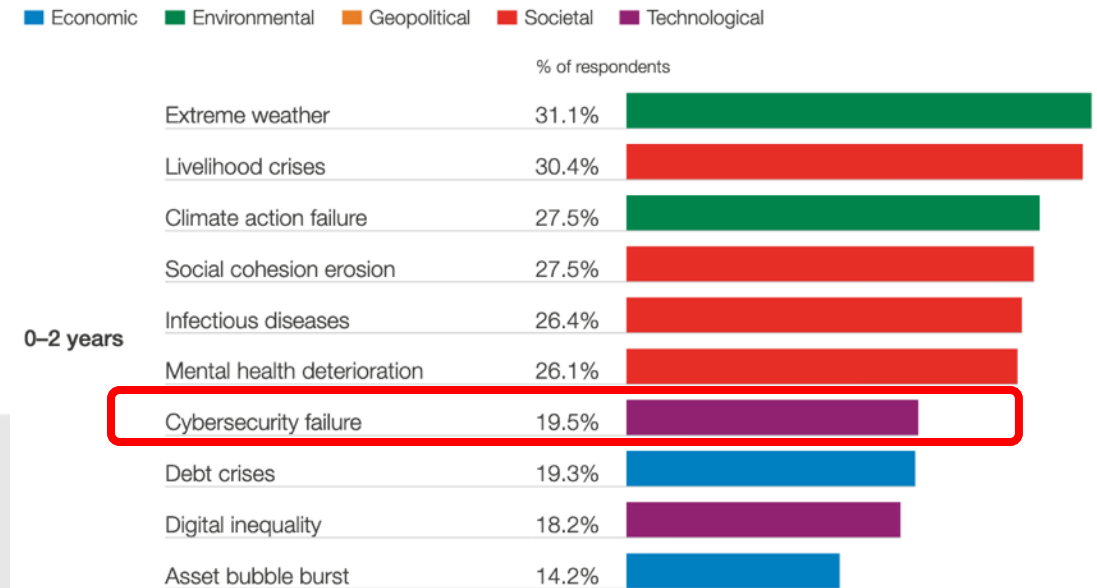
When do respondents forecast risks will become a critical threat to the world?



Quelle: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

FIGURE II
Global Risks Horizon

When will risks become a critical threat to the world?



Quelle: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Die Schweiz ist ein Synonym für Kreativität und Innovationskraft...
 ... aber die Cyber-Sicherheit der Schweiz hinkt im globalen Vergleich massiv hinterher

Country/Economy	Score (0–100)	Rank
Switzerland	66.08	1
Sweden	62.47	2

Global Innovation Index 2021 rankings

GII rank	Economy	Score	Income group rank	Region rank
1	Switzerland	65.5	1	1
2	Sweden	63.1	2	2
3	United States of America	61.3	3	1
4	United Kingdom	59.8	4	3
5	Republic of Korea	59.3	5	1
6	Netherlands	58.6	6	4

GII rank	Economy	Score	Income group rank	Region rank
1	Switzerland	64.6	1	1
2	United States	61.8	2	1
3	Sweden	61.6	3	2
4	United Kingdom	59.7	4	3
5	Netherlands	58.0	5	4
6	Republic of Korea	57.8	6	1
7	Singapore	57.3	7	2
8	Germany	57.2	8	5
9	Finland	56.9	9	6
10	Denmark	55.9	10	7



Country Name	Score	Rank	Country Name	Score	Rank
United States of America**	100	1	Indonesia	94.88	24
United Kingdom	99.54	2	Viet Nam	94.59	25
Saudi Arabia	99.54	2	Sweden	94.55	26
Estonia	99.48	3	Qatar	94.5	27
Korea (Rep. of)	98.52	4	Greece	93.98	28
Singapore	98.52	4	Austria	93.89	29
Spain	98.52	4	Poland	93.86	30
Russian Federation	98.06	5	Kazakhstan	93.15	31
United Arab Emirates	98.06	5	Denmark	92.6	32
Malaysia	98.06	5	China	92.53	33
Lithuania	97.93	6	Croatia	92.53	33
Japan	97.82	7	Slovakia	92.36	34
Canada**	97.67	8	Hungary	91.28	35
France	97.6	9	Israel**	90.93	36
India	97.5	10	Tanzania	90.58	37
Turkey	97.49	11	North Macedonia	89.92	38
Australia	97.47	12	Serbia	89.8	39
Luxembourg	97.41	13	Azerbaijan	89.31	40
Germany	97.41	13	Cyprus	88.82	41
Portugal	97.32	14	Switzerland**	86.97	42
			Ghana	86.69	43

The Global Innovation Index 2020 / 2021 / 2022

- https://www.wipo.int/global_innovation_index/en/2020/
- https://www.wipo.int/global_innovation_index/en/2021/
- https://www.wipo.int/global_innovation_index/en/2022/

Global Cybersecurity Index 2020

<https://www.itu.int/en/myitu/Publications/2021/06/28/13/22/Global-Cybersecurity-Index-2020>



Die drei Schutz-Ziele der Cyber-Sicherheit

C
Confidentiality

I
Integrity

A
Availability



Braches im 2023

DDoS-Attacke auf Parlaments-Website

Von **Reto Vogt**, 8. Juni 2023 um 10:56

SECURITY BUND PARLAMENT CYBERANGRIFF DDOS



Die Webseite der eidgenössischen Räte ist angegriffen worden. Seit Mittwoch ist sie zeitweise nicht abrufbar.

<https://www.inside-it.ch/ddos-attacke-auf-parlaments-website-20230608>

Availability

Hacker klauen Mitarbeiterdaten der Kapo Bern

Von **Keystone-sda / hjm**, 21. August 2023 um 11:06

SECURITY BREACH



<https://www.inside-it.ch/hacker-klauen-mitarbeiterdaten-der-kapo-bern-20230821>

Confidentiality

NEWS

Nach Cyberangriff auf Xplain

Update: Sensible Daten von Bundesverwaltung und Fedpol landen im Darknet

Mo 19.06.2023 - 12:13 Uhr

von **Yannick Züllig** und **Yannick Chavanne** und **René Jaun** und **Maximilian Schenner** und lha, cka, yzu, rja

Cyberkriminelle haben den IT-Dienstleister Xplain angegriffen. Unter den Opfern sind auch die SBB, der Kanton Aargau und die Landespolizei des Fürstentums Liechtenstein. Auch sensible Daten der Bundesverwaltung und des Fedpol sind betroffen, wie Analysen nun zeigen.

<https://www.netzwoche.ch/news/2023-06-05/ransomware-angriff-auf-it-dienstleister-trifft-auch-bundesstellen>

Confidentiality

Integrity



Breaches der (20)20er

'Shocking' hack of psychotherapy records in Finland affects thousands

Distressed patients flood support services after hack of private firm Vastaamo



Vastaamo patients reported receiving emails with demands for €200 to prevent the documents' publication. Photograph: Kimmo Brandt/EPA

<https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland>

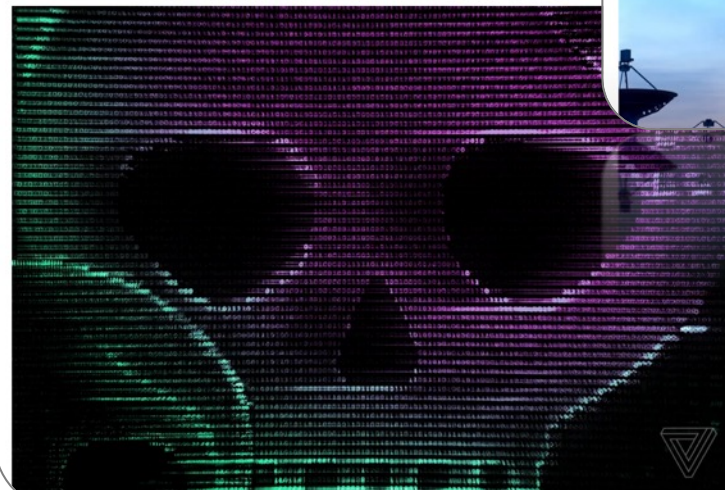
POLICY | TECH | CYBERSECURITY

White House now says 100 companies hit by SolarWinds hack, but more may be affected

Plus nine federal agencies

By Jon Porter | @JonPorty | Feb 18, 2021, 4:40am EST

f t SHARE



See by Alex Costas / The Verge

<https://www.theverge.com/2021/2/18/22288961/solarwinds-hack-100-companies-9-federal-agencies>

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.



<https://www.wired.com/story/viasat-internet-hack-ukraine-russia/>

Subscribe to approved tech

Email (required)

By submitting your

Terms and Privacy any time. This site and the Google Pr Service apply.

SU

Treiber für die aktuelle Cyber-Situation: Schwachstellen / Bugs werden zum Einfallstor

Menschen machen Fehler

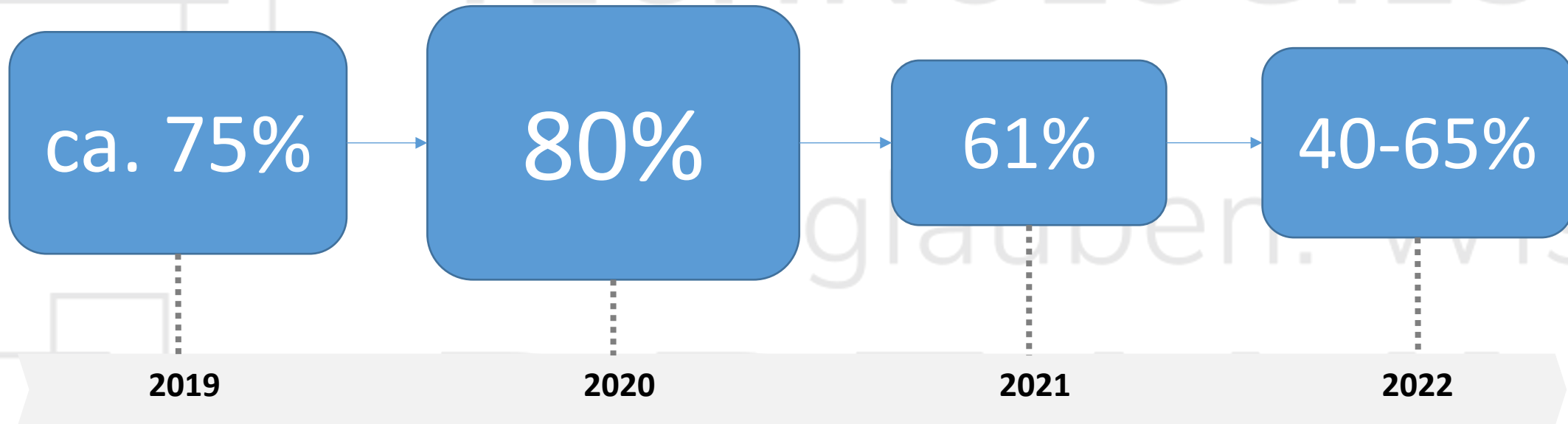
Menschen bauen Software,
Prozesse und Produkte

Software, Prozesse und Produkte
weisen Schwachstellen auf

Schwachstellen lassen sich
ausnutzen



Treiber für die aktuelle Cyber-Situation:
Schwache, gestohlene oder geleakte und wiederverwendete Passwörter
tragen zu Grossteil aller Hacks bei



<https://www.verizon.com/business/resources/reports/2019-data-breach-investigations-report.pdf>
<https://www.verizon.com/business/resources/reports/2020-data-breach-investigations-report.pdf>
<https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf>
<https://www.verizon.com/business/resources/T744/reports/dbir/2022-data-breach-investigations-report-dbir.pdf>

Treiber für die aktuelle Cyber-Situation:
(Spear-) Phishing / Malspam Attacken und ungenügend befähigte
Mitarbeiter

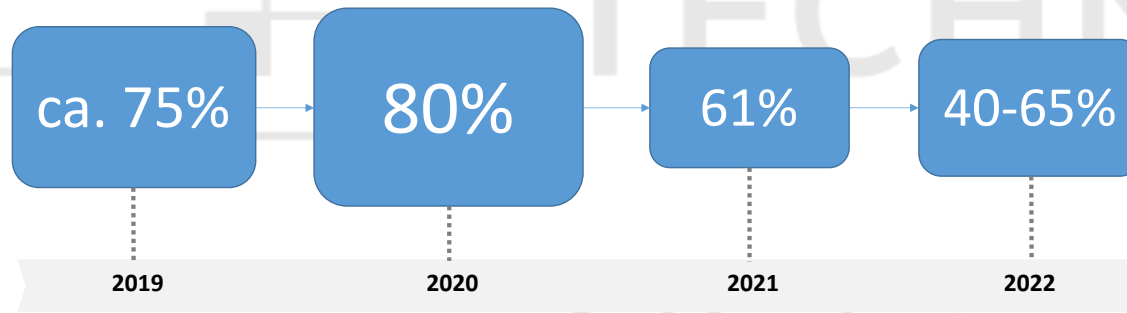


<https://www.avepoint.com/blog/de/protect-de/so-schuetzen-sie-sich-vor-phishing-ransomware-angriffen>



Treiber für die aktuelle Cyber-Situation:

Cyber-Security ist ein Prozess und Hygienefaktor, wird aber nicht so verstanden.



Wer sind die Angreifer?

HACKTIVIST

My Motives:
Disrupting the status quo, seeking virtual mischief and mayhem to make a point to the government and large corporations, freeing terrorists, vigilante-ish, "doxing," cyber protest, anarchy, etc.

My Boss:
Myself and what I believe in, totally decentralized

My Conrades:
Achan, Anonymous, LulzSec, AnonSec

My Favorite Beverage:
Energy drinks

My Tools:
Web application attacks using freely available tools

My Methods:
I use freely available exploit kiddie tools to launch DDoS attacks or web application attacks to try to hijack a legitimate website or steal data

My Street Cred:
I was responsible for 55% of all data theft in 2011, but in 2012 my fellow hackers got a bigger piece of the pie

My Claims to Fame:
Project Chronology, Operation Payback, Arab Spring activities, Operation Hecate, Operation Durbanus, Operation Sony, Operation Megaupload, just to name a few

My Hero:
Guy Fawkes, the face of Anonymous



CYBER CRIMINAL

My Motives:
Identity theft, credit card information, extortion (via ransomware or DDoS), click-jacking, pirating software, monetizing computer data in any way possible

My Boss:
My financier, a traditional criminal organization that has decided to recruit tech savvy kids

My Conrades:
Other cyber criminals in the underground market, where we swap hacking kits

My Favorite Beverage:
Vodka

My Tools:
Exploit kits sold on underground internet (or darknet) markets and forums. I also buy and sell prepackaged botnets and botnet modules

My Methods:
I prefer web-based drive-by downloads, phishing, click-jacking, installing ransomware and malware, and can even use my victims to attack others

My Street Cred:
I took \$20.7 billion from consumers last year

My Claims to Fame:
I recently completed a global bank heist, stealing about \$45 million from ATM

My Hero:
Albert Gonzalez, who stole over 170 million credit and debit card numbers in two years



NATION STATE

My Motives:
Obtaining intelligence from my foes, cyber espionage, stealing secrets from my adversaries, disrupting or damaging an enemy's military infrastructure, propaganda, distracting an enemy during a real attack

My Boss:
My government

My Conrades:
I only trust a few people within my government organization

My Favorite Beverage:
A martini - shaken, not stirred

My Tools:
Customized, advanced malware and toolkits designed for a very specific goal (i.e. Stuxnet, Flame, Gauss)

My Methods:
Advanced persistent threats, zero day exploits, rootkit technology, strong encryption, and many evasion techniques - I use malware customized for non-traditional computing systems

My Street Cred:
In the Aurora attacks of 2009, I introduced the watering hole attack and have targeted over 30 large companies including Google

My Claims to Fame:
Google Aurora attacks, New York Times hack, and other classified security breaches

My Hero:
ng10r1ll4 (real name: Jack Wang)



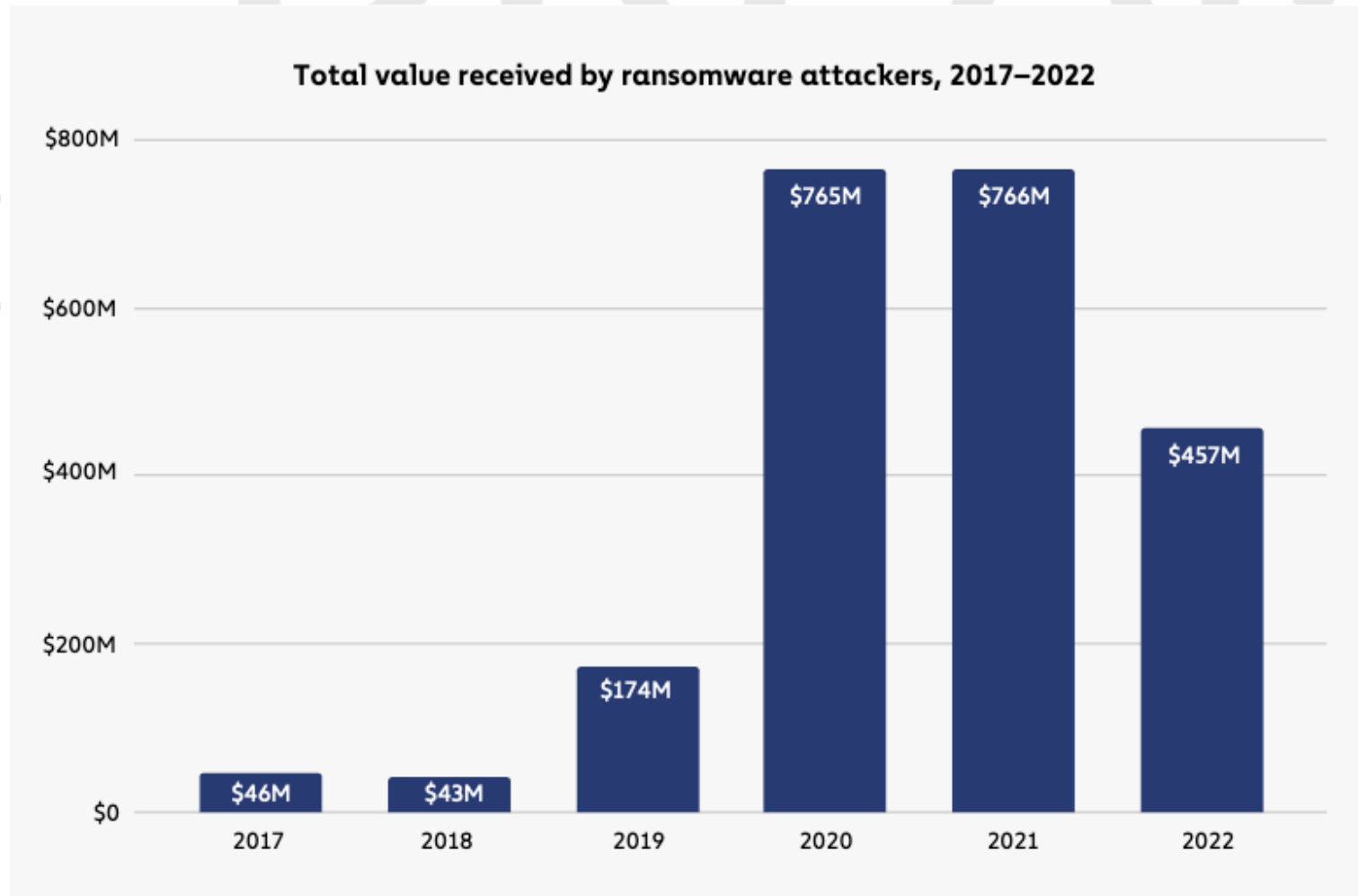

Wer sind die Angreifer in der Cyber-Dimension?



Motivation + Fähigkeiten + **Opportunität (Angriffsfläche)** → **Risiko**.
Die Übergänge sind fließend, Attribution ist sehr schwierig



Die Motivation von Cyberkriminellen



https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf



Meet Conti: Einblick in eine professionelle Cybergang



Programmers



Testers



Administrators



Reversers



Penetrationstester/Hacker

Schreibt bösartigen Code und integriert unterschiedliche Technologien

Testet Conti-Malware gegen Sicherheitstools und verschleiert diese (alle 4h!)

Auf- und Abbau von Servern und Angriffsinfrastrukturen (botnets)

Zerlegen Code und identifizieren Schwachstellen in gängiger Software, Hardware, und Cloud Services

Kämpfen an vorderster Front gegen Sicherheitsteams von Unternehmen, um Daten zu stehlen und Ransomware einzuschleusen.

Die meisten Antivirus Lösungen wirkungslos!



Wie gehen Cyber-Akteure vor?

Ein Schritt nach dem anderen...

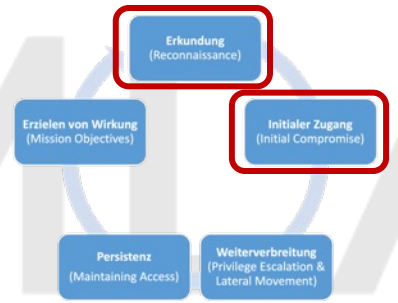
Verschlüsseln von Daten
Diebstahl von Daten
Manipulation von Daten
Beeinflussung von
Kontrollprozessen
...



**Fernsteuerung /
Command and
Control (C2)**



Erkundung? Opportunismus oder Outsourcing



Продам USA VPN revenue 1kkk\$ Подписаться 1

Автор: i4R320bKZzQ1z13, Во вторник в 17:01 в [Доступы] - FTP, shell'ы, руты, sql-inj, БД, дедики

[Создать тему](#) [Ответить в тему](#)

i4R320bKZzQ1z13 Опубликовано: Во вторник в 17:01 Жалоба

гигабайт

Платная регистрация

105 публикаций

Регистрация 18.04.2020 (ID: ...)

Деятельность вирусология / malware

является глобальной компанией по технологиям и услугам для клиентов, специализирующейся на проектировании, внедрении
Employees: 50k+
Revenue: \$1 Billion
USA
Price: 7000\$
Тип доступа: VPN (global-prote

ведущий поставщик решений для предприятий малого и среднего
Employees: 2k+
Revenue: 700kk\$
USA
Price: 5000\$
Тип доступа: VPN (global-prote

Работаем через гарант, либо ж первый контакт в пм.

I sell VPN accounts of USA companies, revenue is 1kkk\$

Post

Company is a global organization that provides technologies and services for customers and specializes in design and implementation
Employees: more than 50 000
Revenue: \$1 billion
USA
Price: 7 000\$
Access type: VPN
Company is a leading provider of web presence solutions for small and mid-sized businesses worldwide.
Employees: 2k+
Revenue: 700kk\$
USA
Price: 5 000\$
Access type: VPN
We work with guarantees; otherwise, you pay a deposit and I will provide you with access information in advance.
First contact in private messages.

<https://securelist.com/initial-access-data-price-on-the-dark-web/106740/>

// EXPLORE THE PLATFORM

Beyond the Web

Websites are just one part of the Internet. Use Shodan to discover everything from power plants, mobile phones, refrigerators and Minecraft servers.

Monitor Network Exposure

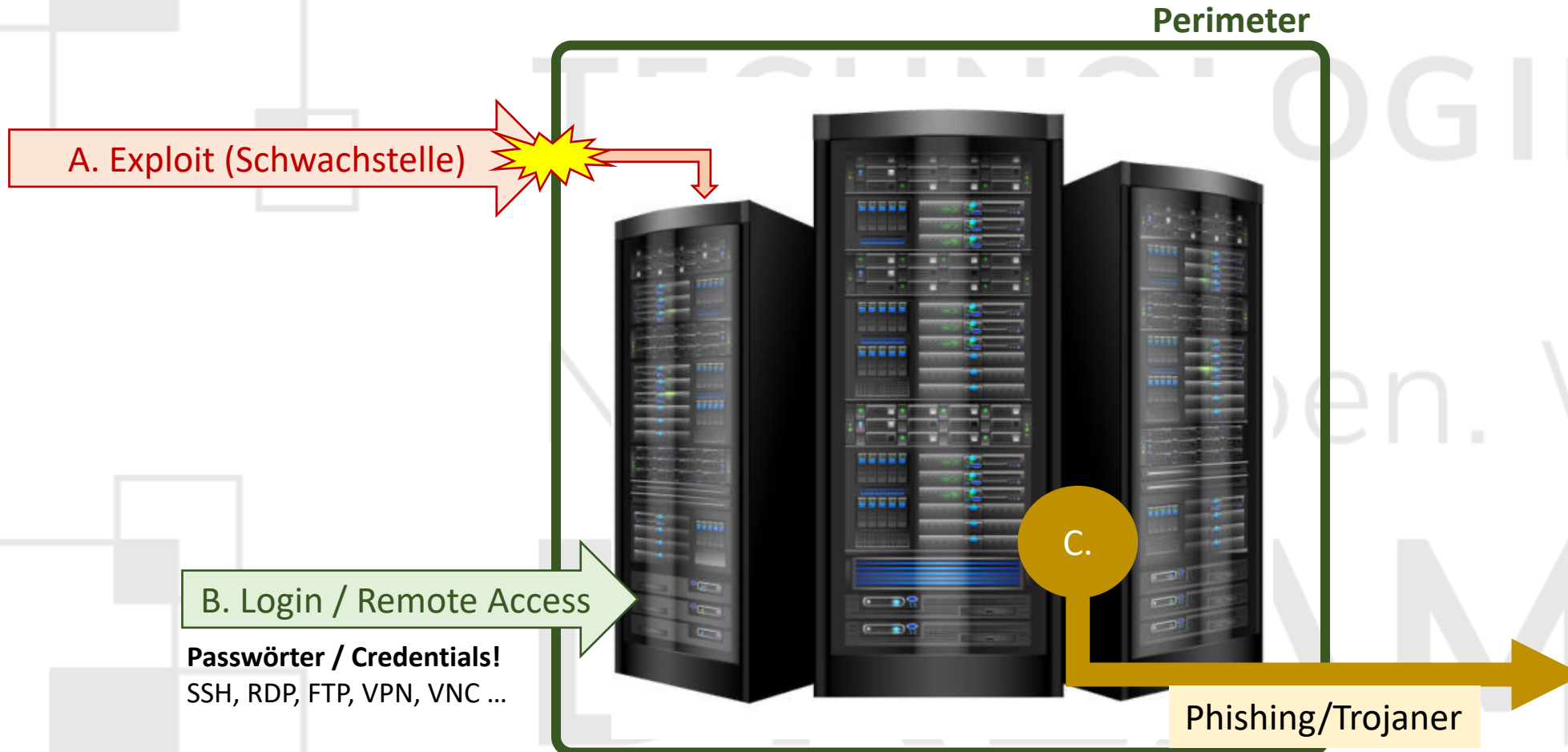
Keep track of all your devices that are directly accessible from the Internet. Shodan provides a comprehensive view of all exposed services to help you stay secure.

Internet Intelligence

Learn more about who is using various products and how they're changing over time. Shodan gives you a data-driven view of the technology that powers the Internet.

Wie gehen Cyber-Akteure vor?

Drei Wege zum Initial Compromise





Kritische Fortinet-Schwachstelle: 533 direkt angreifbare IT-Systeme in der Schweiz identifiziert



SWITZERLAND OVERVIEW

EXPLORE RESULTS

vulnerability.cve = CVE-2022-40684 x AND vulnerability.status = Confirmed x Enter the conditional operator for the next filter

Showing 1 to 10 of 533 results.

Location	Vulnerabilities
Zurich, Switzerland	1 Confirmed, 9 Potential
Zug, Switzerland	1 Confirmed, 1 Potential
Zurich, Switzerland	1 Confirmed

Name	Quantity
Zurich	280
Vaud	48
Bern	44
Valais	30
Sankt Gallen	19

Name	Quantity
[Redacted]	240
[Redacted]	71
[Redacted]	26
[Redacted]	14
[Redacted]	9

17.10. 2022 10:11 Von [Dreamlab Techno...](#)

Kritische Fortinet-Schwachstelle: 533 direkt angreifbare IT-Systeme in der Schweiz identifiziert

Bild Rechte: Dreamlab Technologies AG

(Bern)(PPS) **Die seit zehn Tagen bekannte kritische Fortinet-Schwachstelle CVE-2022-40684 erlaubt Hackern, sich mit Administratorenrechten in verwundbare Systeme einzuloggen. Aktuellste Messungen legen offen, dass die IT-Infrastrukturen von 533 Schweizer Unternehmen diesbezüglich weiterhin ungeschützt sind. Unter den angreifbaren Firmen befinden sich mehrere Telekommunikationsanbieter, ISPs und Elektrizitätswerke. Schnelles Handeln ist dringend notwendig.**

Fortinet warnte am 6. und am 10. Oktober 2022 davor, dass die dokumentierte Schwachstelle "Authentication Bypass" ihre drei Produkte FortiOS, FortiProxy und FortiSwitchManager betrifft. Die Schwachstelle (CVE-2022-40684) ist im Fortinet Vulnerability Scoring System (VSS) als kritisch eingestuft und ermöglicht Angreifenden, sich mit Administratorenrechten einzuloggen. Am 10. Oktober 2022 wurde von Horizon3-Forschern gezeigt, wie die Schwachstelle ausgenutzt werden kann.

17.10.2022

→ <https://www.presseportal-schweiz.ch/pressemeldungen/kritische-fortinet-schwachstelle-533-direkt-angreifbare-it-systeme-der-schweiz>
 → <https://www.netzwoche.ch/news/2022-10-11/fortinet-bug-ermoeglicht-unerlaubten-admin-zugriff>



Wo eine Schwachstelle ist, ist der Exploit meist nicht weit



CVE-2022-40684 exploit

All News Images Videos Books More Tools

About 53'700 results (0.50 seconds)

What is the Impact of CVE-2022-40684 Vulnerability? The CVE-2022-40684 vulnerability **allows adversaries to bypass authentication and login into the vulnerable systems as an administrator in FortiOS / FortiProxy / FortiSwitchManager products.** 18 Oct 2022

<https://www.picussecurity.com/resource/blog/cve-2022-40684-fortinet-authentication-bypass-vulnerability>

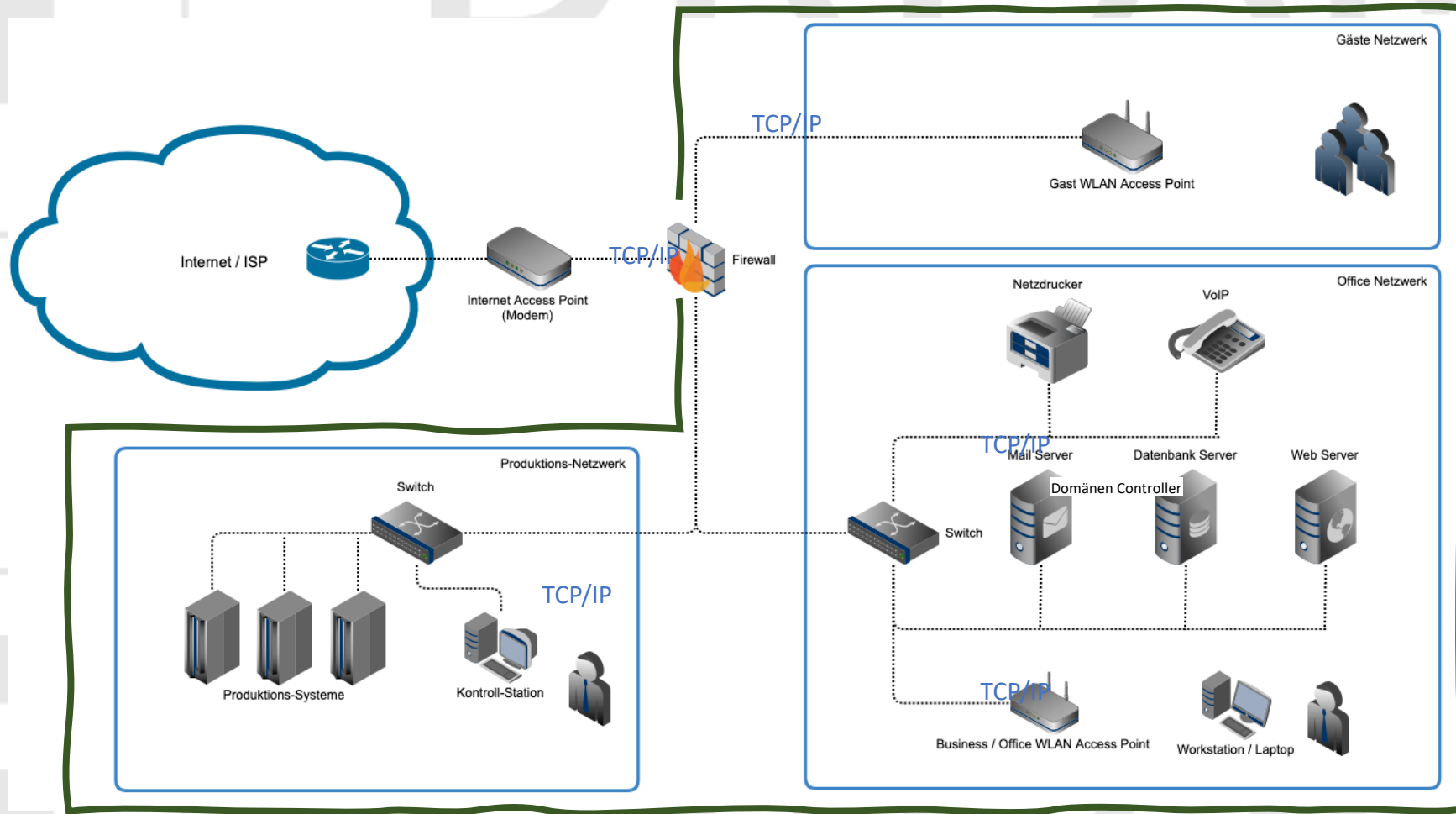
<https://github.com/Chocapikk/CVE-2022-40684>
Chocapikk/CVE-2022-40684: Fortinet Critical ... - GitHub
7 days ago — This POC abuses the authentication bypass **vulnerability** to set an SSH key for the specified user. Usage. root@kali:~# python **exploit.py** -h ...

<https://github.com/horizon3ai/CVE-2022-40684>
horizon3ai/CVE-2022-40684 - GitHub
14 Oct 2022 — A proof of concept **exploit** for **CVE-2022-40684** affecting Fortinet FortiOS, FortiProxy, and FortiSwitchManager - GitHub ...

<https://securityaffairs.co/fortinet-cve-2022-40684-poc>
Experts released PoC exploit code for critical bug CVE-2022 ...
14 Oct 2022 — Experts released the PoC **exploit** code for the authentication bypass flaw **CVE-2022-40684** in FortiGate firewalls and FortiProxy web proxies.

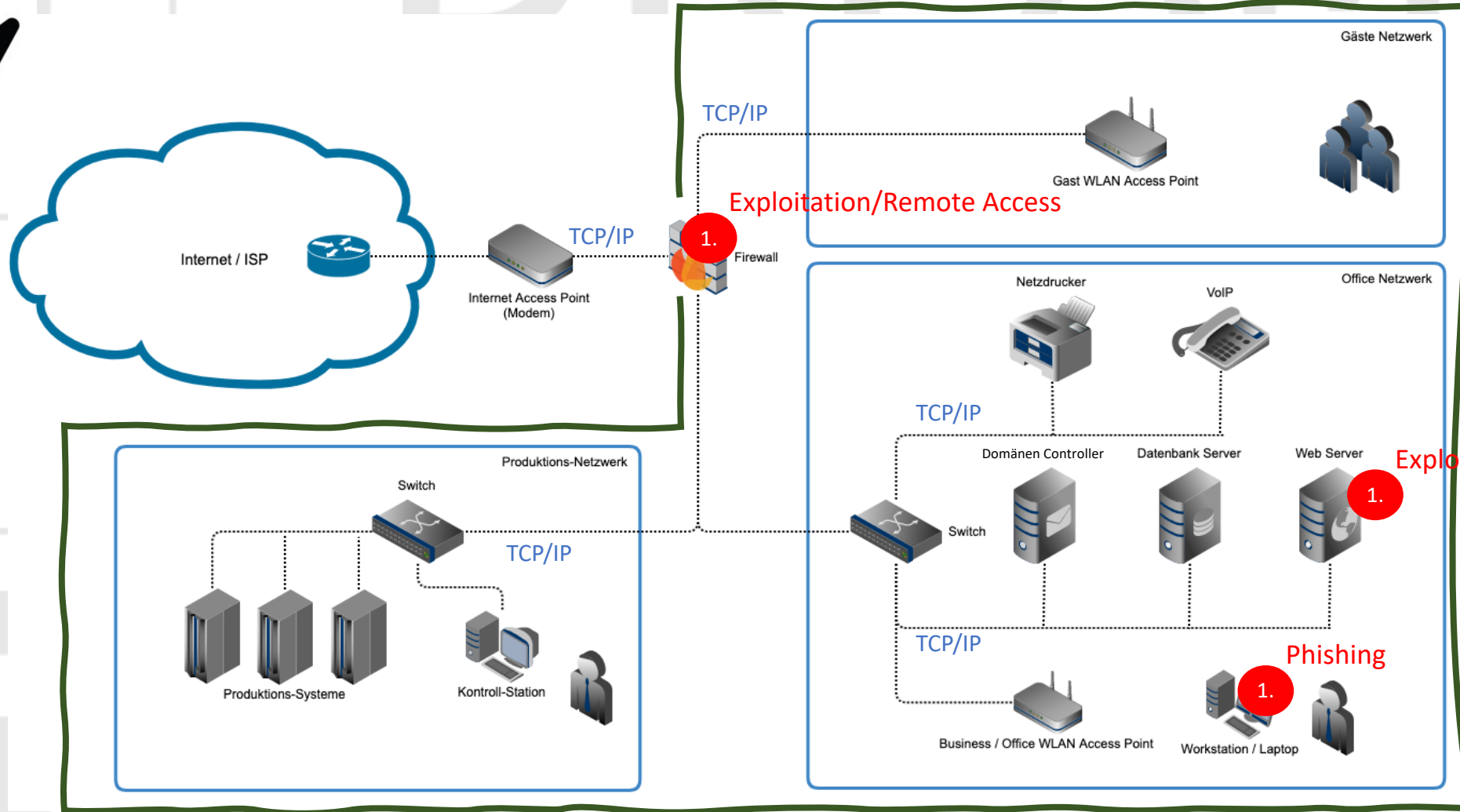
Wie gehen Cyber-Akteure vor?

Vereinfachtes, typisches Unternehmensnetzwerk



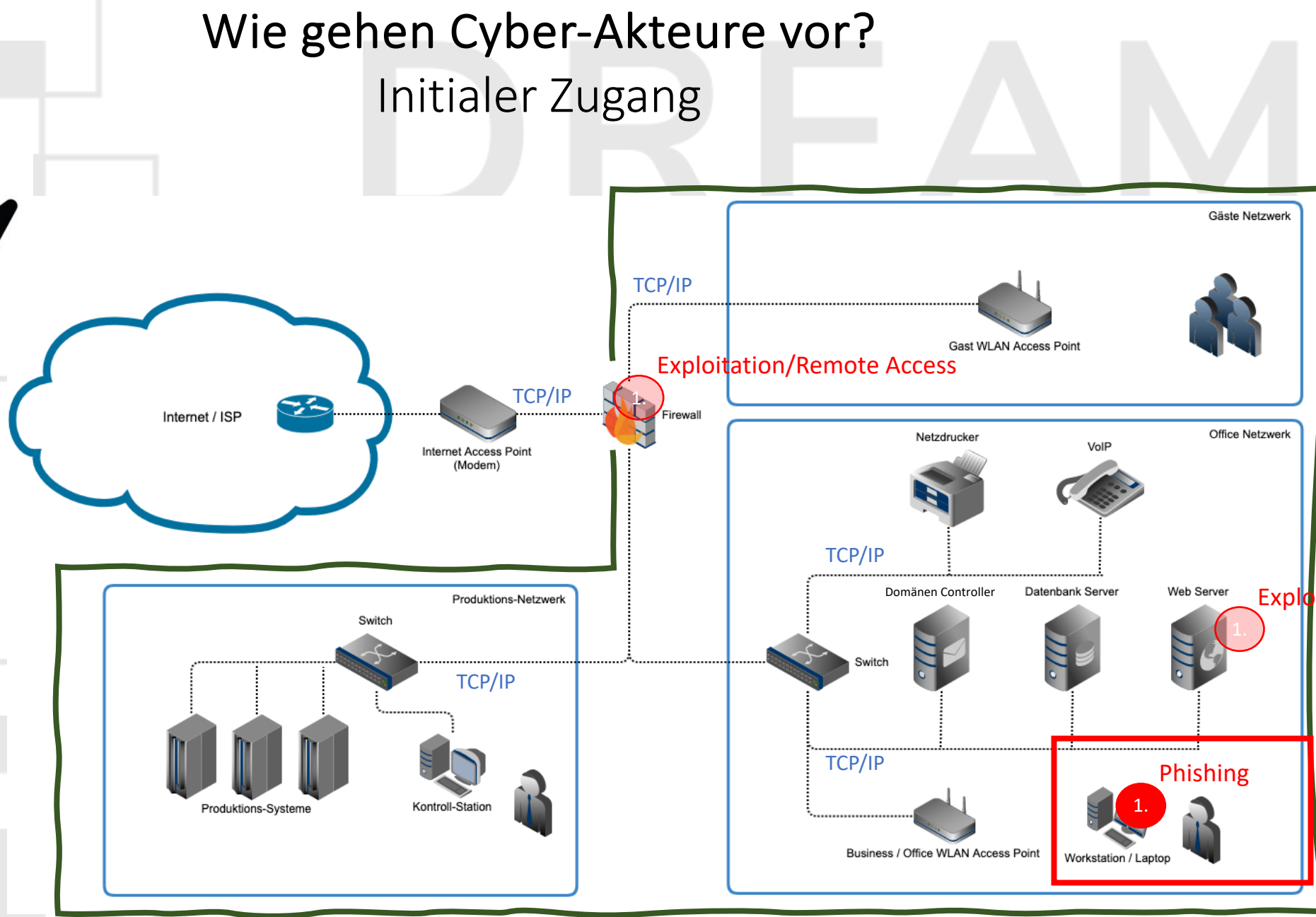
Wie gehen Cyber-Akteure vor?

Initialer Zugang



Wie gehen Cyber-Akteure vor?

Initialer Zugang

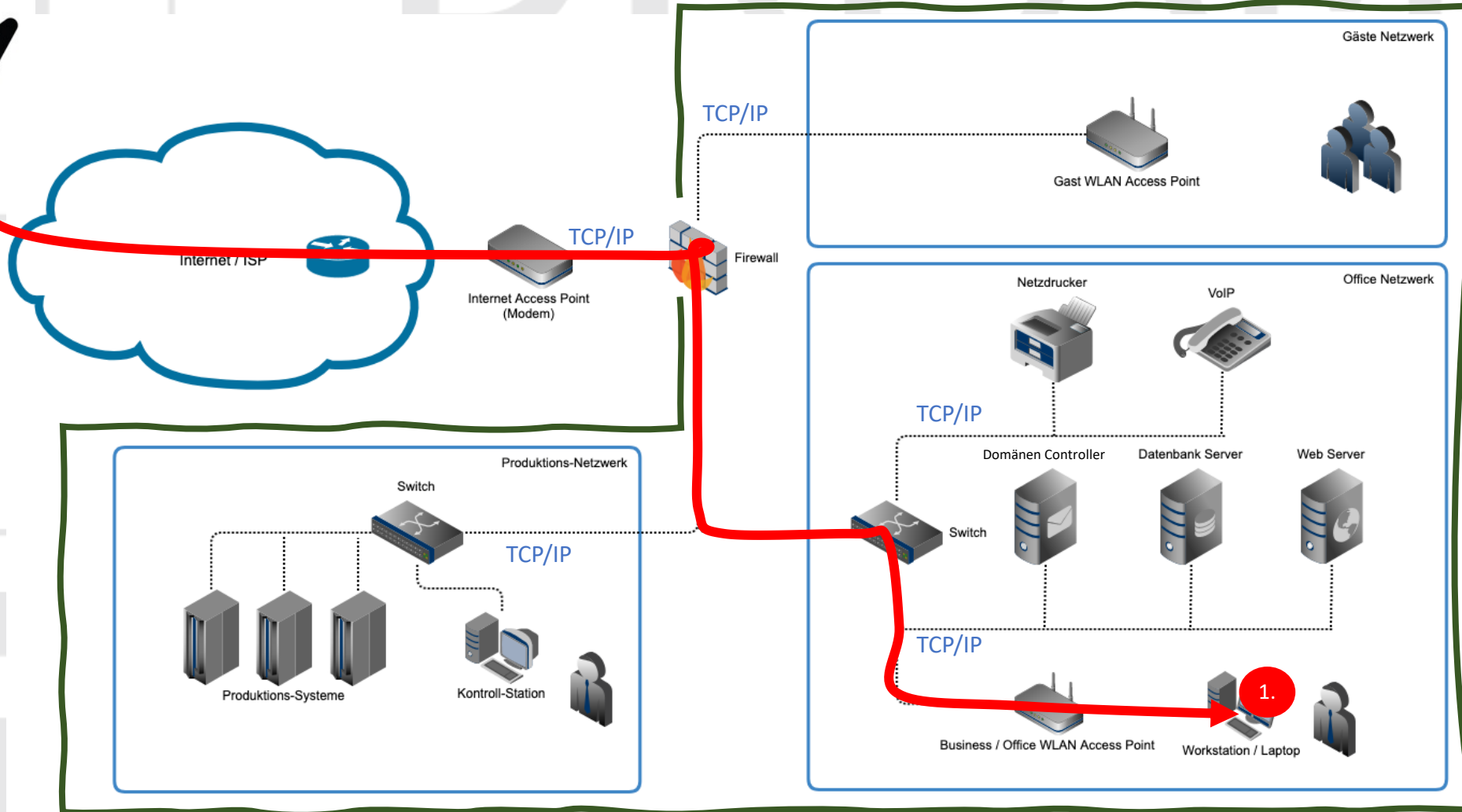


Wie gehen Cyber-Akteure vor?

Command & Control (C2)



2.
C2



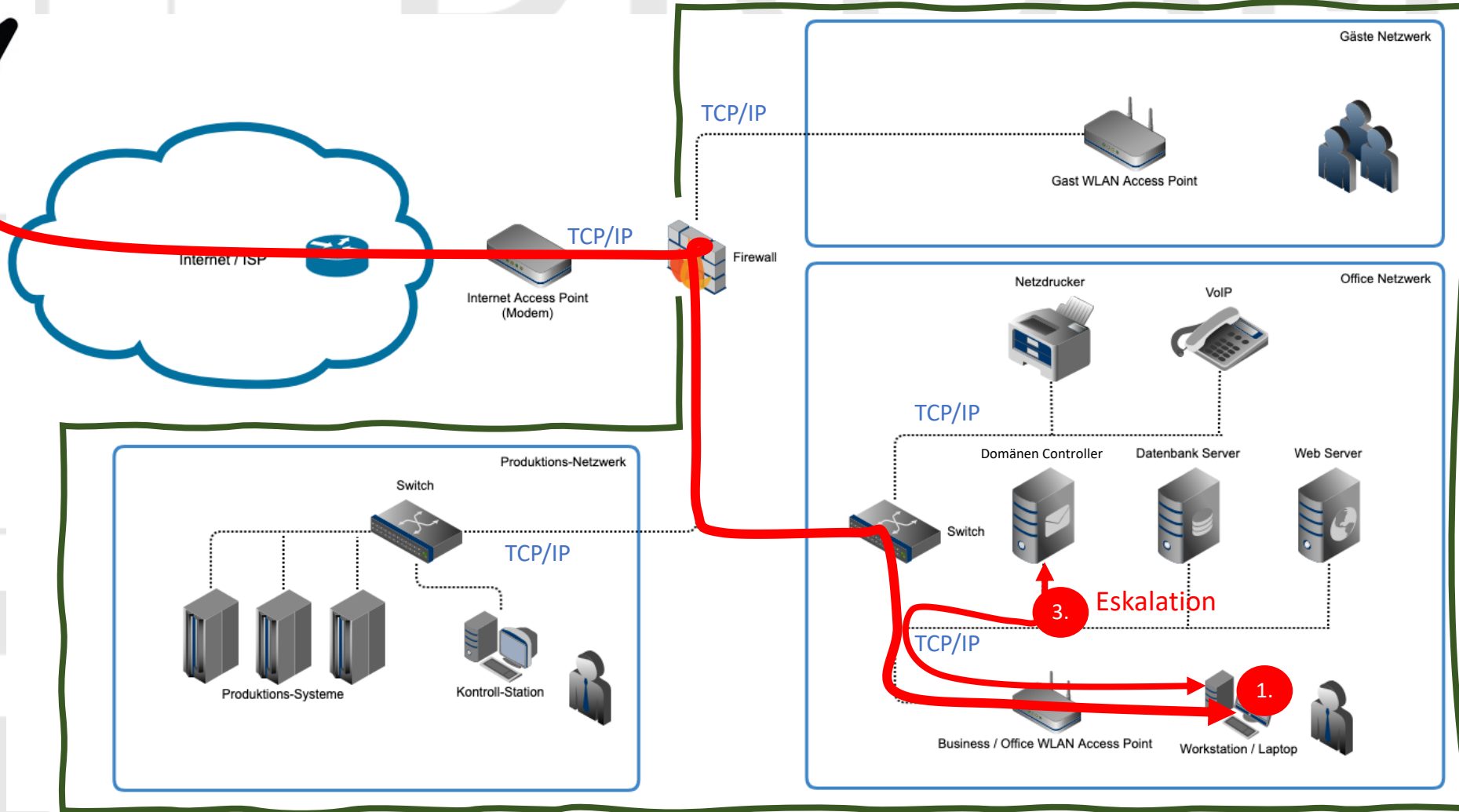
Perimeter

Wie gehen Cyber-Akteure vor?

Erweitern von Rechten und Weiterverbreitung



2.



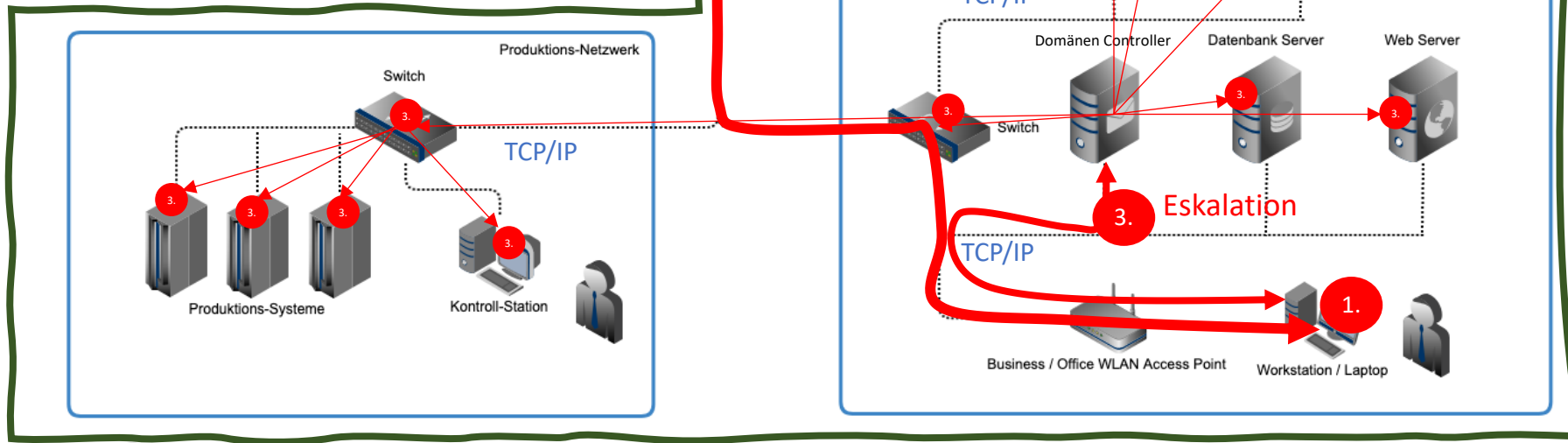
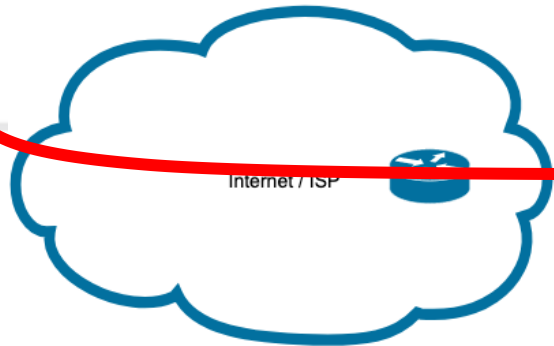
Perimeter

Wie gehen Cyber-Akteure vor?

Erweitern von Rechten und Weiterverbreitung



2.



Perimeter

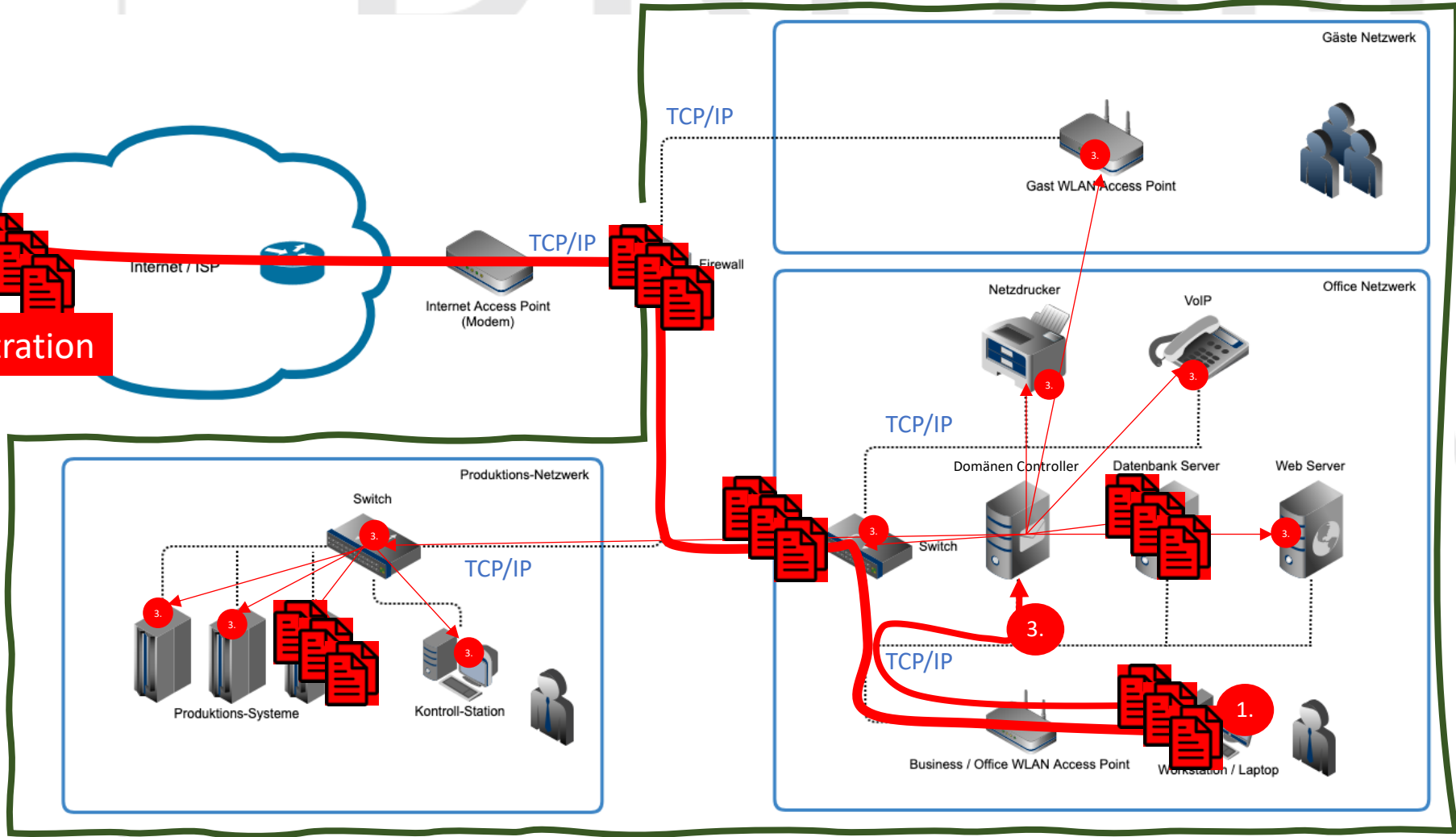
Wie gehen Cyber-Akteure vor?

Erreichen von Wirkung



2.

Exfiltration



Perimeter

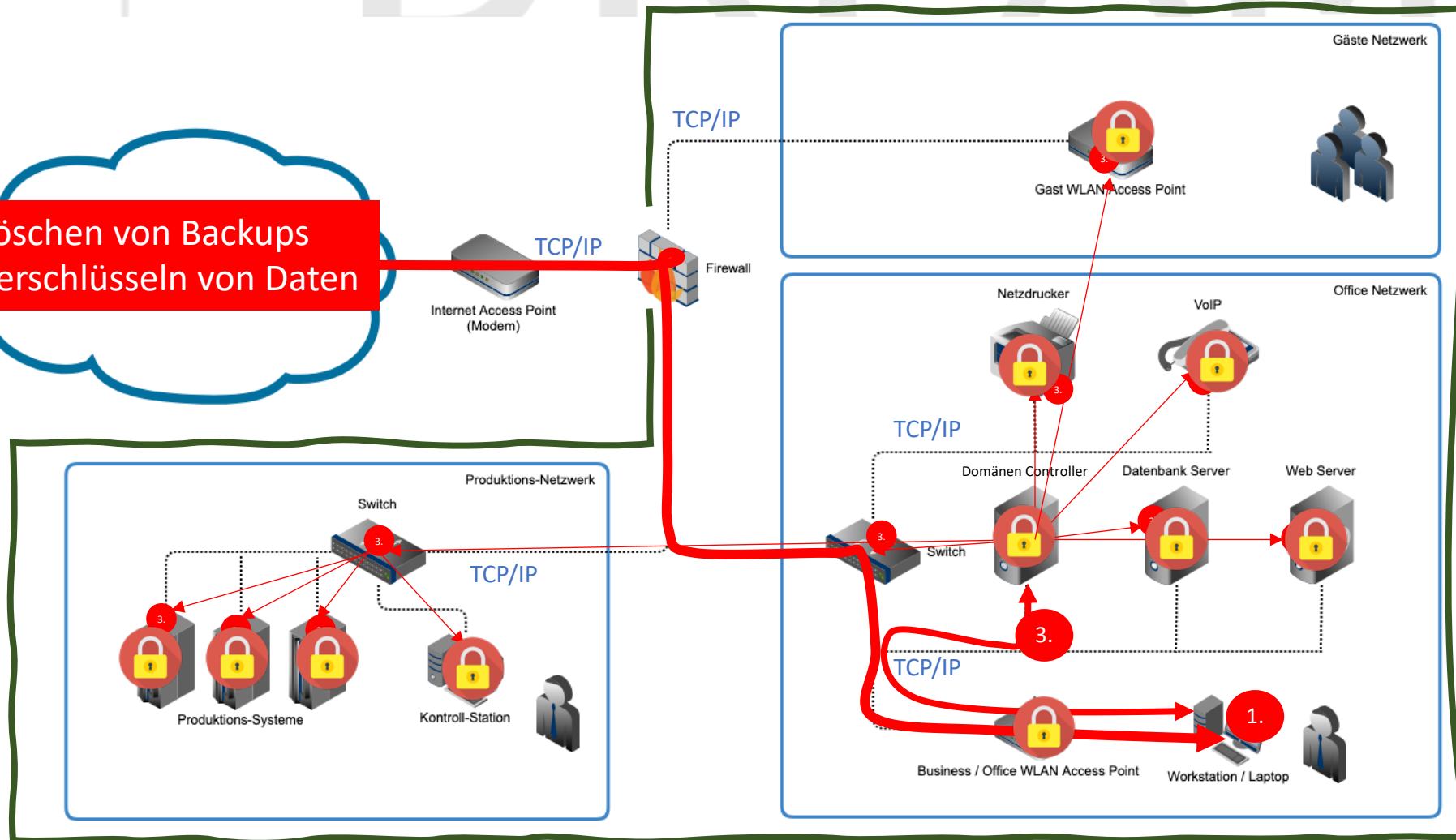
Wie gehen Cyber-Akteure vor?

Erreichen von Wirkung



2.

Löschen von Backups
Verschlüsseln von Daten



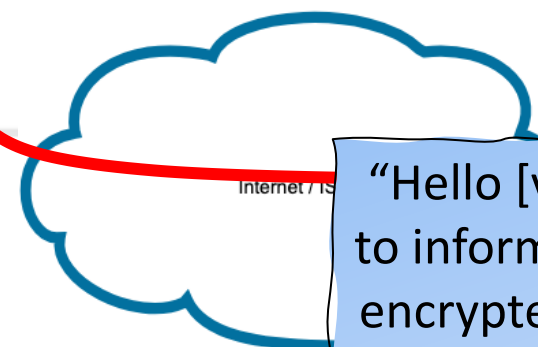
Perimeter

Wie gehen Cyber-Akteure vor?

Erreichen von Wirkung

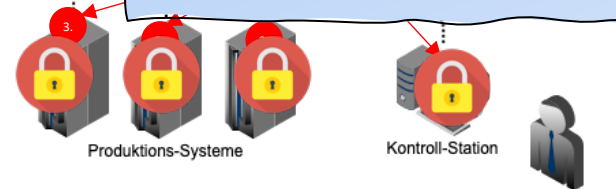


2.



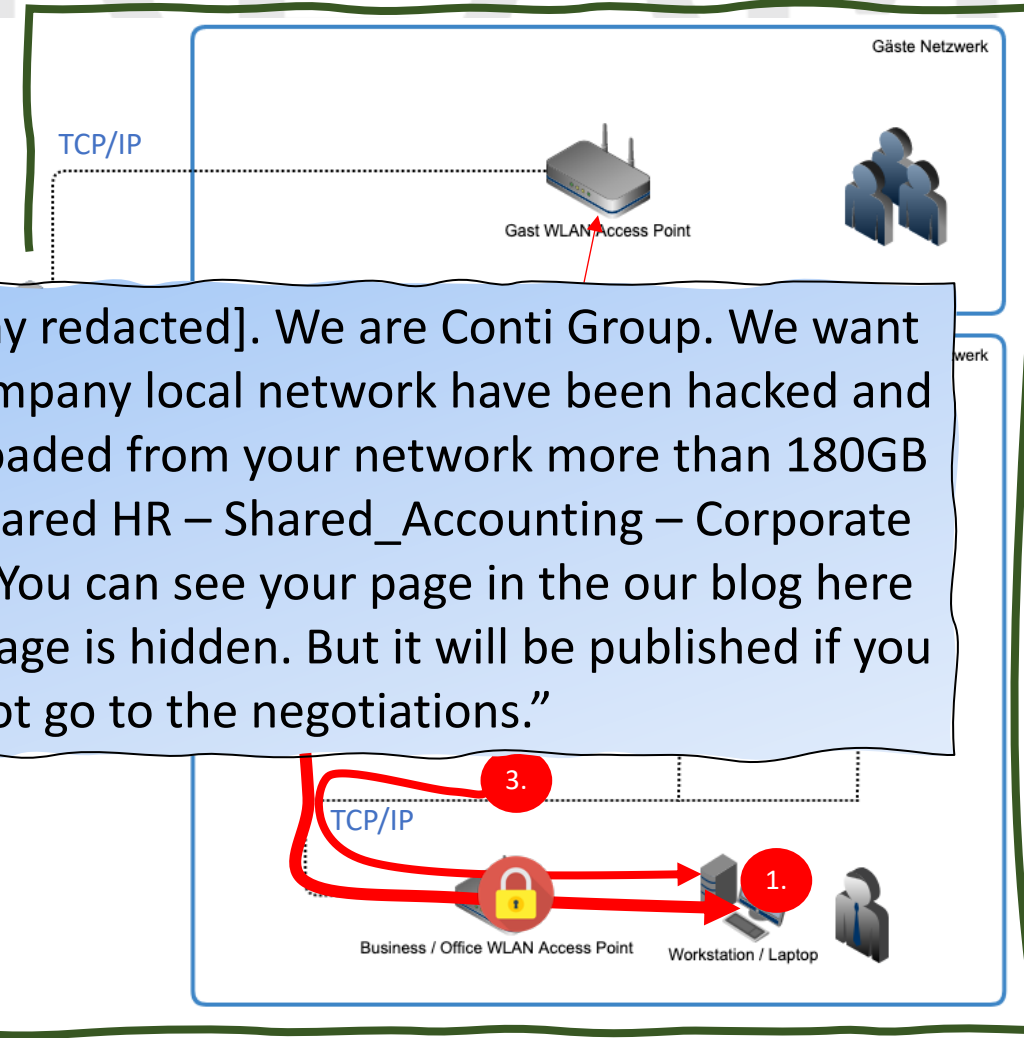
Internet / IS

“Hello [victim company redacted]. We are Conti Group. We want to inform that your company local network have been hacked and encrypted. We downloaded from your network more than 180GB of sensitive data. – Shared HR – Shared_Accounting – Corporate Debt – Departments. You can see your page in the our blog here [dark web link]. Your page is hidden. But it will be published if you do not go to the negotiations.”



Produktions-Systeme

Kontroll-Station



TCP/IP

Gäste Netzwerk

Gast WLAN Access Point

TCP/IP

Business / Office WLAN Access Point

Workstation / Laptop



Erzielen von Wirkung (Mission Objectives)

Erkundung (Reconnaissance)

Initieller Zugang (Initial Compromise)

Persistenz (Maintaining Access)

Welterbreitung (Privilege Escalation & Lateral Movement)

Perimeter



Auswirkungen

Datenverlust

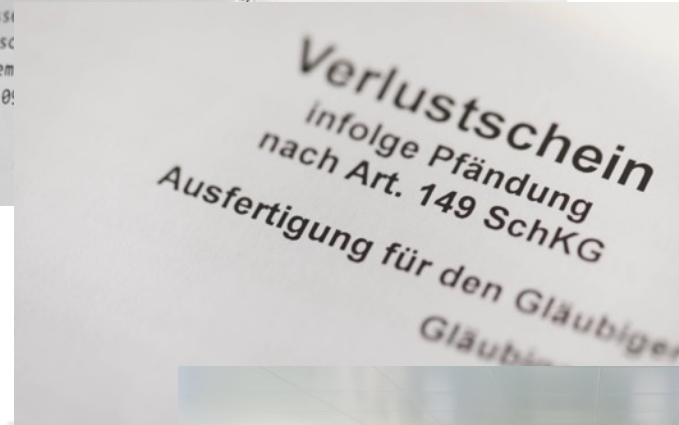
- Reputationsschaden
- Wirtschaftlicher Schaden

Unterbruch der operativen Tätigkeiten:

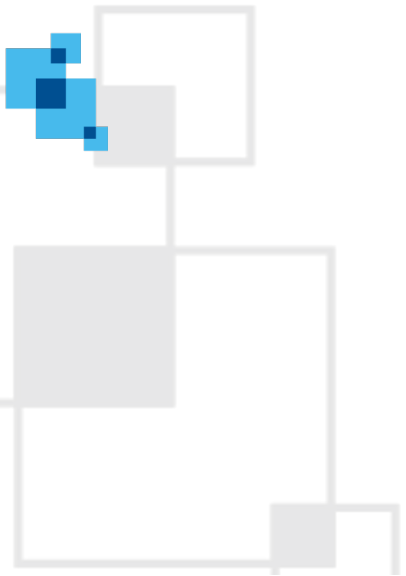
- Auftragsausfall
- Zahlungsausfall

Aufräum- und **Wiederherstellungsarbeiten:**

- Massive Belastung für Schlüsselressourcen
- Kostenfaktor



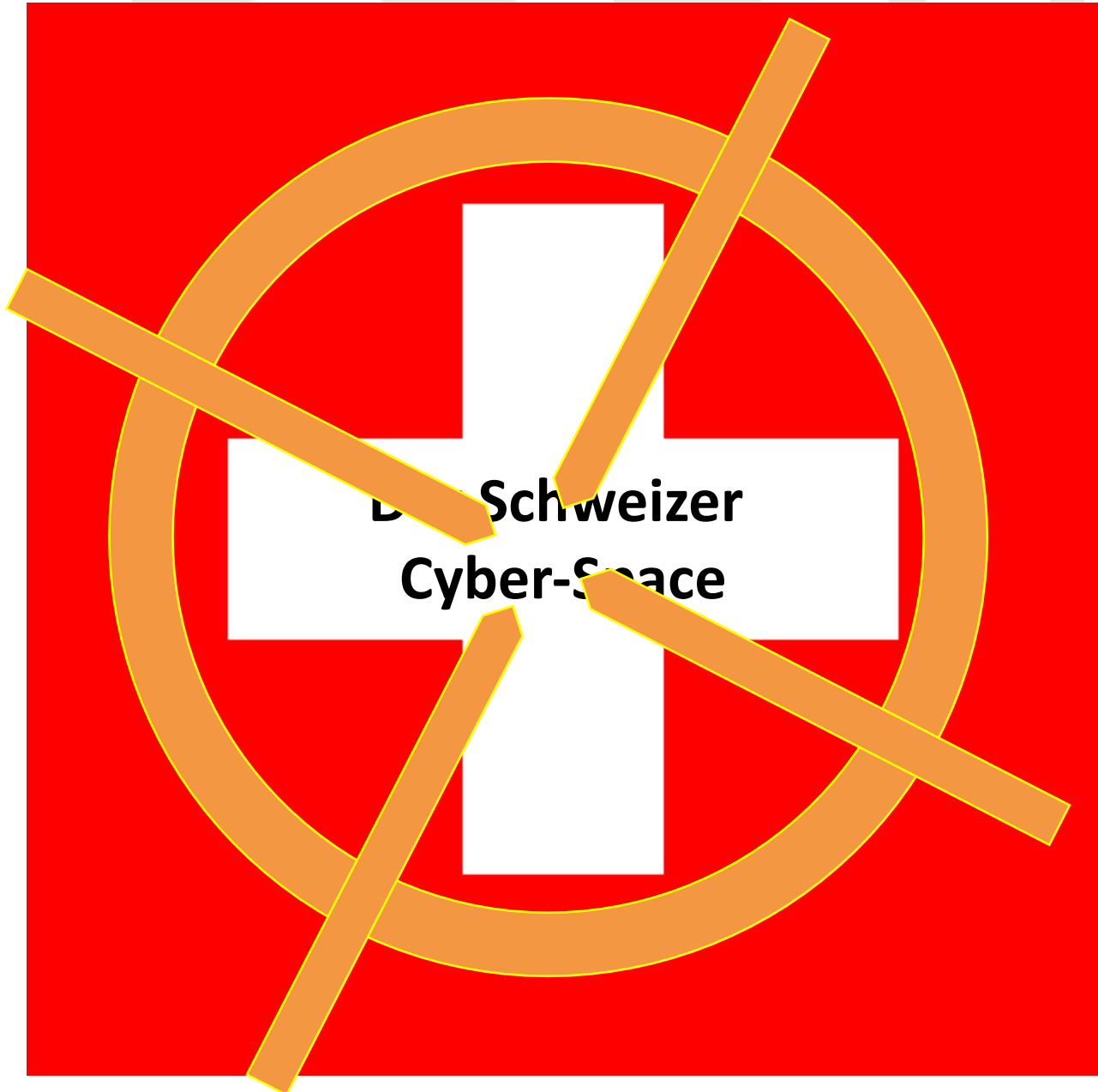
KONKURS



KATZ- UND MAUSSPIEL

«Der Markt für Cyber-Versicherungen funktioniert grundsätzlich»

<https://www.handelszeitung.ch/insurance/cyber-versicherungen-der-markt-funktioniert-598743>



MILA
GIES
Wisse
MILA

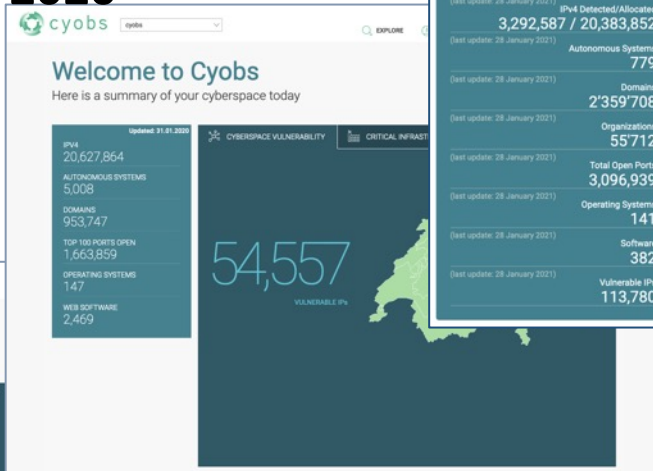


Die bekannten, öffentlich zugänglichen Schwachstellen im Schweizer Cyber Space nehmen zu

2019



2020



2021



2022




Quelle: Dreamlab Technologies AG, CyObs & Audit Department, 31 January 2021




Der Schweizer Cyber Space in 2022


Weitere populäre Schwachstellen



- XML External Entity injection (XXE) vulnerability
- CVE-2019-9670
- CVSS Score **7.5**
- Modification of system files possible
- 15 IPs affected**



- Microsoft Exchange Server Remote Code Execution
- CVE-2021-344
- CVSS Score **9.1**
- Remote Code Execution
- 84 IPs affected**



- Microsoft Exchange Server Remote Code Execution
- CVE-2021-26855
- CVSS Score **9.1**
- Part of an attack chain - Remote Code Execution
- 73 IPs affected**

Source: Dreamlab Technologies AG, CyObis & Audit Department, 2. März 2022

Der Schweizer Cyber Space in 2022

Bluekeep




98 hits for Bluekeep (CVE-2019-0708)

Kritische Fortinet-Schwachstelle: 533 direkt angreifbare IT-Systeme in der Schweiz identifiziert




17.10.2022

→ <https://www.ceresportal.ch/news/2022-10-11/fortinet-bue-ermoeslicht-unerwaelteten-admin-zugriff>


→ <https://www.netwoche.ch/news/2022-10-11/fortinet-bue-ermoeslicht-unerwaelteten-admin-zugriff>

Der Schweizer Cyber Space in 2022

Weitere populäre Schwachstellen




- Vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA)
- CVE-2020-3452
- CVSS Score **7.5**
- Directory traversal attacks and read sensitive files on a targeted system
- 536 IPs affected**



- Webmin Cross-Site Scripting RCE Vulnerability
- CVE-2021-31761
- CVSS Score **9.6 critical**
- Remote Code Execution
- 22 IPs affected**

Der Schweizer Cyber Space in 2022

Log4Shell – Log4j Vulnerability




- CVE-2021-4428
- High-severity (CVSS 10) vulnerability
- Affects the core function of **Apache Log4j2**
- Discovered in December 2021

57 IPs vulnerable
(as of 21.12.2021)











11 IPs vulnerable
(as of Feb 2022)

Swiss Universities and Government sites amongst affected IPs.



Command & Control Server in der Schweiz


[Copy](#) [Excel](#) [CSV](#) [PDF](#)
Search:

IP	PORT	TYPE	PAYLOAD	COUNTRY	FLAG	CERTIFICATE	FIRST DETECTION	LAST DETECTION	JARM	OTX PULSES
	80	cobalt_strike		Switzerland			2022-10-14 05:05	2022-10-14 05:05		
	443	metasploit	multi/meterpreter/reverse_http	Switzerland			2022-10-09 05:06	2022-10-09 05:06		
	443	cobalt_strike		Switzerland			2022-10-09 05:06	2022-10-09 05:06		
	80	cobalt_strike		Switzerland			2022-10-07 05:05	2022-10-07 05:05		
	2222	cobalt_strike		Switzerland			2022-09-21 05:04	2022-09-21 05:04		
	444	cobalt_strike		Switzerland			2022-09-21 05:04	2022-09-21 05:04		
	8080	cobalt_strike		Switzerland			2022-09-21 05:04	2022-09-21 05:04		
	443	cobalt_strike		Switzerland			2022-09-21 05:04	2022-09-21 05:04		
	443	cobalt_strike		Switzerland			2022-09-19 05:04	2022-09-19 05:04		
	80	cobalt_strike		Switzerland			2022-09-11 05:03	2022-09-11 05:03		

134 in 10.2022
(vs. 98 in 03.2022
vs. 36 in 02.2021)

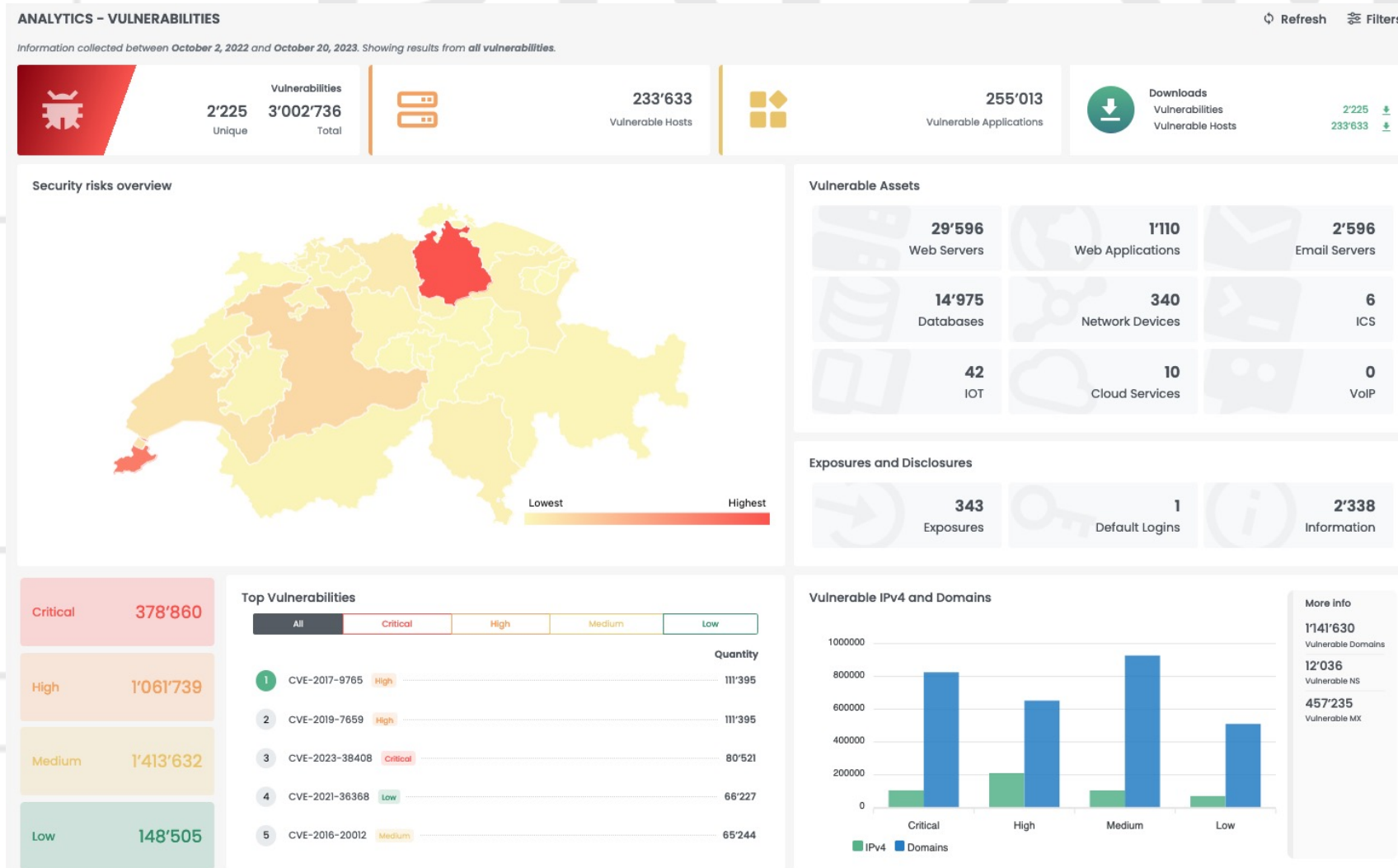


IP	Port	Type	Payload	Switzerland	Flag	Certificate	First Detection	Last Detection	JARM	OTX Pulses
----	------	------	---------	-------------	------	-------------	-----------------	----------------	------	------------

Showing 1 to 10 of 136 entries (filtered from 33,866 total entries)

[Previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) ... [14](#) [Next](#)

Messung des Schweizer Cyberspace



A scenic landscape at sunset. In the foreground on the left, a large tree with green and yellowing leaves stands prominently. The sun is low on the horizon, creating a bright glow and lens flare effects. The sky is filled with soft, white and grey clouds. The background shows a vast valley with rolling hills, green fields, and distant mountains under a clear blue sky.

Was hat sich bewährt?



Working on update 100% complete
Don't turn off your PC. This will take a while.

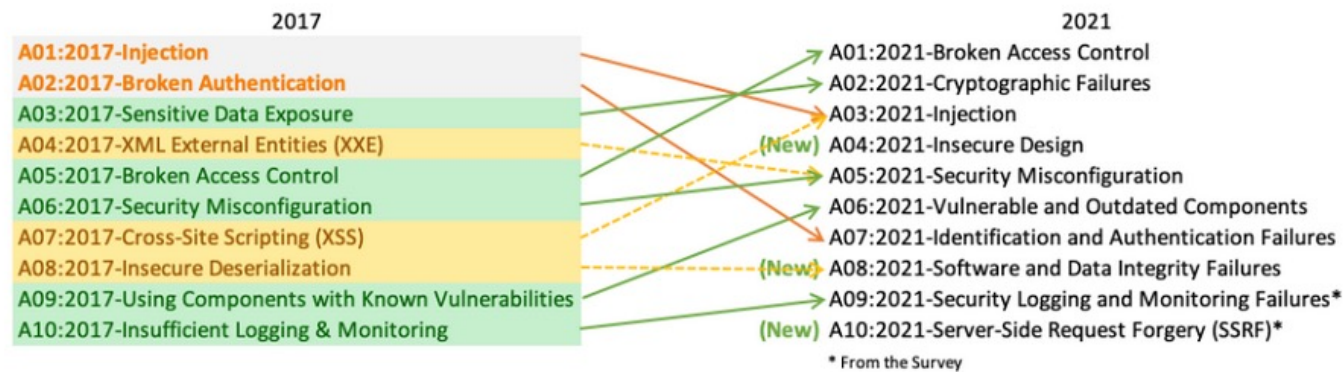
PATCH PATCH PATCH

Your PC will restart several times.

OWASP Top Ten – “Swiss Army Knife” for Web App Security

Top 10 Web Application Security Risks

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.

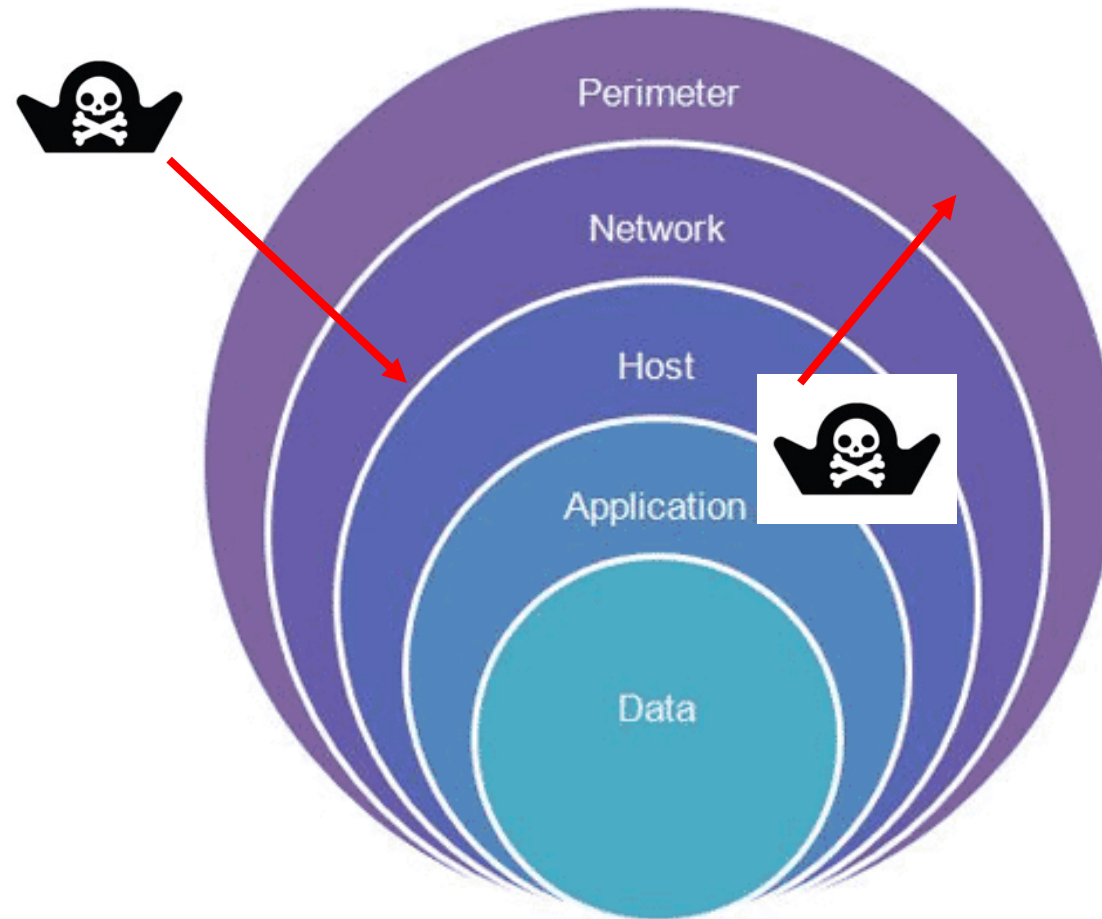


<https://owasp.org/www-project-top-ten/>

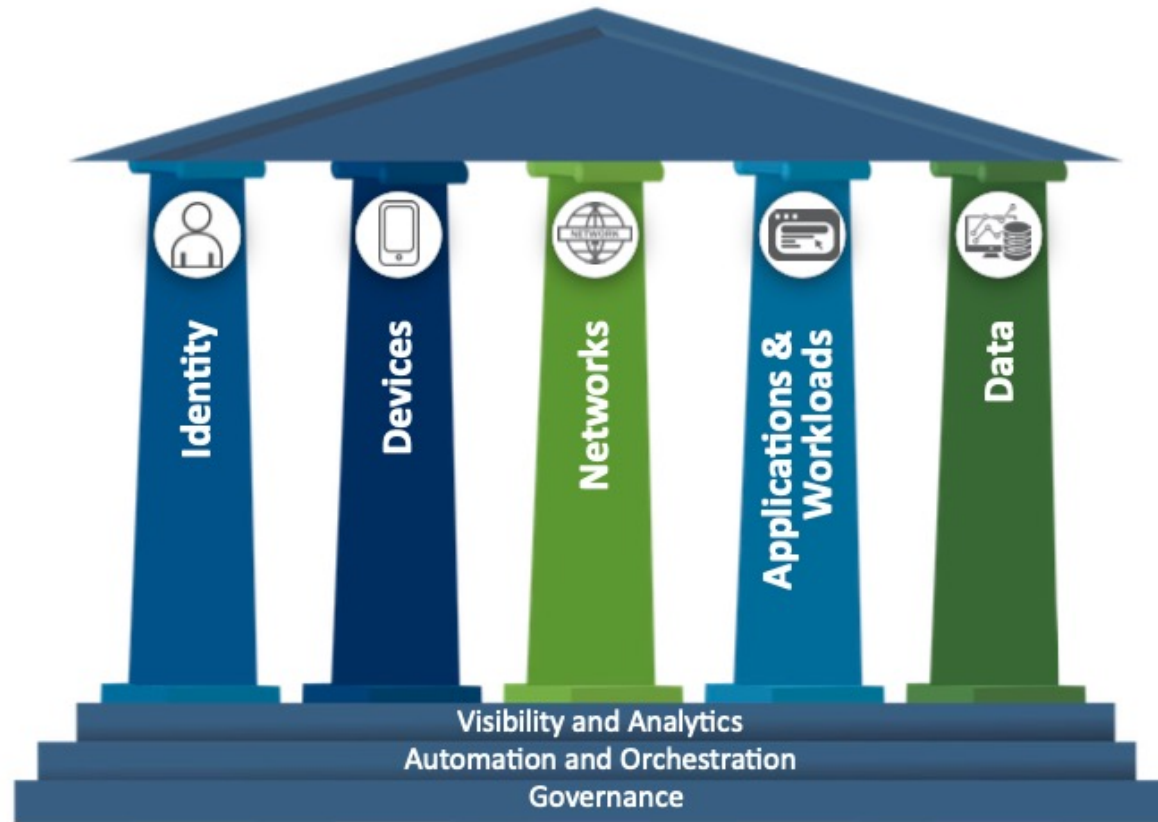
**Top Ten Cybersecurity
Misconfigurations
by NSA & CISA**

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a>

Mehrschichtige Verteidigung (Defense in Depth) schafft Resilienz



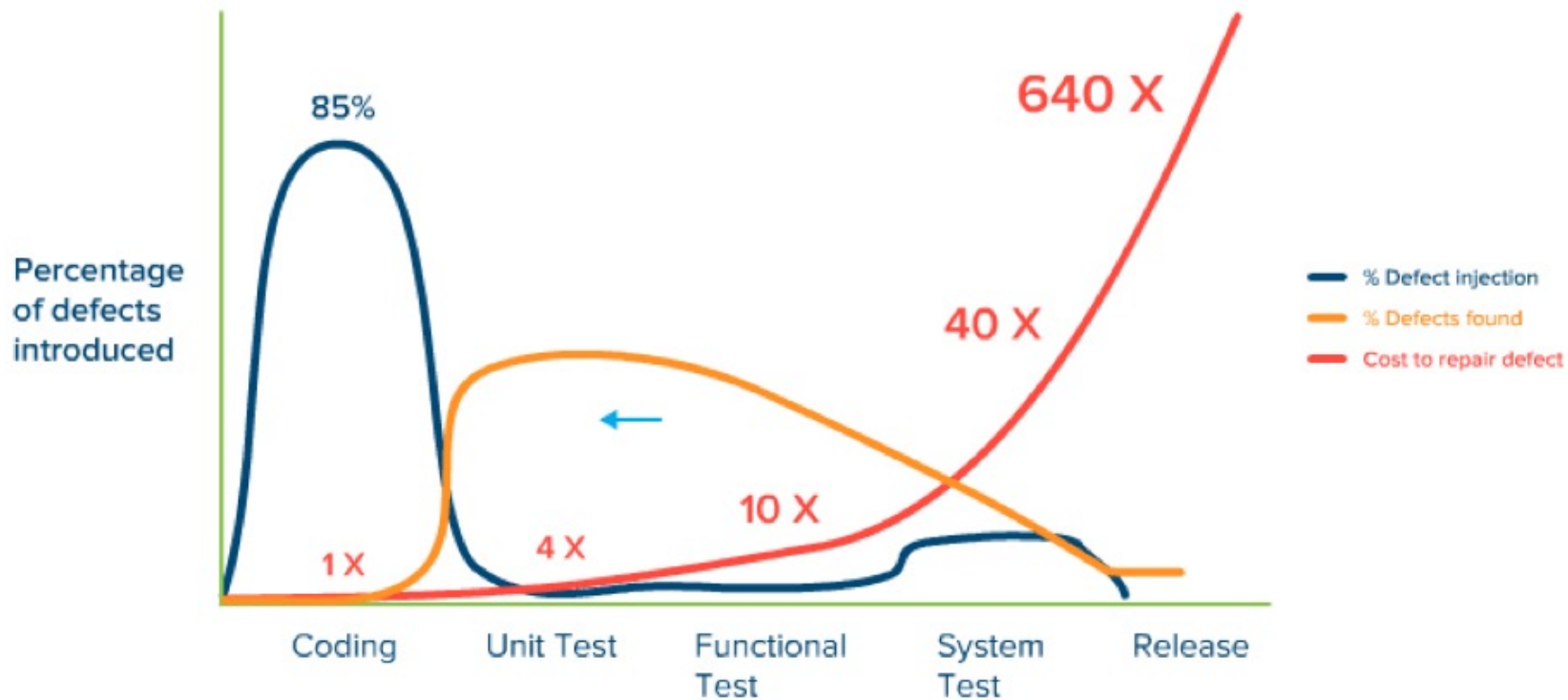
“Zukunft”: Zero Trust Architekturen



https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

IT-Sicherheit in Projekten

<<<< SHIFT LEFT gilt auch für Cyber Security



Jones, Capers. *Applied Software Measurement: Global Analysis of Productivity and Quality*.



IT-Sicherheit in Projekten





IT-Sicherheit in agilen Projekten

Idealfall: Addendum zum Agile Manifesto

“Business people and developers must work together daily throughout the project.”



“Business people, **IT Security** and developers must work together daily throughout the project. “

<http://agilemanifesto.org/principles.html>



IT-Sicherheit in agilen Projekten

Ein Security-Epic als Dreh- und Angelpunkt für Security Requirements

Analog anderer Nicht-Funktionaler Requirements

Jeweilige Gründe für Story aufzeigen

Akzeptanzkriterien definieren und durchsetzen

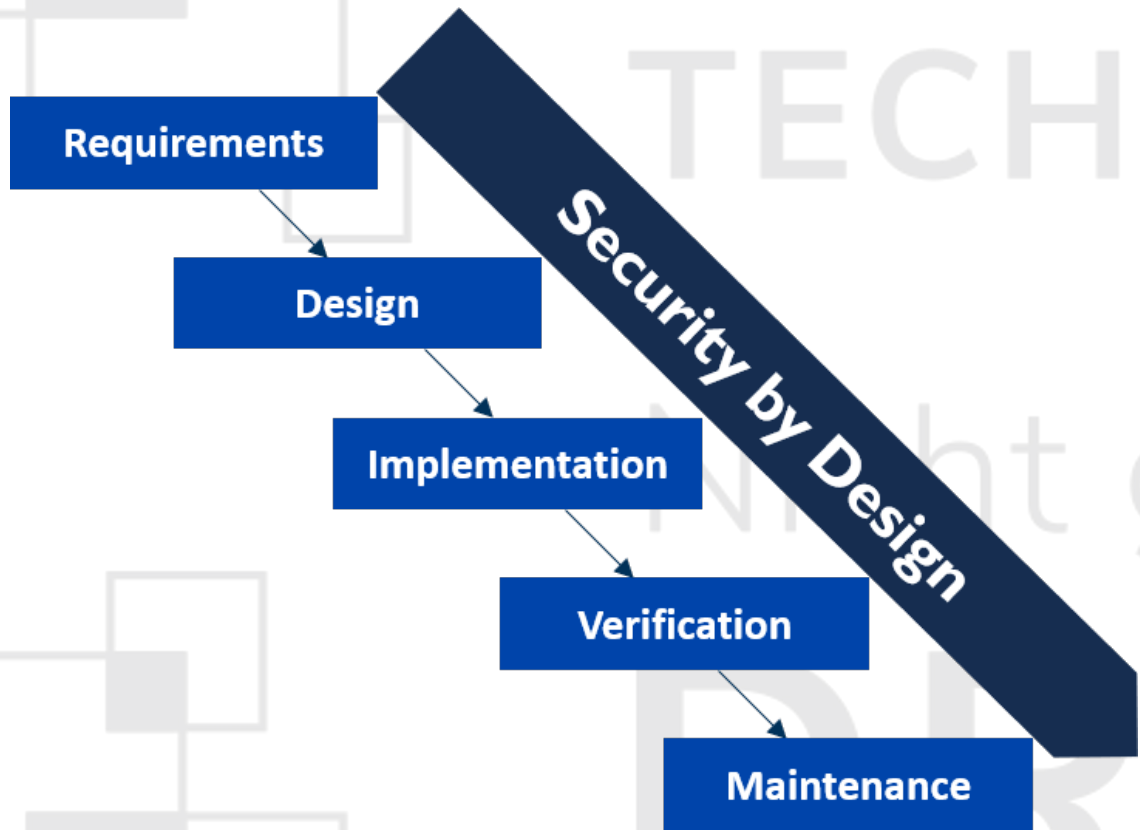
Quellen für generische User-Stories:

- **SAFECode: Practical Security Stories and Security Tasks for Agile Development Environments**
http://safecode.org/publication/SAFECode_Agile_Dev_Security0712.pdf
- **Handbook of secure agile software development.**
<https://docplayer.net/657918-Handbook-of-the-secure-agile-software-development-life-cycle.html>

Patching & upgrading

As	a service manager
I want	that any software component that is part of the product can be quickly and cost-efficiently security patched
so that	we minimise the time we are vulnerable to an attack.
Description	From the moment we become aware of a security vulnerability in our product, it will be a race against time. A failure to provide a security fix quickly enough may lead to the company having to take drastic measures, such as shutting down the service. This timespan typically ranges from hours to weeks, but cannot be known in advance. It is important to note that the security vulnerability may be in third-party code, but we still need to be able to provide a fix.
Acceptance criteria	<ul style="list-style-type: none">>> For all (third-party) code that we do not have a formal maintenance contract in place, we must have a formal patch back-porting process in place.>> We have automated test cases that try to patch each component in the running system.
Refinement questions	<ul style="list-style-type: none">>> How can we deploy patches?>> Are there components that are exceptionally hard to patch (e.g., third-party binaries, firmware or ROM code, components requiring formal certification or digital signature)?

Security by Design



Include security in every decision of the design process

Expect attacks and think about possible, realistic threats

Standards & Legislation

- ISO/IEC 27000-series
- ETSI EN 303 645: Baseline requirements for consumer IoT devices
- EU-GDPR, Art. 25: Privacy by design and default

<https://cetome.com/images/security-by-design.png>



IT-Sicherheit in Unternehmen

People

- **Befähigung** von Mitarbeitern
- Awareness und Verantwortung im Alltag
- Befolgen Richtlinien
- Umsetzen von Massnahmen
- Awareness und Verantwortung im Alltag

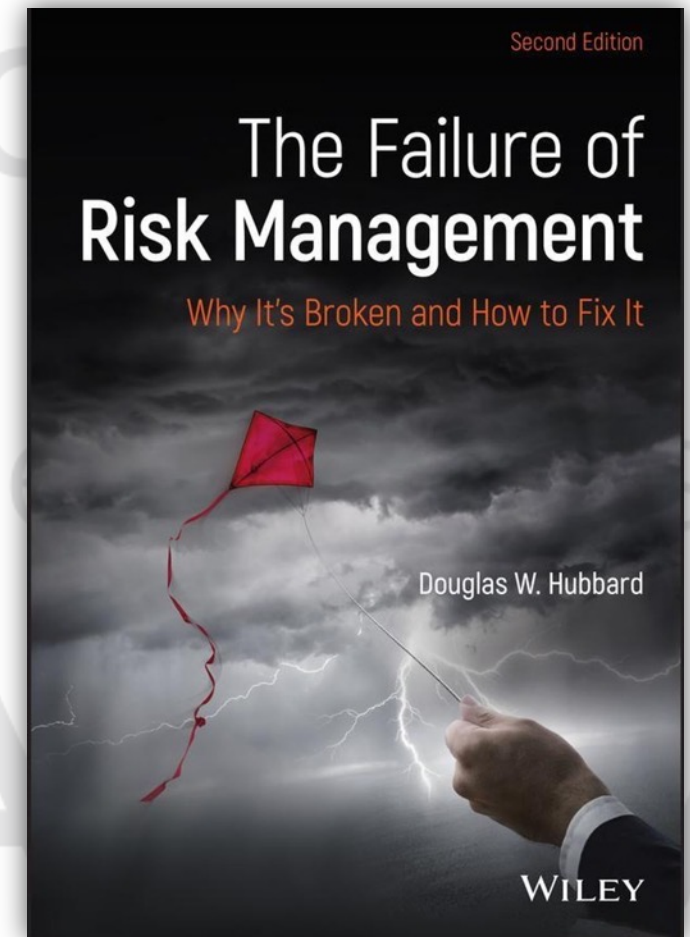
Processes

- **Gesamtverantwortung beim Top-Management**
- Management Buy-in mittels **einfacher (!)** IT-Security Policy
- Integration in Risikomanagement
- IT- und Security-Strategie
- Regelmässige Audits und Reviews
- IT-Sicherheit in Projekten

Technology

- Patchmanagement
- Vulnerability- und Netzwerk-Monitoring
- EDR-/ Antivirenlösung
- Regelmässige Penetrationstests
- Automatisierte Überwachung / Vulnerability Scanning

Empfohlene Lektüre



**STOP
BEING
NAÏVE**



**DREAMLAB
TECHNOLOGIES**



Thank
You!





Contact

Dreamlab Offices

Get in touch with us: contact@dreamlab.net
And follow us at: twitter.com/DreamlabGlobal
linkedin.com/company/dreamlab-technologies-ag



Dreamlab Switzerland

Dreamlab Technologies
Monbijoustrasse 36
Switzerland – 3011 Bern

Dreamlab Chile

Dreamlab Technologies
Villavicencio 361, Oficina 113
Chile – 8320154 Santiago de Chile

Dreamlab Spain

Dreamlab Technologies
Calle Hermosilla 48
1. Dcha
Spain – 28001 Madrid

Dreamlab Oman

Dreamlab Technologies LLC
Minarit Al Qurum Building
2nd floor, Office No. 233
Postal Code 133
Al Khuwair, Sultanate of Oman