



# Digitalisierung und Cyber Security

## Learnings aus dem Blackout in der Ukraine

30. August 2022, Swissgrid Netzforum, Verkehrshaus Luzern  
[cyrill.brunschwiler@compass-security.com](mailto:cyrill.brunschwiler@compass-security.com)



# Wie sicher ist unsere Stromversorgung?





Neue Zürcher Zeitung

# Ein längeres Blackout hätte katastrophale Folgen – doch undenkbar ist es nicht

Eine Welt ohne Elektrizität können wir uns kaum vorstellen. Doch das Szenario einer anhaltenden Strommangellage ist keineswegs abwegig. Und die Politik tut zu wenig, um es abzuwenden.

01.06.2021, 05.30 Uhr David Vonplon



Gaëtan Bally / Keystone

# Unterwerk (UW Mettlen)



<https://www.solutec.ch/de/aktuelles/referenzen/hs-netze/380-220kV-Schaltanlage-UW-METTLEN.php>



# Wie sicher ist unsere Stromversorgung ?



<https://www.youtube.com/watch?v=UF5EDV6T7es>

# Unterwerk Schutzgeräte, Protokollwandler, Automatisierung (IEDs)



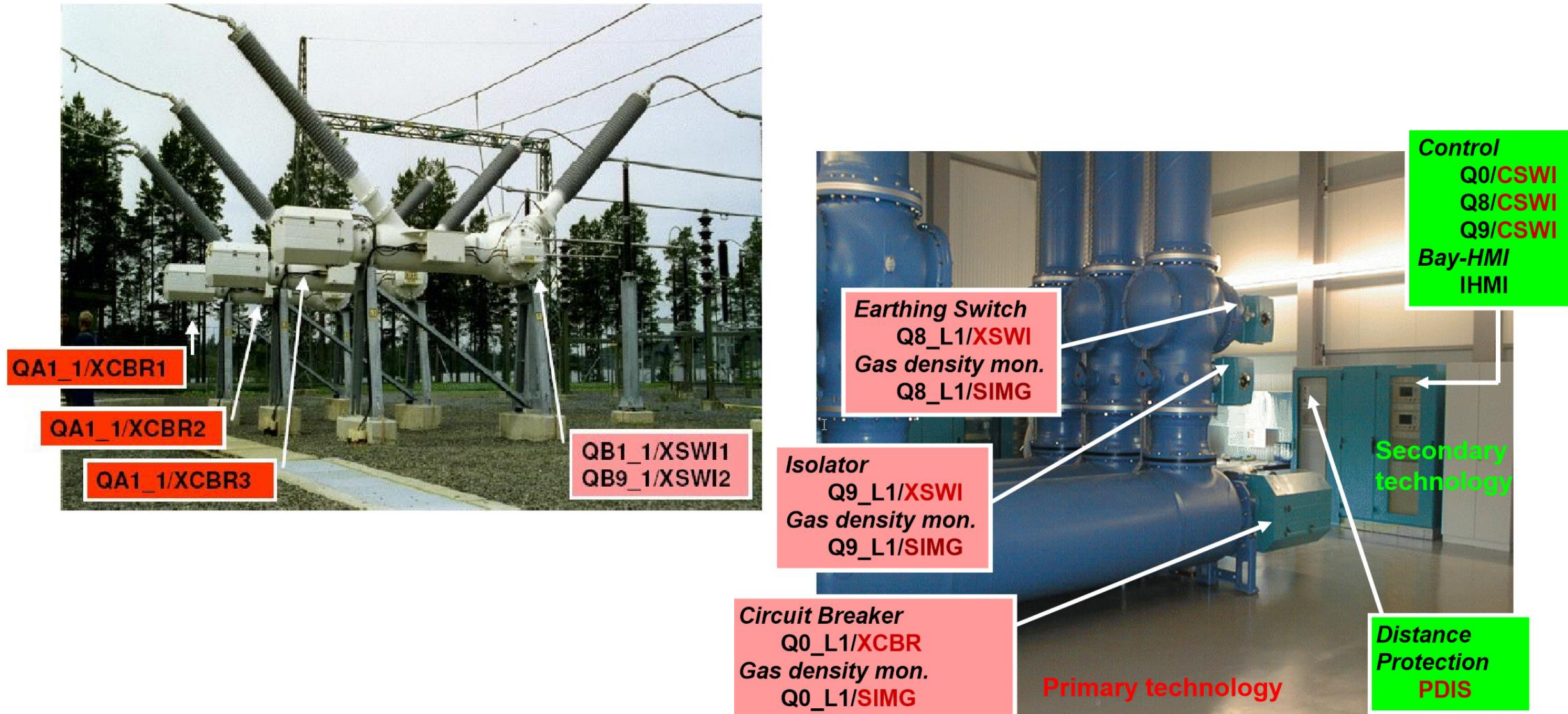
<https://new.abb.com/substation-automation/products/the-power-of-one>

<https://www.directindustry.com/prod/siemens-energy-automation/product-30064-589133.html>

<https://www.se.com/in/en/work/products/product-launch/easergy/easergy-p3.jsp>

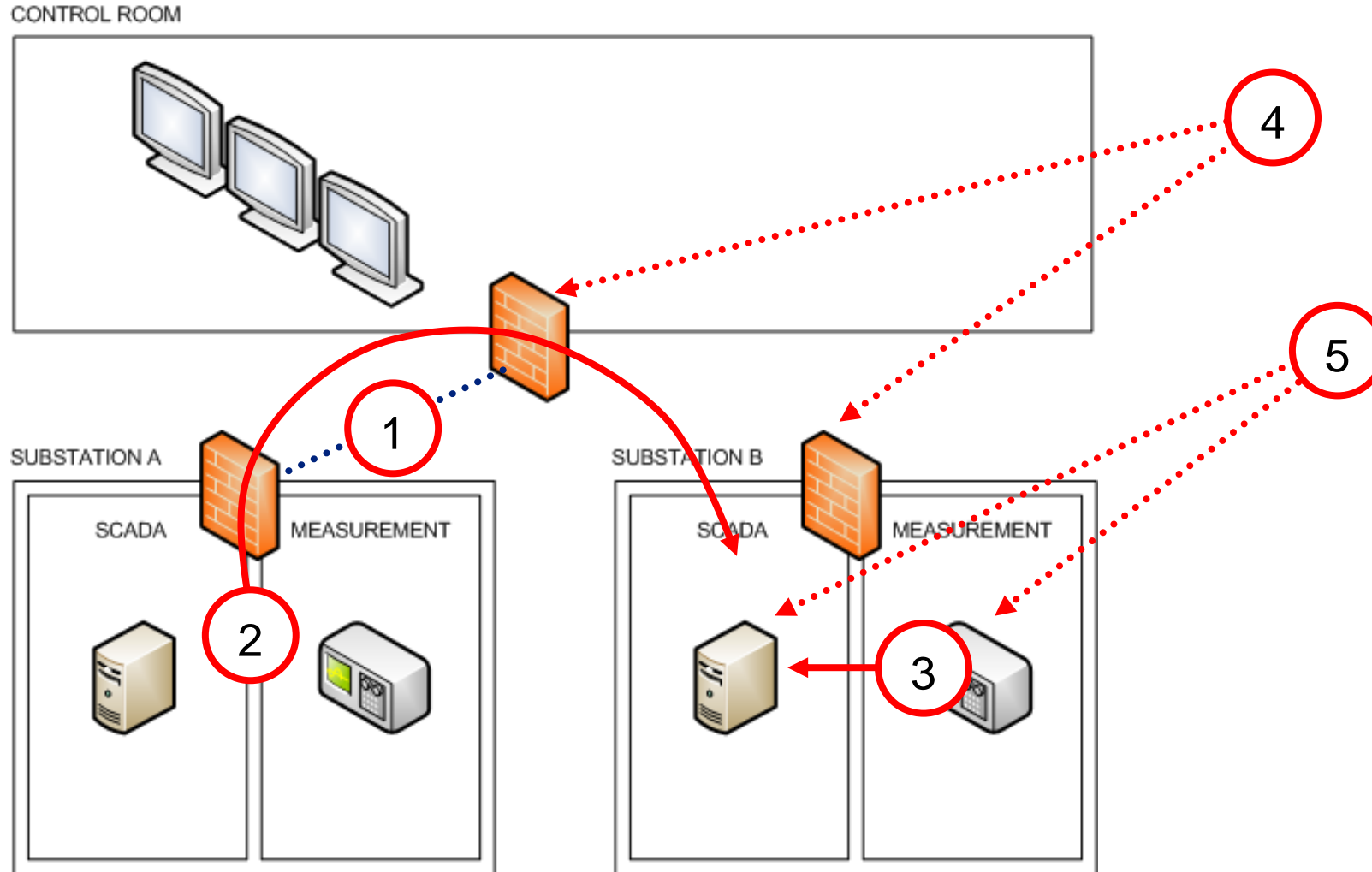


# Namensgebung mittels Objektmodell (IEC 61850 MMS)



ABB, Kirmann, [https://web.fe.up.pt/~asousa/sind/acetat/AI\\_EPFL/AI\\_421\\_IEC61850.pdf](https://web.fe.up.pt/~asousa/sind/acetat/AI_EPFL/AI_421_IEC61850.pdf)

# Angriffsszenarien gegen Unterwerke





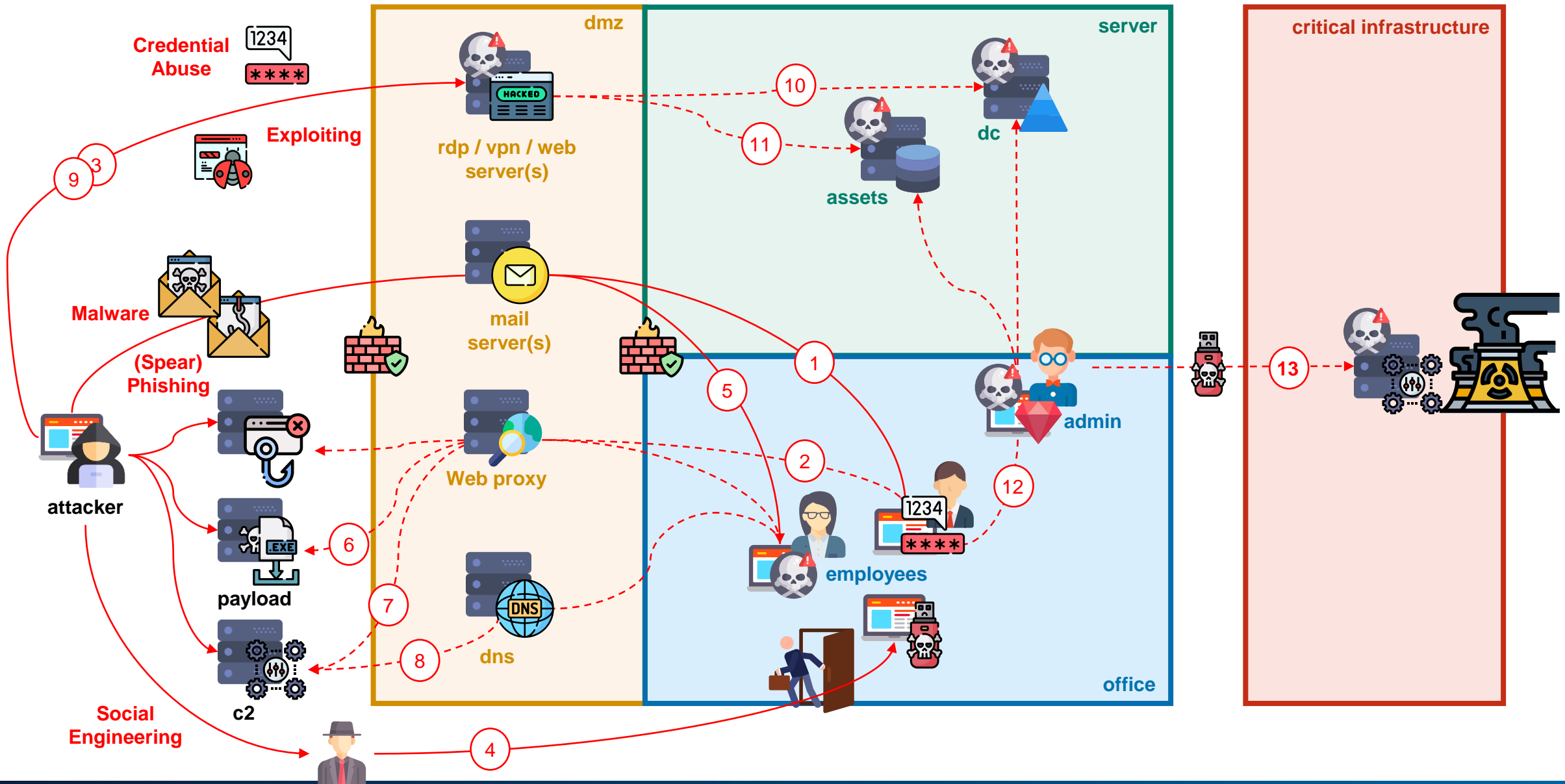
# Typische Einbruchsmuster

Nicht jeder Vorfall ist so super-genial, wie die Medien glauben gemacht werden.

In der Regel fallen die Unternehmen auf einfache Dinge herein

- **Malspam**
- **Schlechte Passwörter**
- **Fehlende 2FA**
- **Anfälligkeit von Geräten oder Software (fehlende Patches)**

# Typische Einbruchsmuster





# Was bedeutet das im Detail?

## MITRE ATT&CK Framework

# MITRE ATT&CK Framework

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	14 techniques	25 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Boot or Logon Autostart Execution (12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data from Cloud Storage Object	Exfiltration Over Other Network Medium (1)	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Browser Extensions	Direct Volume Access	Input Capture (4)	Cloud Service Dashboard	Remote Services (6)	Data from Configuration Repository (2)	Data Obfuscation (3)	Exfiltration Over C2 Channel	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Compromise Client Software Binary	Execution Guardrails (1)	Man-in-the-Middle (2)	Cloud Service Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Supply Chain Compromise (3)	System Services (2)	Software Deployment Tools	Create or Modify System Process (4)	Create or Modify System Process (4)	Exploitation for Defense Evasion	Modify Authentication Process (4)	Domain Trust Discovery	Software Deployment Tools	File and Directory Discovery	Encrypted Channel (2)	Exfiltration Over Network Medium (1)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Trusted Relationship	User Execution (2)	System Services (2)	Event Triggered Execution (15)	Event Triggered Execution (15)	File and Directory Permissions Modification (2)	Network Sniffing	File and Directory Discovery	Taint Shared Content	Network Service Scanning	Fallback Channels	Exfiltration Over Physical Medium (1)	Firmware Corruption
Search Open Websites/Domains (2)	Valid Accounts (4)	Windows Management Instrumentation	User Execution (2)	Group Policy Modification	Group Policy Modification	Group Policy Modification	OS Credential Dumping (8)	Network Share Discovery	Use Alternate Authentication Material (4)	Network Share Discovery	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Victim-Owned Websites			Valid Accounts (4)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Hide Artifacts (7)	Steal Application Access Token	Network Sniffing		Network Sniffing	Multi-Stage Channels	Exfiltration Over Web Service (2)	Network Denial of Service (2)
				External Remote Services	External Remote Services	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (4)	Network Sniffing		Network Sniffing	Non-Application Layer Protocol	Scheduled Transfer	Resource Hijacking
				Hijack Execution Flow (11)	Hijack Execution Flow (11)	Impair Defenses (7)	Steal Web Session Cookie	Password Policy Discovery		Password Policy Discovery	Non-Standard Port	Transfer Data to Cloud Account	Service Stop
				Implant Container Image	Implant Container Image	Indicator Removal on Host (6)	Two-Factor Authentication Interception	Peripheral Device Discovery		Peripheral Device Discovery	Protocol Tunneling		System Shutdown/Reboot
				Office Application Startup (6)	Office Application Startup (6)	Indirect Command Execution	Unsecured Credentials (6)	Permission Groups Discovery (3)		Permission Groups Discovery (3)	Proxy (4)		
				Pre-OS Boot (5)	Pre-OS Boot (5)	Masquerading (6)	Modify Authentication Process (4)	Process Discovery		Process Discovery	Remote Access Software		
				Scheduled Task/Job (6)	Scheduled Task/Job (6)	Modify Cloud Compute Infrastructure (4)	Modify Registry	Query Registry		Query Registry	Traffic Signaling (1)		
				Server Software Component (3)	Server Software Component (3)	Modify Registry	Modify System Image (2)	Remote System Discovery		Remote System Discovery	Web Service (3)		
				Traffic Signaling (1)	Traffic Signaling (1)	Network Boundary Bridging (1)	Obfuscated Files or Information (5)	Software Discovery (1)		Software Discovery (1)			
				Valid	Valid	Obfuscated Files or Information (5)		System Information Discovery		System Information Discovery			
								System Network Configuration Discovery		System Network Configuration Discovery			
								System Network Connections Discovery		System Network Connections Discovery			



# MITRE ATT&CK Framework

## Groups

			primarily interested in users of remote banking systems in Russia and neighboring countries. The group uses a Trojan by the same name (RTM).
G0034	Sandworm Team	ELECTRUM, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, VOODOO BEAR	<p><b>Sandworm Team</b> is a destructive threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST) military unit 74455. This group has been active since at least 2009.</p> <p>In October 2020, the US indicted six GRU Unit 74455 officers associated with <b>Sandworm Team</b> for the following cyber operations: the 2015 and 2016 attacks against Ukrainian electrical companies and government organizations, the 2017 worldwide <b>NotPetya</b> attack, targeting of the 2017 French presidential campaign, the 2018 <b>Olympic Destroyer</b> attack against the Winter Olympic Games, the 2018 operation against the Organisation for the Prohibition of Chemical Weapons, and attacks against the country of Georgia in 2018 and 2019. Some of these were conducted with the assistance of GRU Unit 26165, which is also referred to as <b>APT28</b>.</p>
G0029	Scarlet Mimic		<p><b>Scarlet Mimic</b> is a threat group that has targeted minority rights activists.</p>

# NEWS

Home

Video

World

UK

Business

Tech

Science

Stories

Entertainment & Arts

## Ukraine power cut 'was cyber-attack'



REUTERS



# Ukraine Hack

## Schritt 1

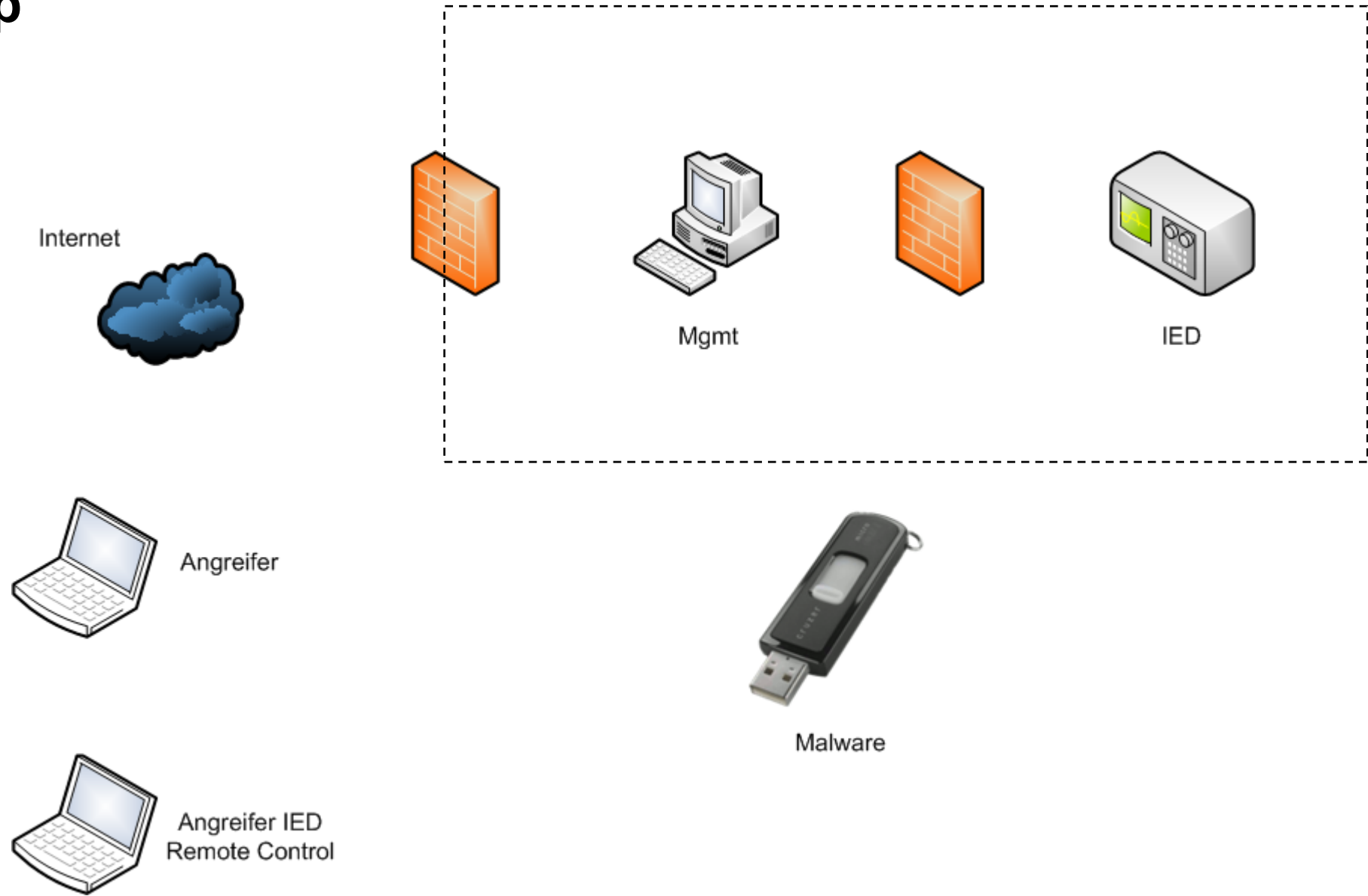
- Phishing E-Mails mit Word Macro, Black Energy Trojaner nachgeladen
- VPN Zugänge und Passwörter gestohlen
- Netzwerkanalyse und Lateral Movement

## Schritt 2

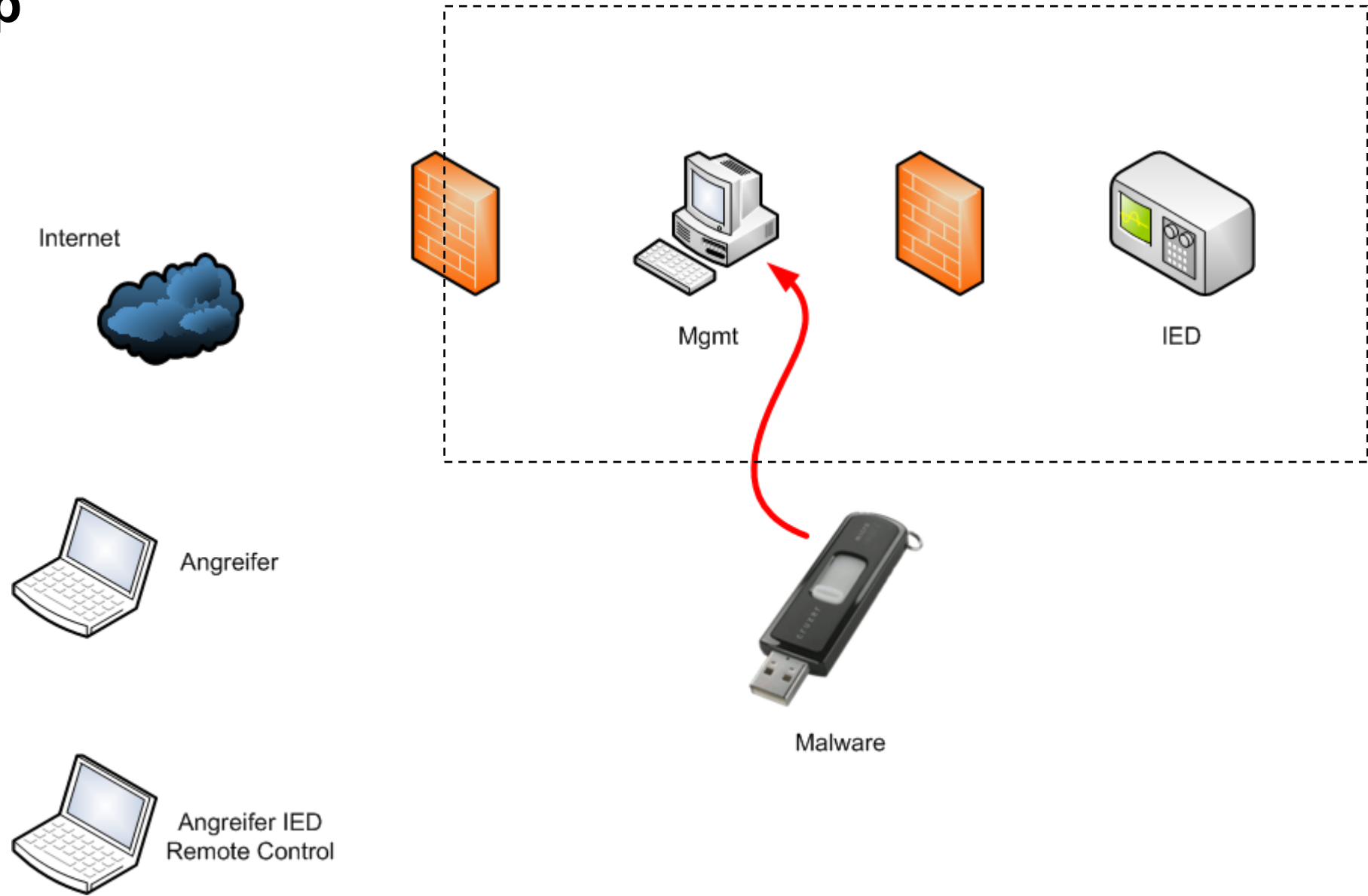
- Böartige Firmware entwickelt
- SCADA Umgebung übernommen via Benutzeroberfläche
- Trennschalter geöffnet
- UPS Abschaltung orchestriert, Firmware auf Converter geladen, Logs und Disks gelöscht
- Telefonie Denial of Service

[https://ics.sans.org/media/E-ISAC\\_SANS\\_Ukraine\\_DUC\\_5.pdf](https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf)

# Demo Setup

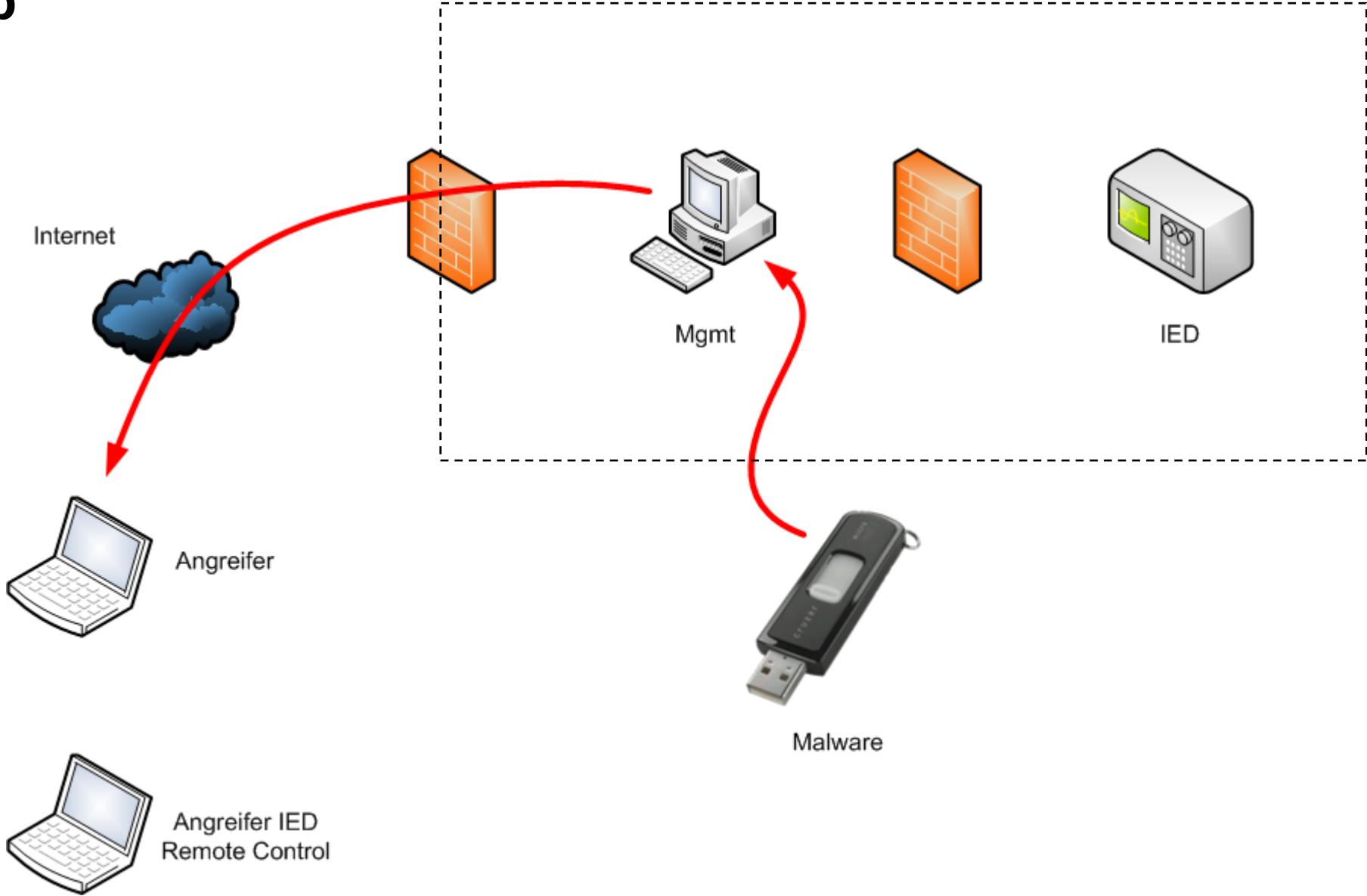


# Demo Setup

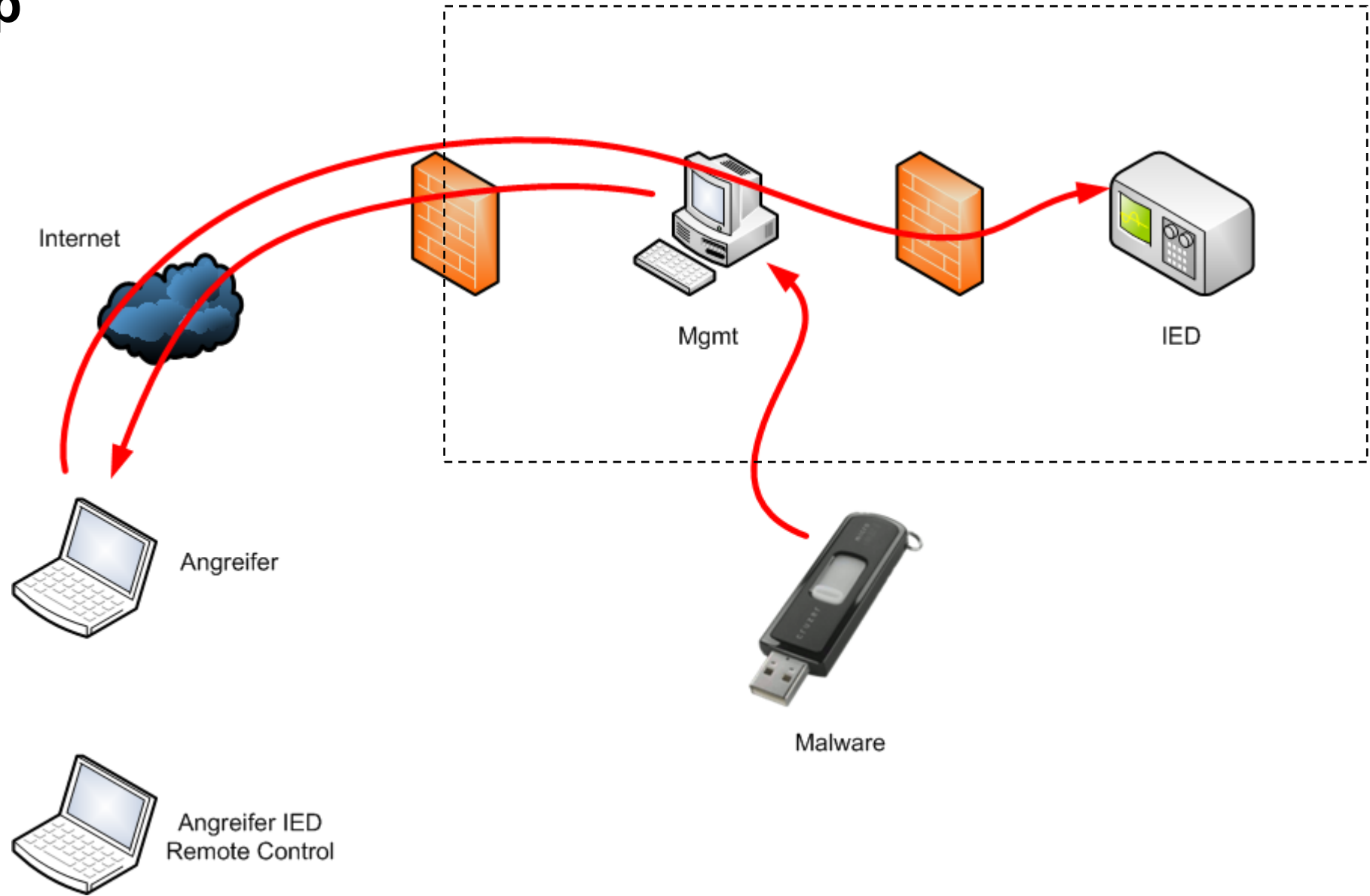




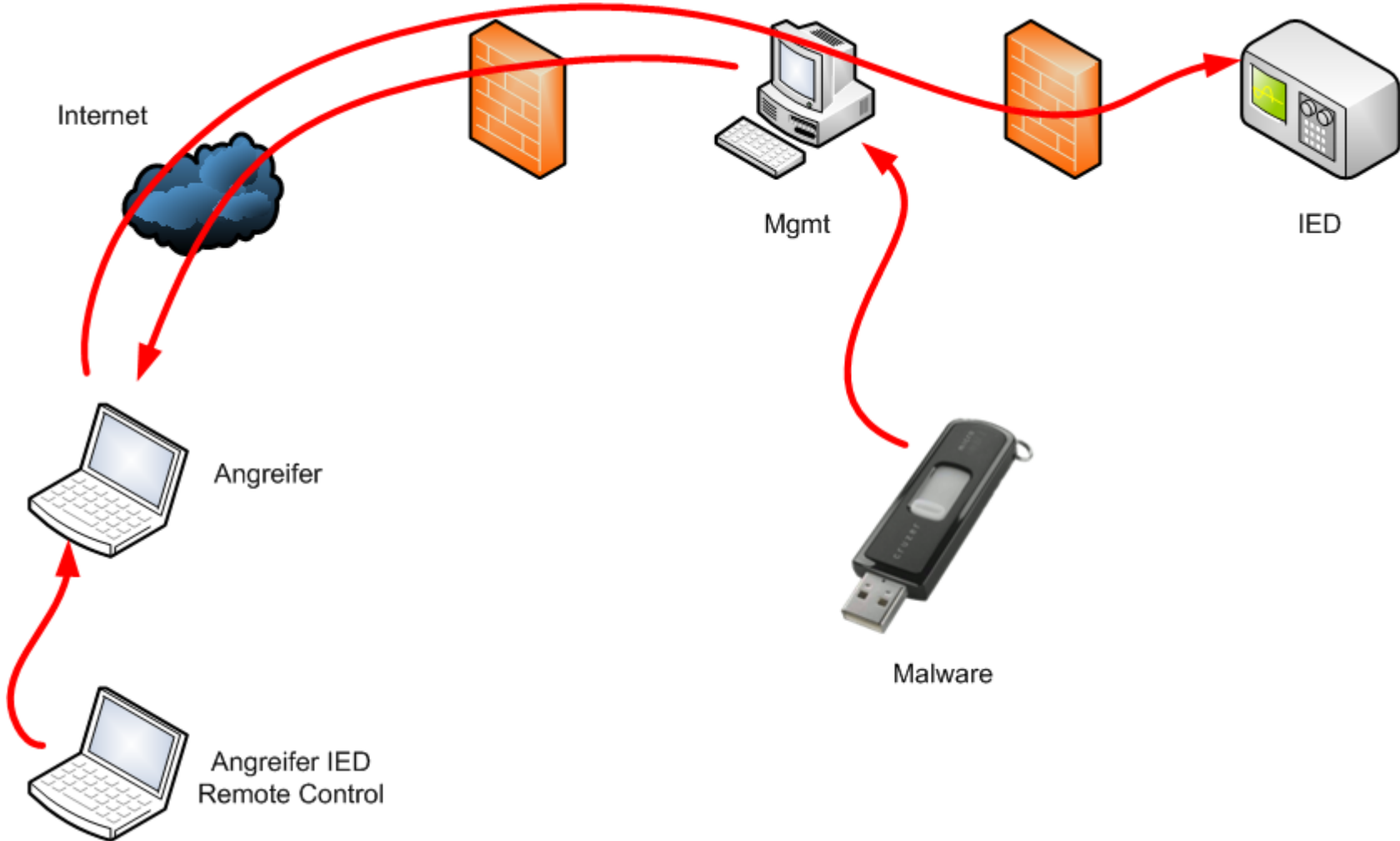
# Demo Setup



# Demo Setup



# Demo Setup





# Was, wenn doch?





# Verhaltensweisen von Angreifern

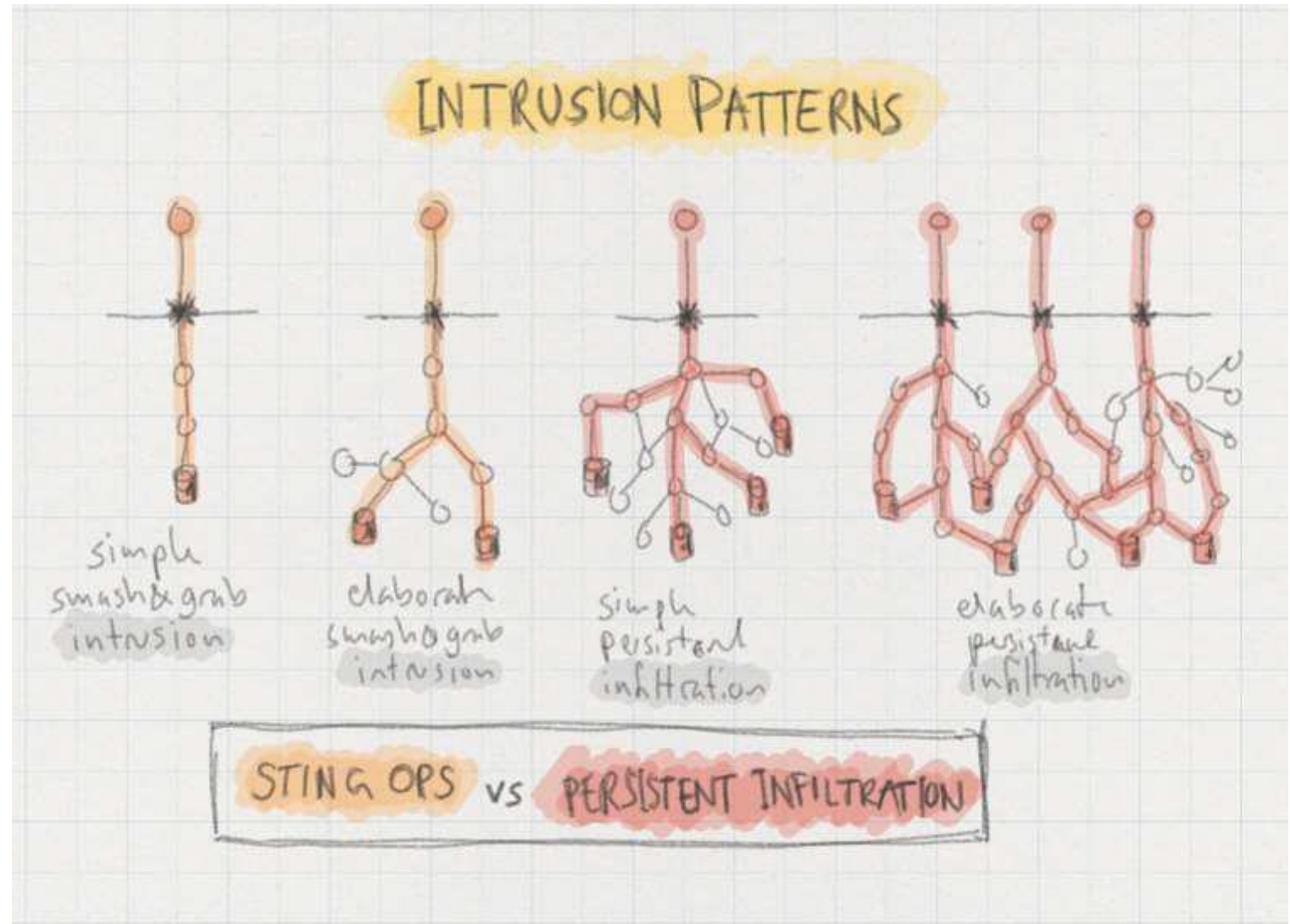
## Intrusion Patterns

### Sting Operation

Auch "smash and grab" genannt. Ein direkter Angriff, um an eine bestimmte Information zu gelangen bzw. eine Aktion auszuführen.

### Persistente Infiltration

Eine lang andauernde Kampagne, bei der sich Ihr Gegner über einen langen Zeitraum hinweg unbefugten Zugang zu Ihrer Infrastruktur verschafft und diesen aufrechterhält.



[Quelle]: <https://www.slideshare.net/FrodeHommedal/taking-the-attacker-eviction-red-pill>  
[https://www.youtube.com/watch?time\\_continue=3&v=WAvO0Y0nOws](https://www.youtube.com/watch?time_continue=3&v=WAvO0Y0nOws)

**Fix the Grid!**



# Grundschutz für «Operational Technology» in der Stromversorgung

## 2.6.1 Grundsätze der physischen Sicherheit

(11) ... Laptops, tragbare Parametrier- oder Fernwirk-PCs und Handhelds **müssen** streng gesichert und nicht ausserhalb des ICS-Netzwerks eingesetzt werden.

# Grundschutz für «Operational Technology» in der Stromversorgung

## 2.8.3 Fernzugriffe und Authentifizierung

(3) ... Die Zugriffe auf die Jump Stationen **muss** mittels Zweifaktor-Authentisierung erfolgen und jederzeit überwacht und kontrolliert werden. ...

alk:~\$ Vielen Dank für Ihre Aufmerksamkeit...

