# Digitalisierung und Cyber Security

## Learnings aus dem Blackout in der Ukraine

30. August 2022, Swissgrid Netzforum, Verkehrshaus Luzern

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

Kommt es zu einer Verkettung unglücklicher Umstände, ist eine

# Unterwerk (UW Mettlen)

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

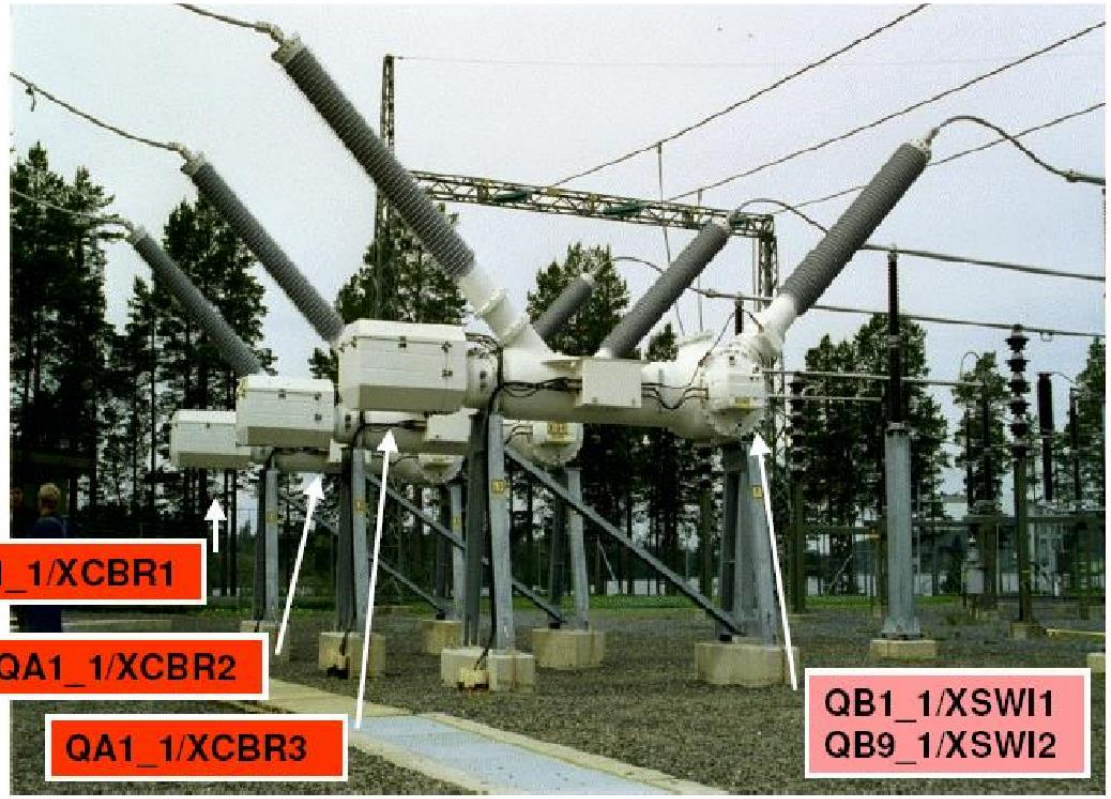
# Wie sicher ist unsere Stromversorgung ?

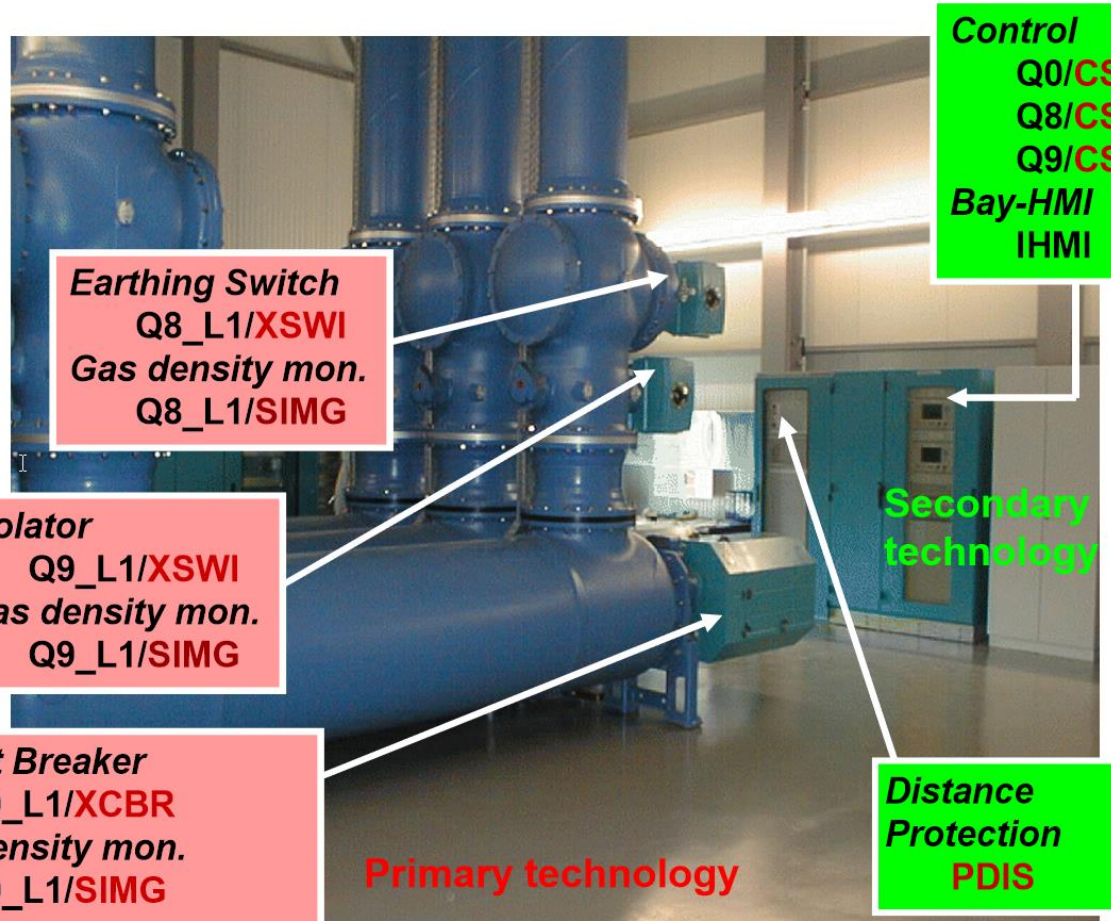
https://www.youtube.com/watch?v=UF5EDV6T7es

# 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

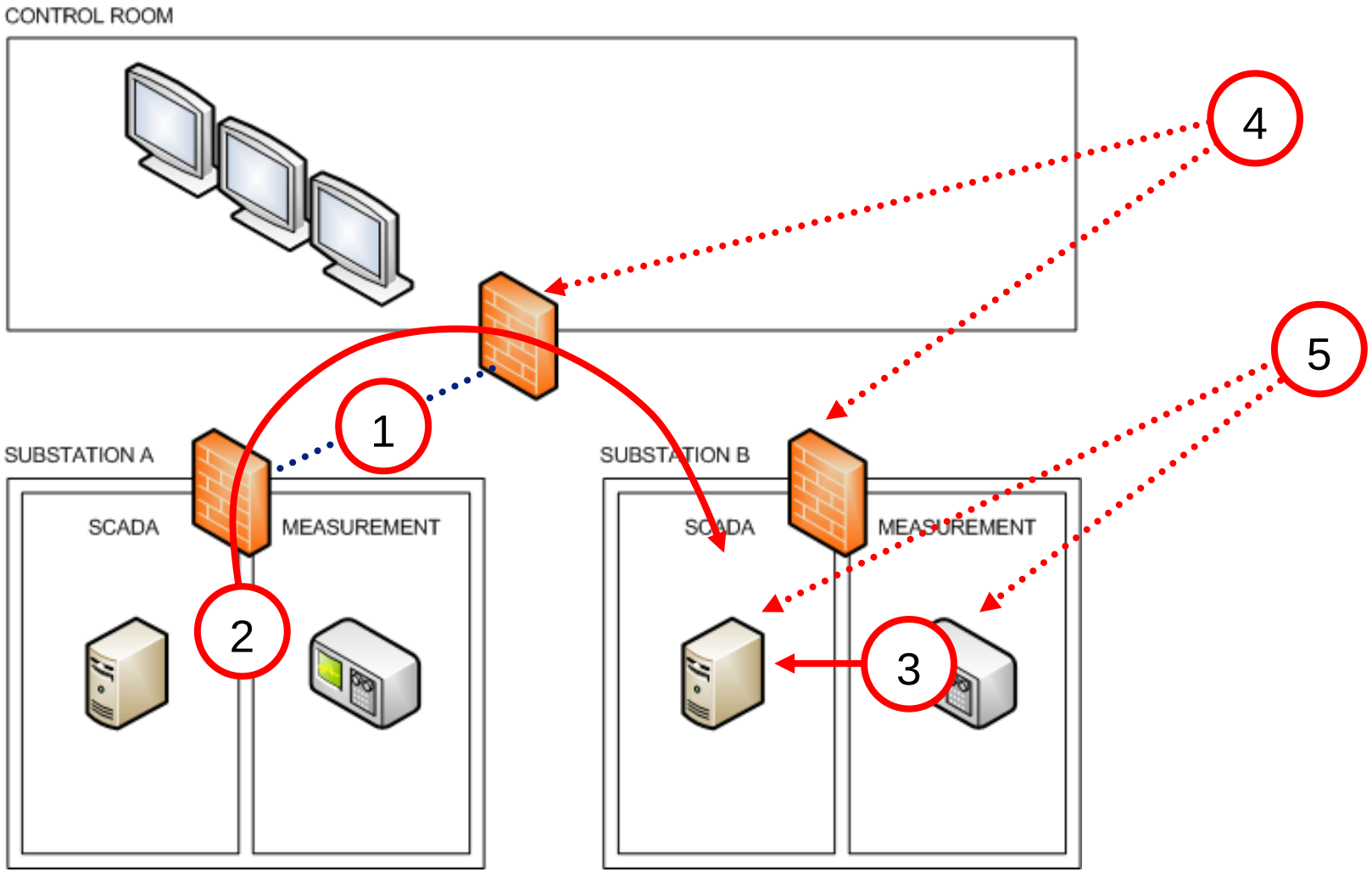
# Namensgebung mittels Objektmodel (IEC 61850 MMS)




ABB, Kirrmann, https://web.fe.up.pt/~asousa/sind/acetat/AI_EPFL/AI_421_IEC61850.pdf

# Angriffsszenarien gegen Unterwerke



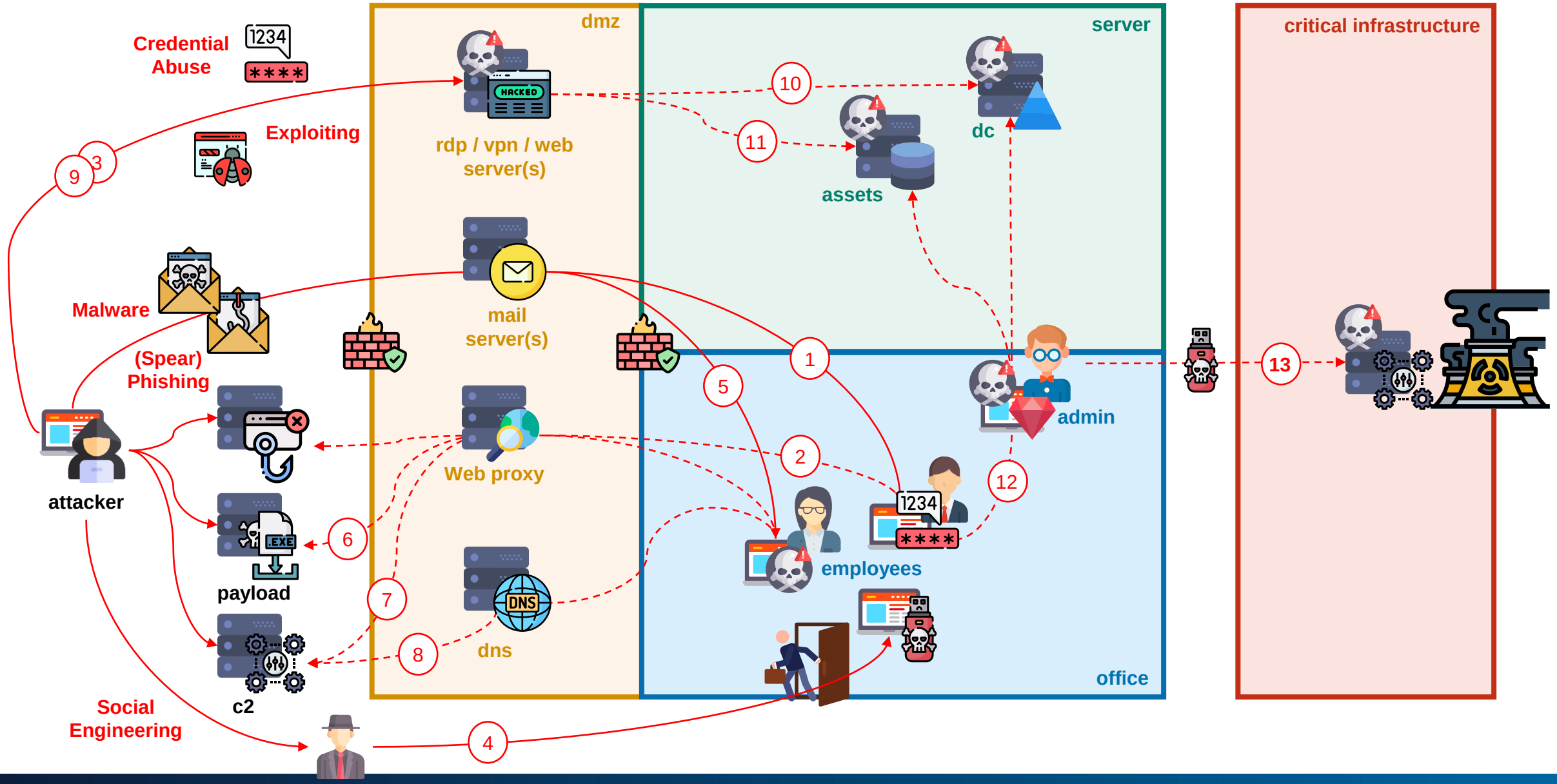
## Typische Einbruchsmuster

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)

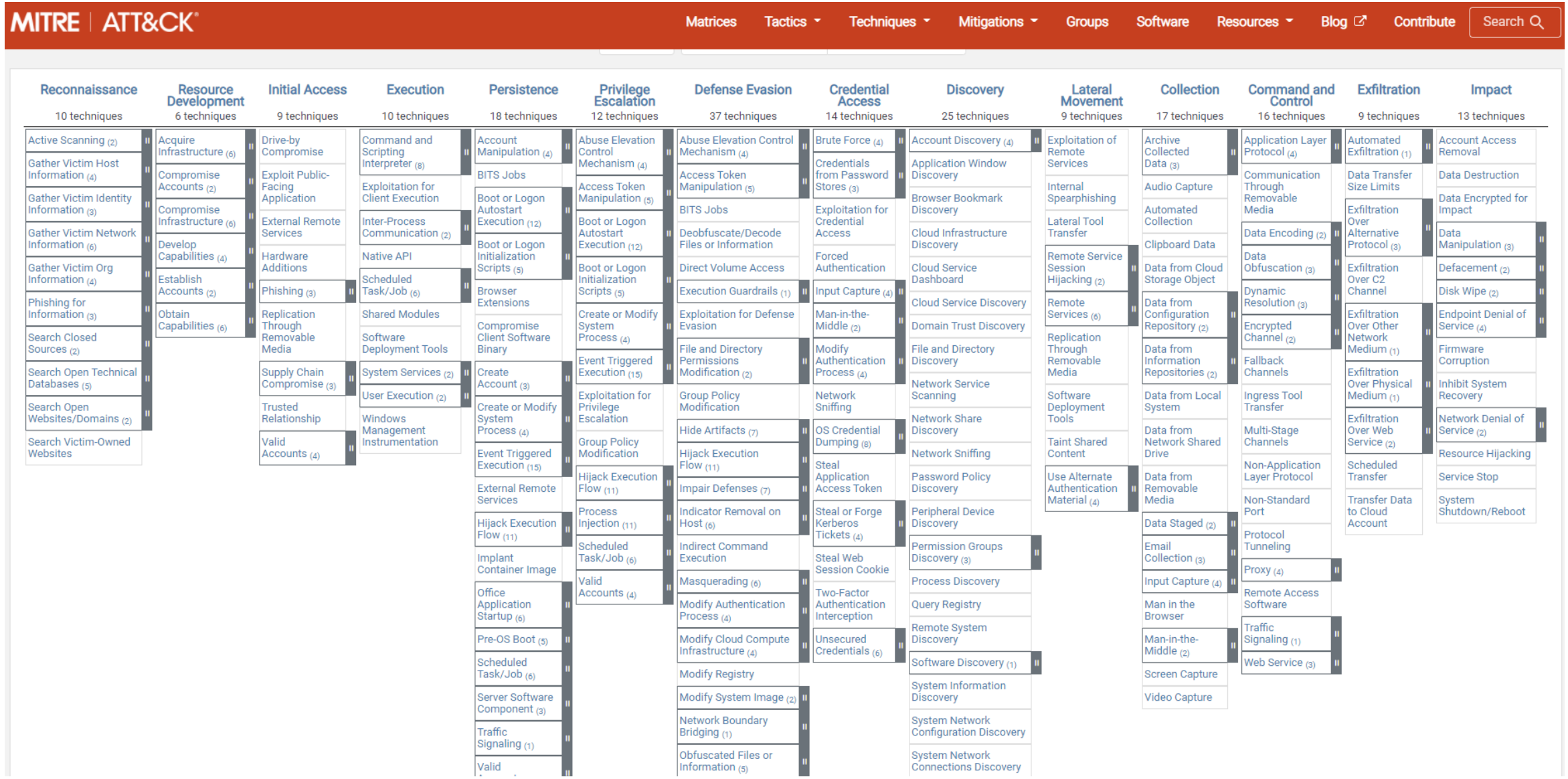
# Typische Einbruchsmuster



# Was bedeutet das im Detail?

MITRE ATT&CK Framework

# MITRE ATT&CK Framework



# 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 | Sandworm Team 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.<br><br>In October 2020, the US indicted six GRU Unit 74455 officers associated with Sandworm Team for the following cyber operations: the 2015 and 2016 attacks against Ukrainian electrical companies and government organizations, the 2017 worldwide NotPetya attack, targeting of the 2017 French presidential campaign, the 2018 Olympic Destroyer 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 APT28. |
| G0029 | Scarlet Mimic | | Scarlet Mimic is a threat group that has targeted minority rights activists. |

# Ukraine power cut 'was cyber-attack'

# Ukraine Hack

## Schritt 1

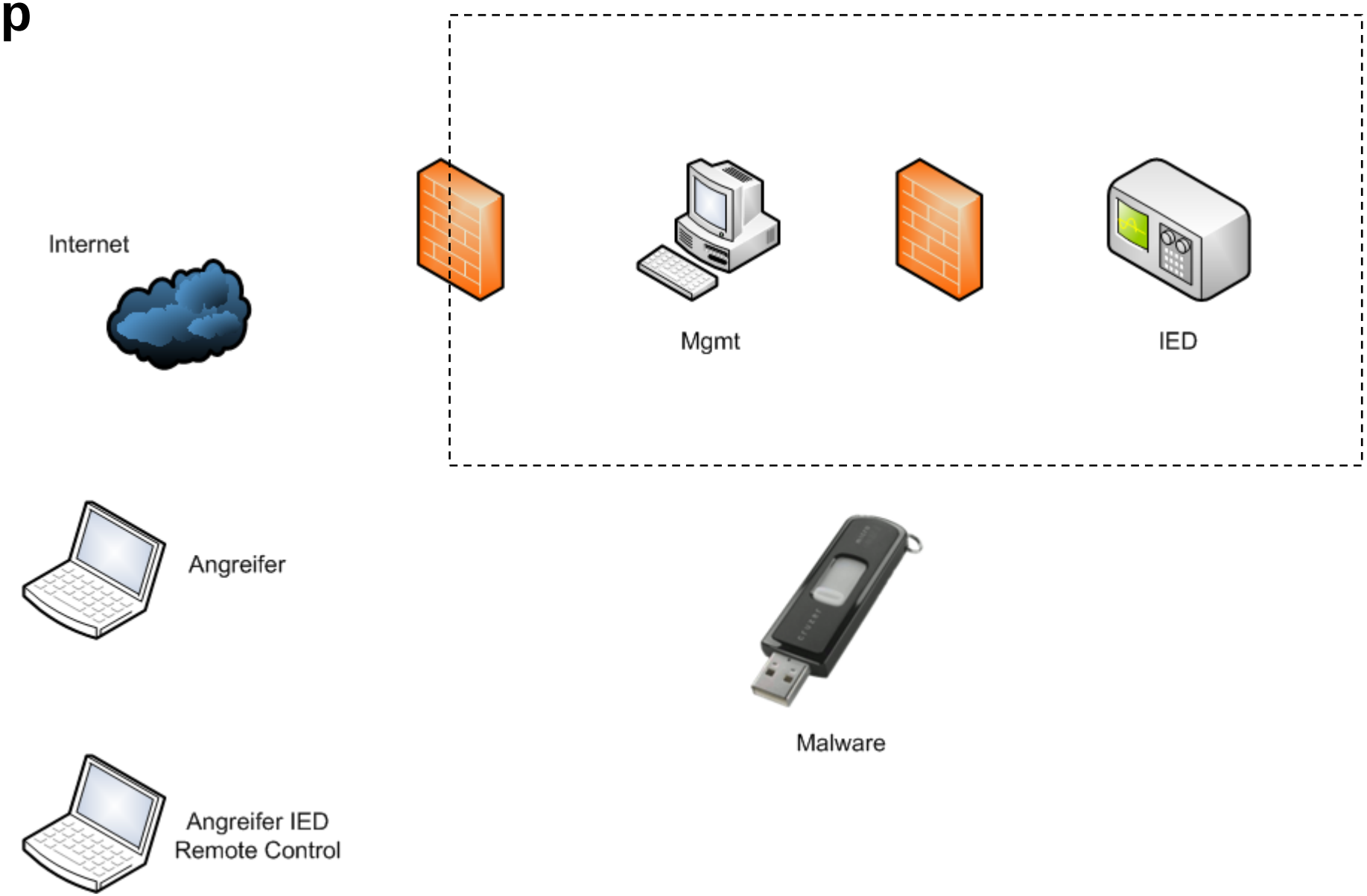
- Phishing E-Mails mit Word Macro, Black Energy Trojaner nachgeladen
- VPN Zugänge und Passwörter gestohlen
- Netzwerkanalyse und Lateral Movement

## Schritt 2

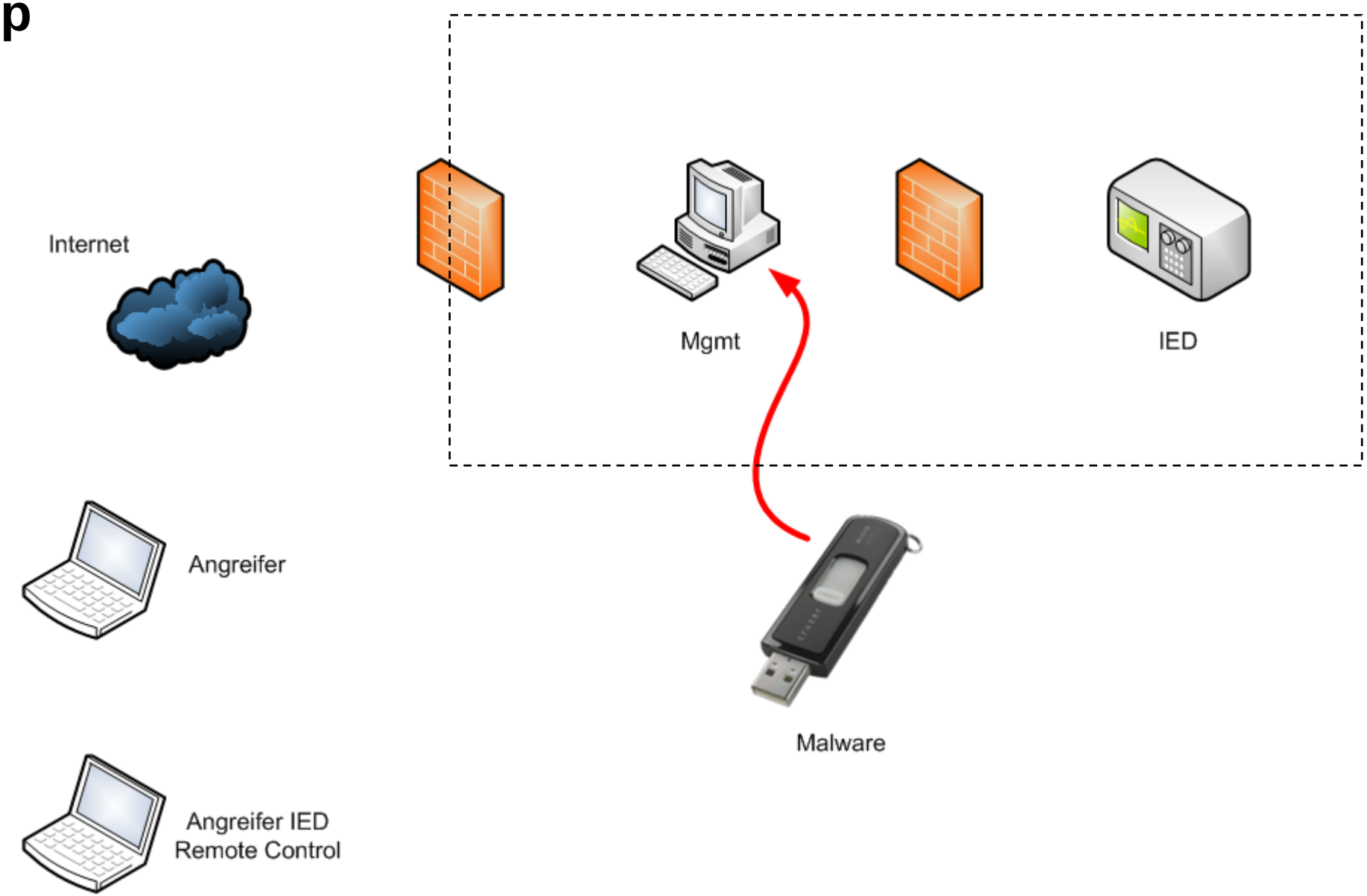
- Bösartige Firmware entwickelt
- SCADA Umgebung übernommen via Benutzeroberfläche
- Trennschalter geöffnet
- UPS Abschaltung orchestriert, Firmware auf Converter geladen, Logs und Disks gelöscht
- Telefonie Denial of Service

https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

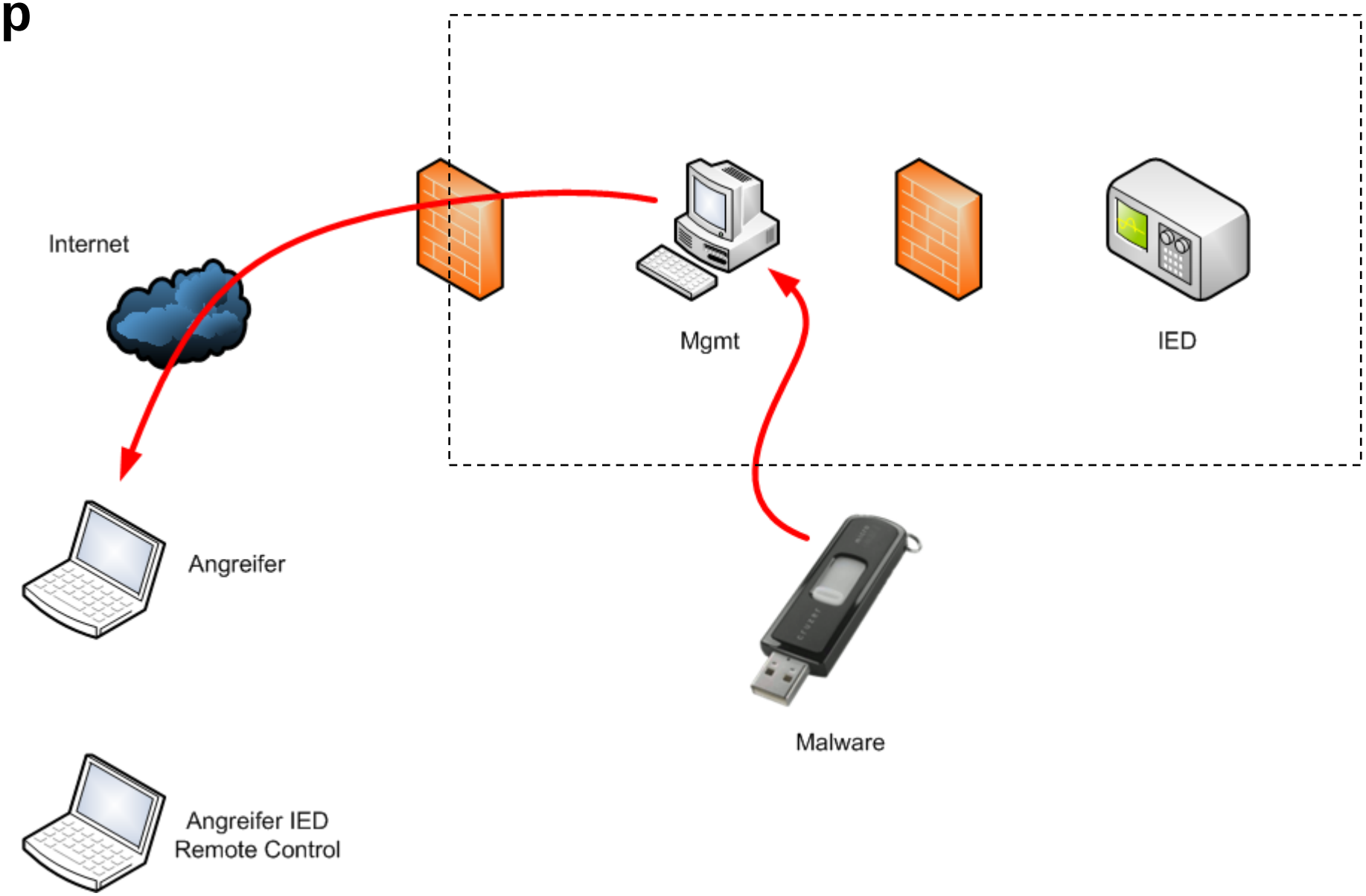
# Demo Setup


Internet
Mgmt
IED
Angreifer
Malware
Angreifer IED
Remote Control

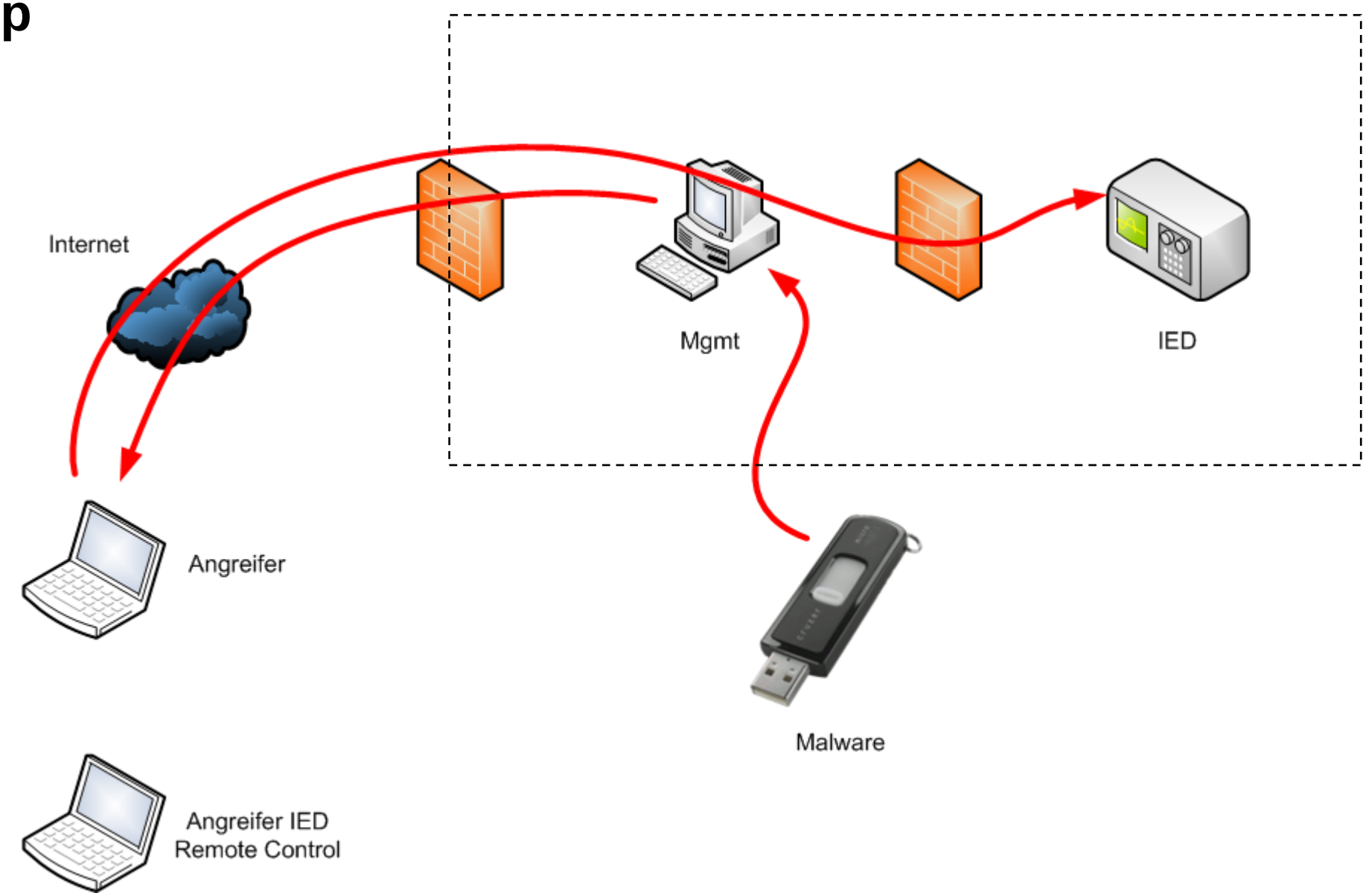
# Demo Setup


Internet
Mgmt
IED
Angreifer
Malware
Angreifer IED
Remote Control

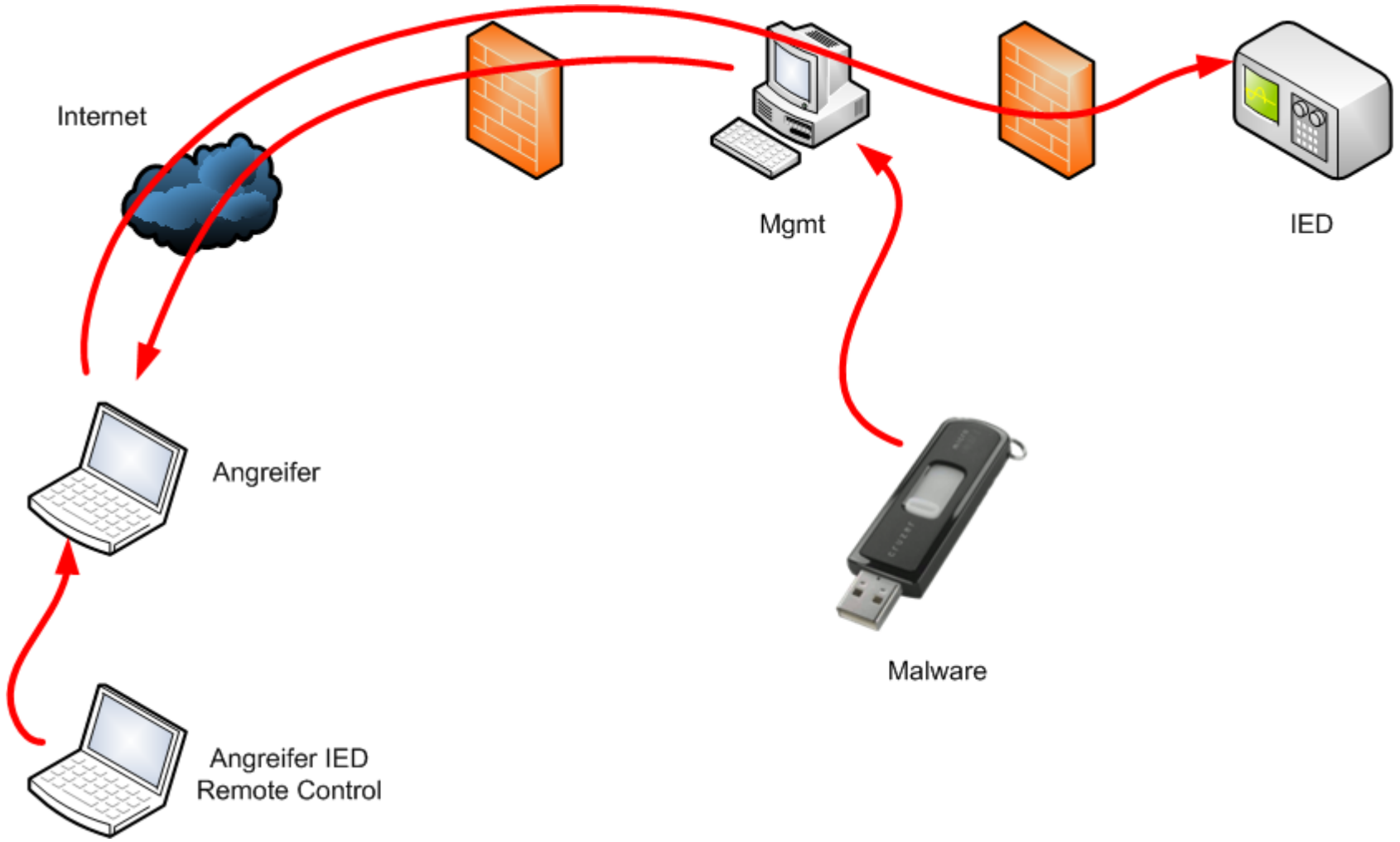
# Demo Setup


Internet
Mgmt
IED
Angreifer
Malware
Angreifer IED
Remote Control

# Demo Setup


Internet
Mgmt
IED
Angreifer
Malware
Angreifer IED
Remote Control

# Demo Setup


Internet
Mgmt
IED
Angreifer
Malware
Angreifer IED
Remote Control

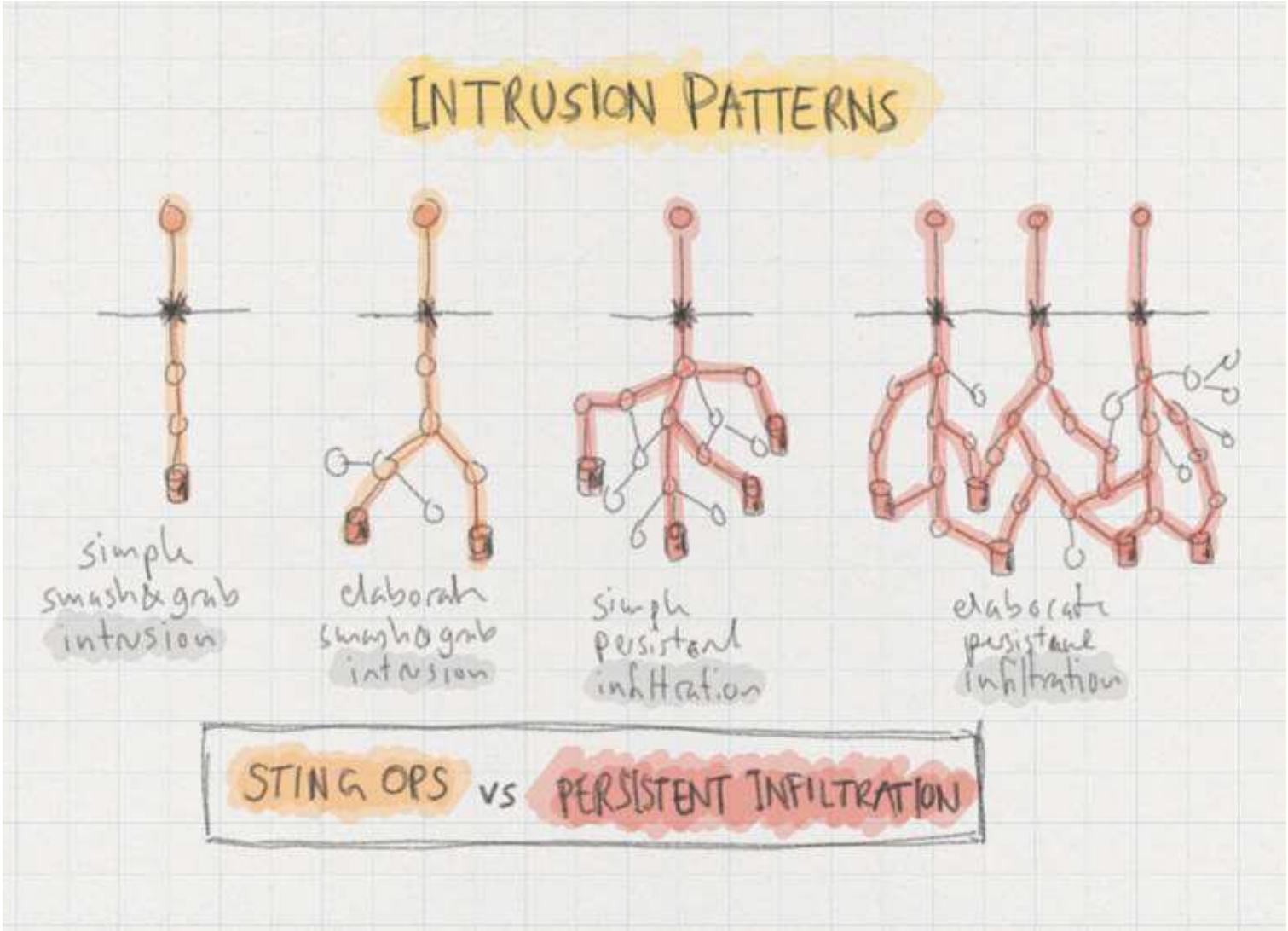
# Was, wenn doch?

# 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

# Fix the Grid !

# 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.

https://www.strom.ch/de/media/8302

# 2.8.3 Fernzugriffe und Authentifizierung

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

https://www.strom.ch/de/media/8302

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