Cyber Defense
Tag 2
25.9.24

Herzlich Willkommen zum zweiten Tag im Modul Cyber Defense

Pager Explosion

Advisory: Wir diskutieren die Explosion der Pager und wie das möglich war

(1

Theorie

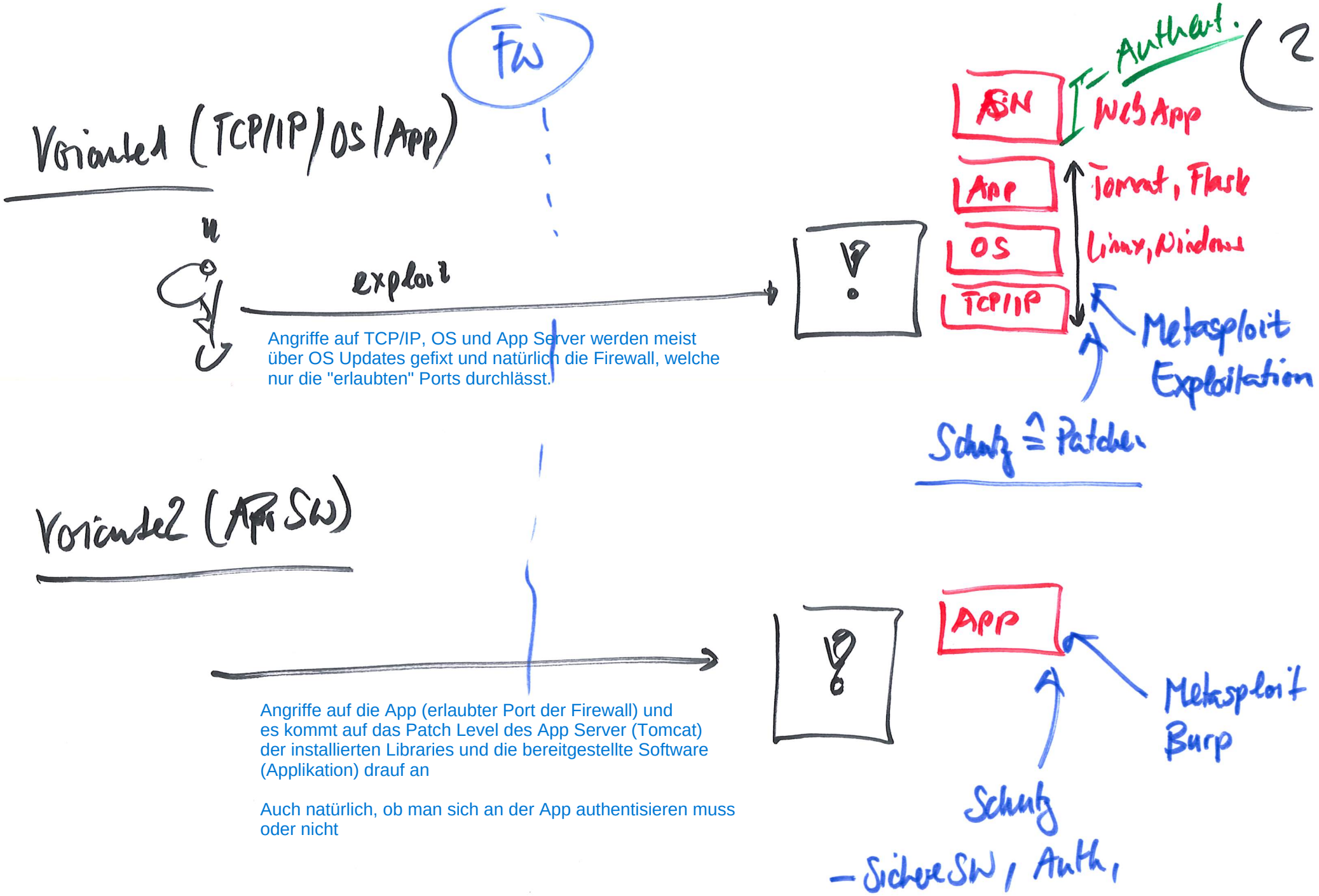
- Explosion von Batterie
- Supply Chain Attack → Sprengstoff im Gerät (+ Firmware Update)

Trigger für Explosion

- Funk → Firmware → Explosion
- Ohne zeitgesteuertes Trigger → fest konfiguriert im Firmware
- Funk → normale Batterie (Idle) erwärmen → ThermoGW → Explosion

Hersteller

- Warnung für Fälschung

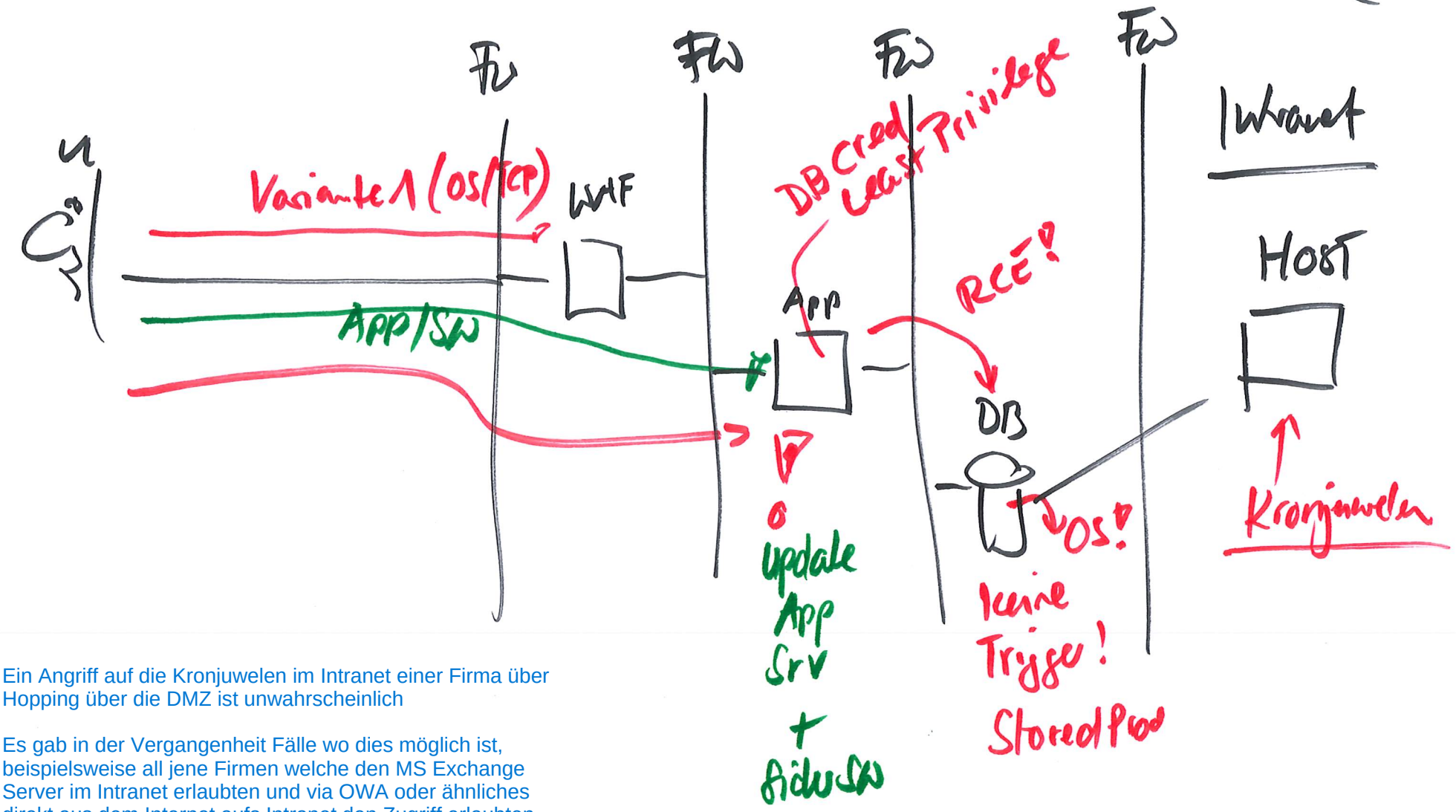


Angriffe auf TCP/IP, OS und App Server werden meist über OS Updates gefixt und natürlich die Firewall, welche nur die "erlaubten" Ports durchlässt.

Angriffe auf die App (erlaubter Port der Firewall) und es kommt auf das Patch Level des App Server (Tomcat) der installierten Libraries und die bereitgestellte Software (Applikation) drauf an

Auch natürlich, ob man sich an der App authentisieren muss oder nicht

(3

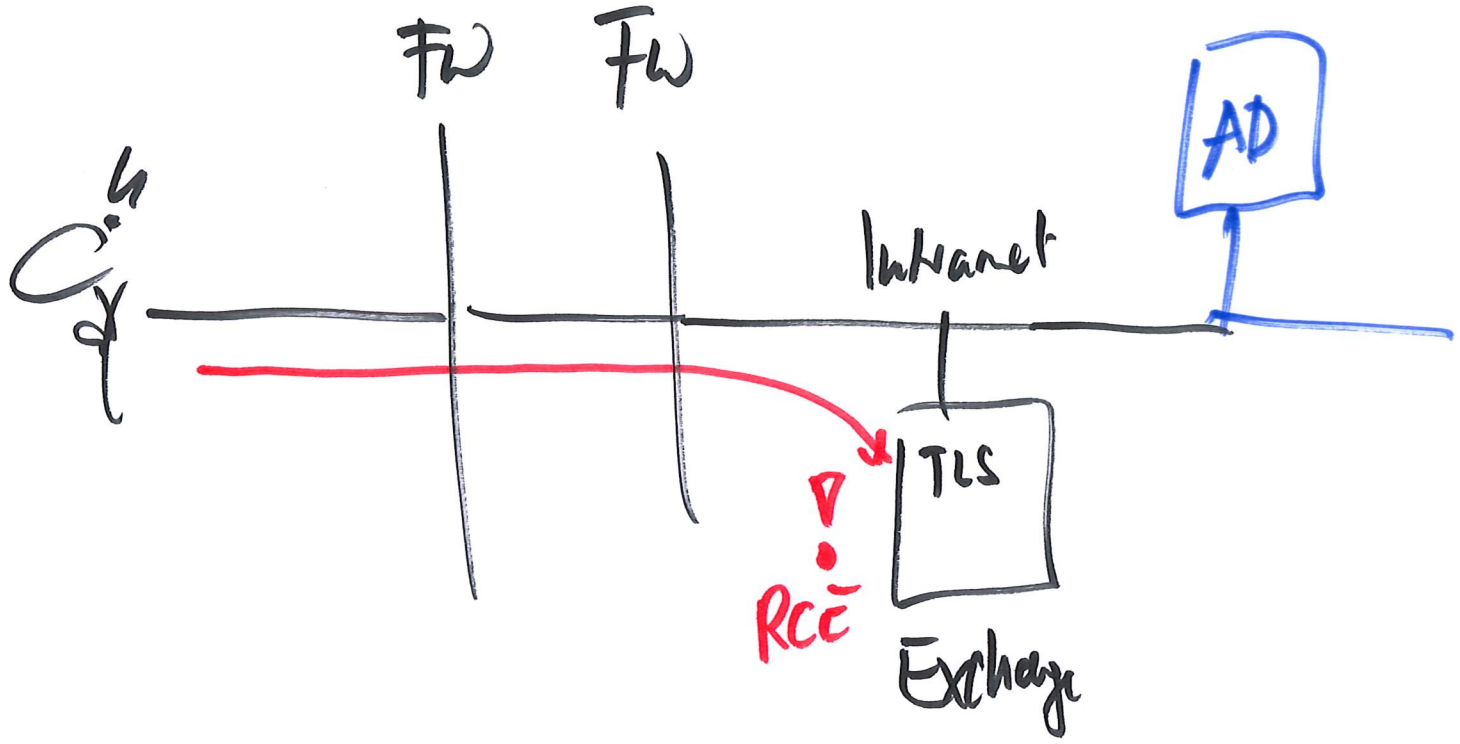


Ein Angriff auf die Kronjuwelen im Intranet einer Firma über Hopping über die DMZ ist unwahrscheinlich

Es gab in der Vergangenheit Fälle wo dies möglich ist, beispielsweise all jene Firmen welche den MS Exchange Server im Intranet erlaubten und via OWA oder ähnliches direkt aus dem Internet aufs Intranet den Zugriff erlaubten.,

Die DB Credentials von der App auf die DB sind wichtig, damit ein erfolgreicher Hacker auf dem App Server nicht ohne Probleme auf den DB Server weiter einbrechen kann.

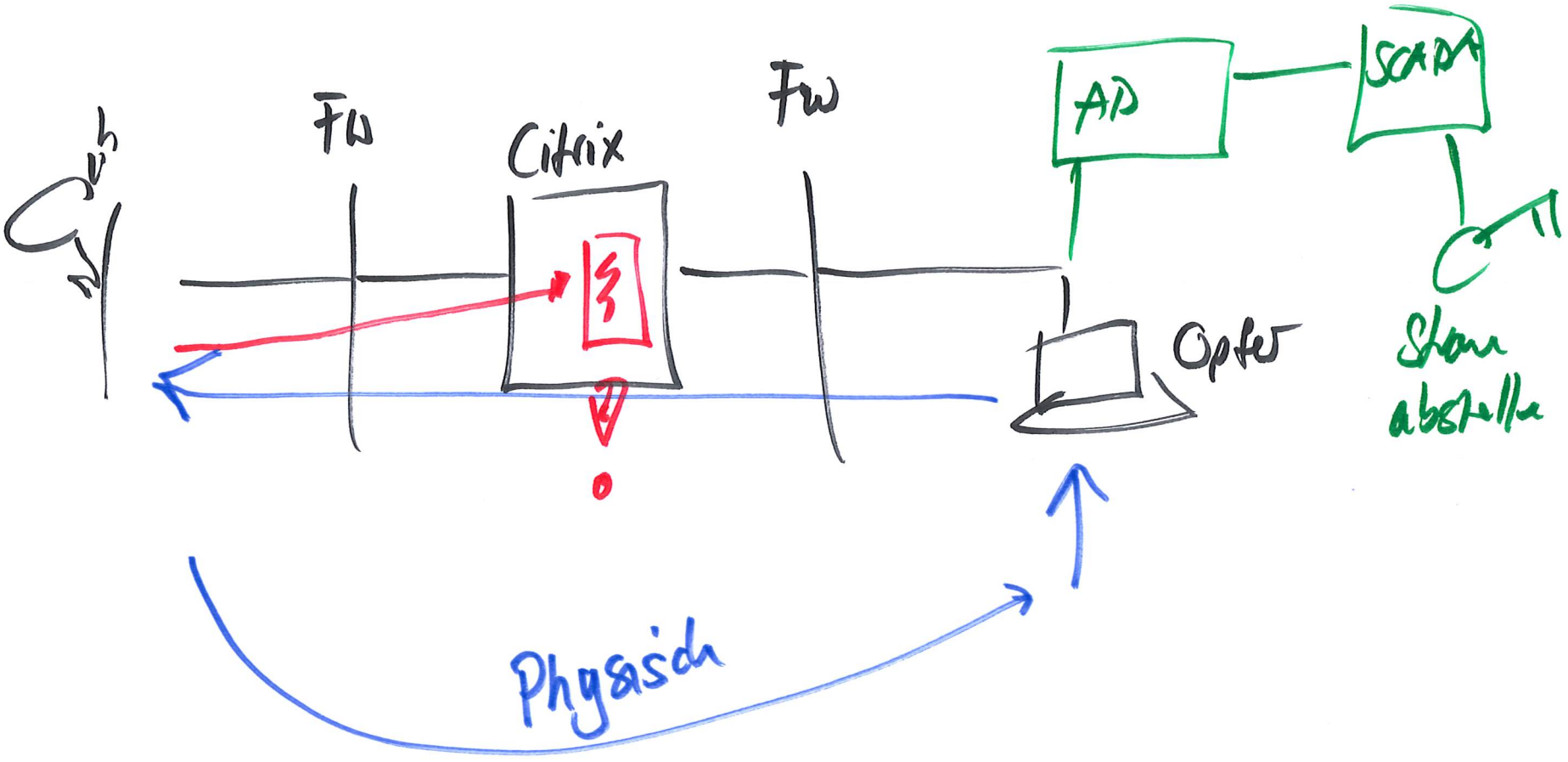
Exchange On-Prem Attack



Wie auf der Vorderseite angesprochen - so waren Firmen die ihren Exchange Server im Intranet hatten verwundbar auf RCE; welcher direkt im Intranet ausgeführt werden konnte.

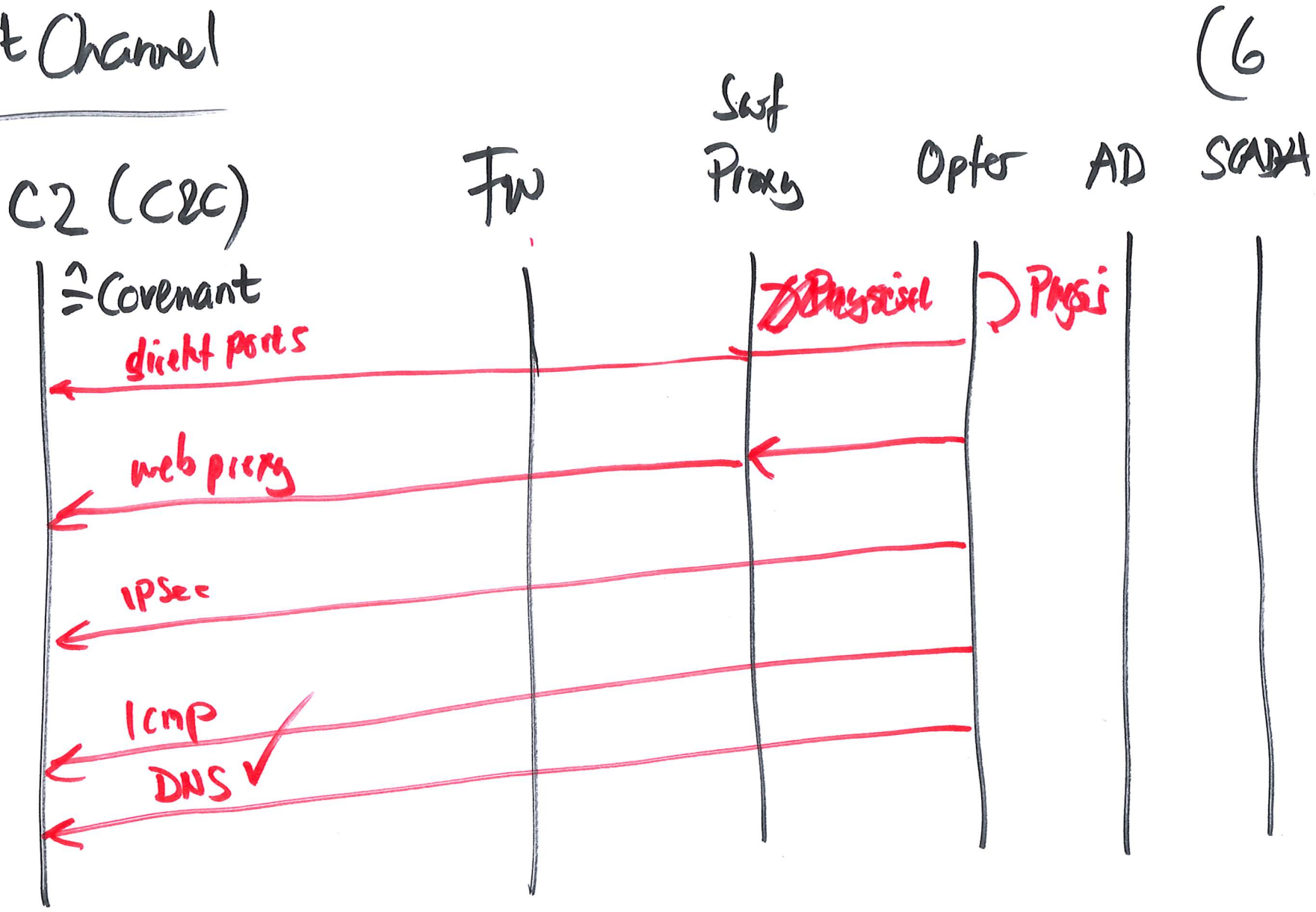
Das sollte man falls immer möglich nie tun. Services die vom Internet her aufgerufen werden können gehören in eine DMZ

Citrix Secure



Hier diskutieren wir den Angriff mittels Viren und Trojaner. Unternehmen die ihre Mitarbeiter den Browser in einer Citrix oder ähnlichen Remote Desktop Lösung bedienen lassen sind besser geschützt vor Viren und Trojanern, weil dieser ja dann auf der Citrix (DMZ) gestartet wird (eine Zone die man im schlimmsten Fall auch verlieren kann, daher heisst diese ja auch DMZ)

Covert Channel



Wir diskutieren welche Verbindungswege es von einem Computer im Intranet ins Internet gibt. Falls einer von diesen Protokollen funktioniert, dann kann ein Trojaner eine Reverse Shell oder eine Verbindung zum C2 aufnehmen - was die Grundlage für Ransomware und viele weiteren Attacken darstellt.

Wir müssen also bei der Cyber Defense darauf schauen, dass wir solchen Traffic erkennen können (mit einer gewissen Wahrscheinlichkeit