FIREWALLING MS EXCHANGE

Mark Semmler

DIE GRÖßTE VERWUNDBARKEIT IST DIE UNWISSENHEIT.

Sunzi

chinesischer General um 544 - 496 v. Chr.,
Militärstratege und Philosoph,
bekanntestes Werk: Die Kunst des Krieges

- PROBLEM -

MICROSOFT: EXCHANGE + FIREWALL = DESASTER!

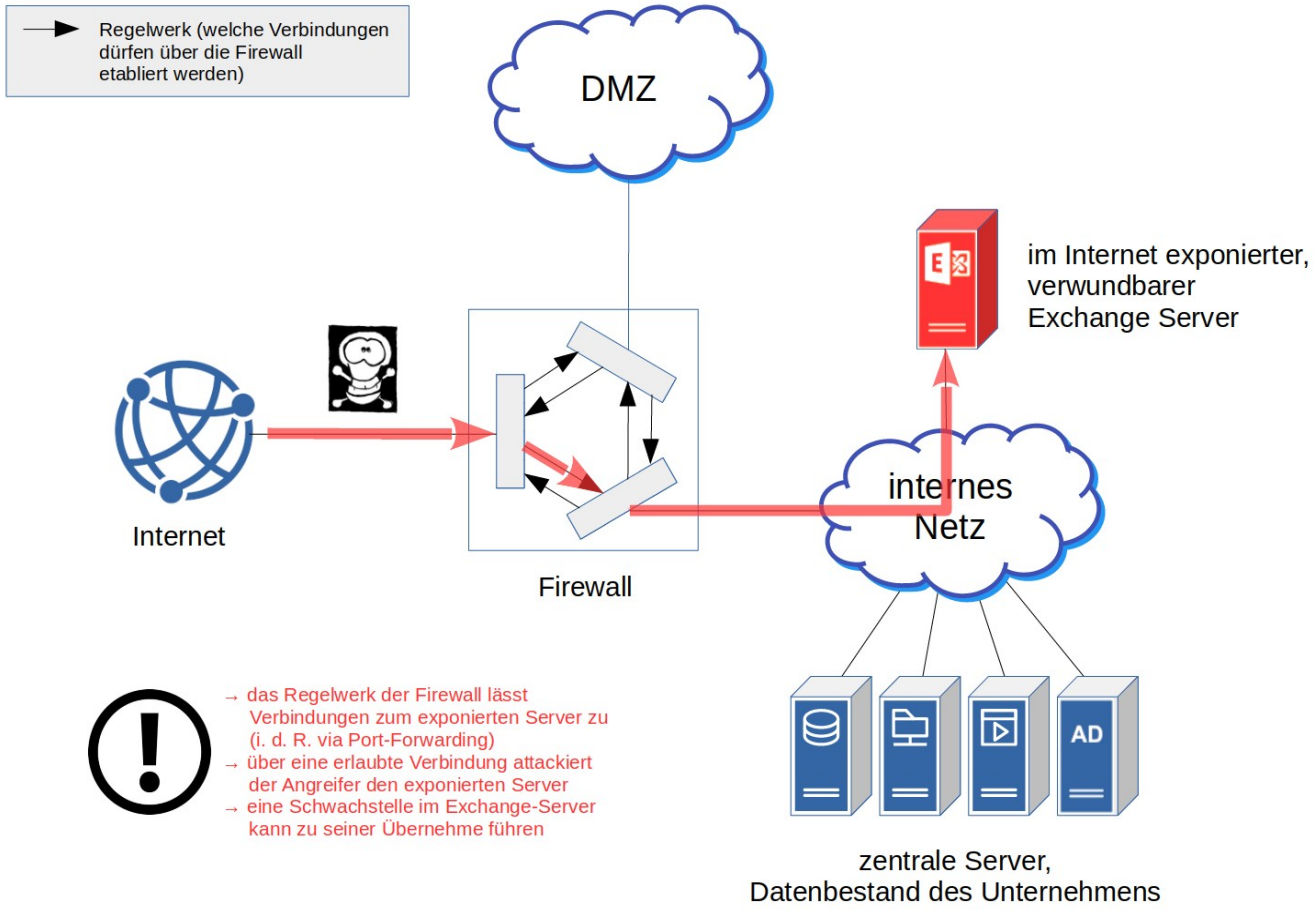
- Microsoft stellt in einem offiziellen Dokument klar, dass ein MS Exchange Server nicht in einer DMZ untergebracht werden kann:
  - “We do not support restricting or altering network traffic between internal Exchange servers, between (...) internal Exchange servers and internal Active Directory domain controllers in any and all types of topologies.
    If you have firewalls or network devices that could potentially restrict or alter this kind of internal network traffic, you need to configure rules that allow free and unrestricted communication between these servers: rules that allow incoming and outgoing network traffic on any port (including random RPC ports) and any protocol that never alter bits on the wire.“

    Quelle: Website von Microsoft (Link)

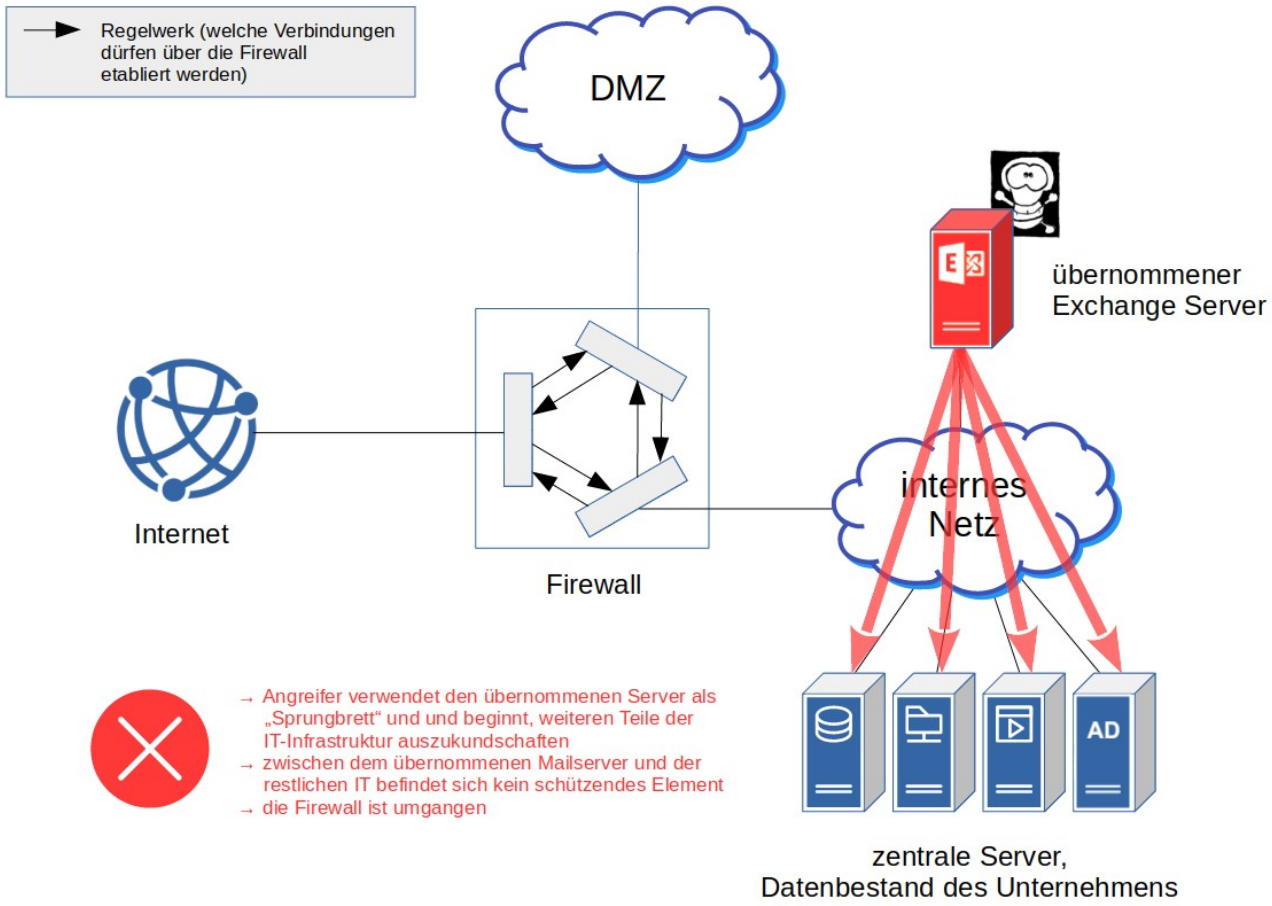
EXCHANGE WIRD ZUR SCHWACHSTELLE

- Damit der Exchange Server problemlos arbeiten kann wird er im internen Netz platziert (eben in direkter Nachbarschaft zum AD Server).
- Damit er aus dem Internet erreichbar ist, wird er (i. d. R. via Port-Forwarding) exponiert.
- Das Exponieren eines internen Servers im Internet ist immer eine schwerwiegende Schwachstelle und sollte UNBEDINGT vermieden werden.

FALSCH POSITIONIERTE (EXCHANGE-)SERVER...



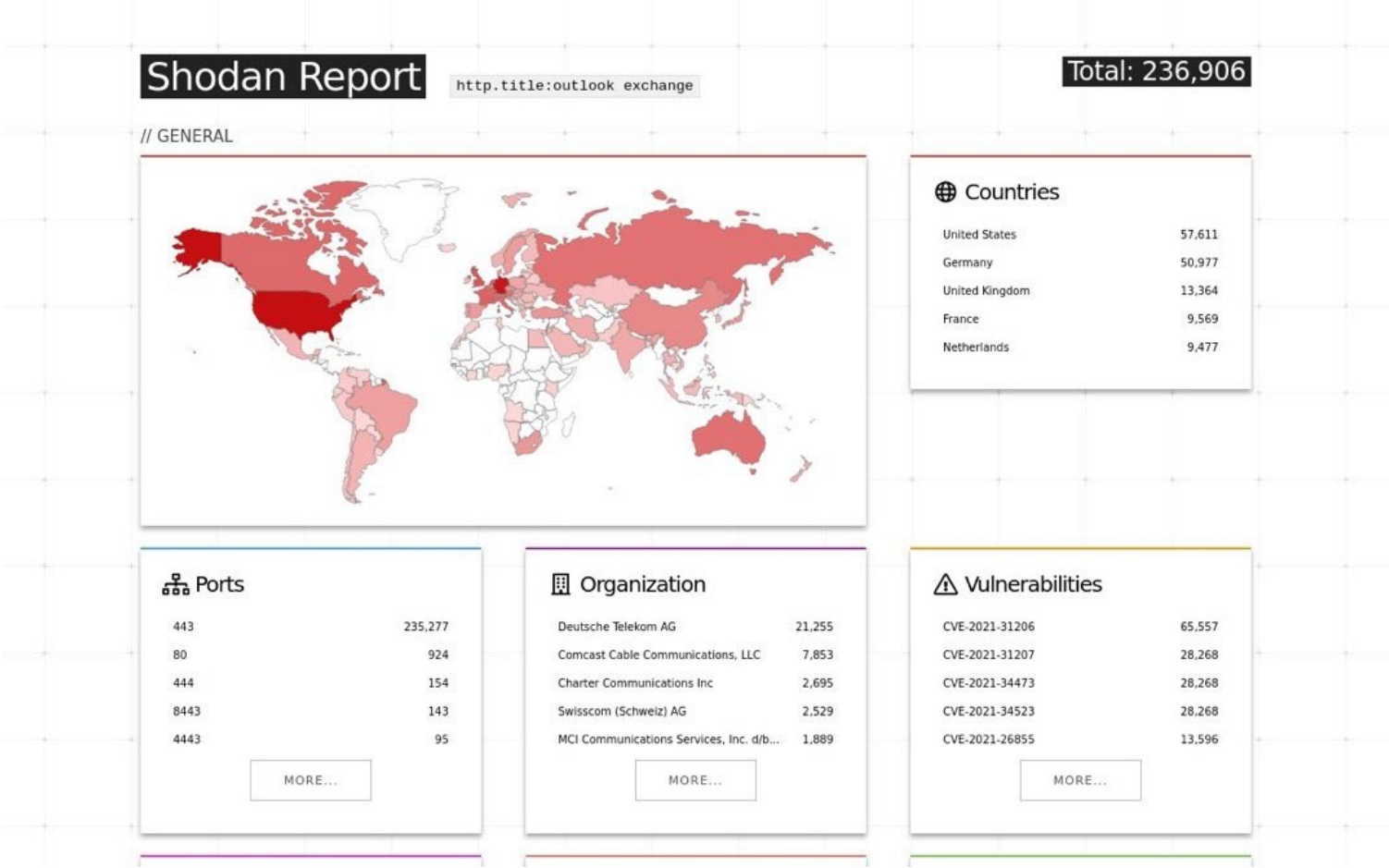
...KÖNNEN EINE MENGE ÄRGER BEDEUTEN!



EXCHANGE = ÄRGER? DA WAR DOCH WAS...

- Ein Mitarbeiter des Consulting-Unternehmens DEVCORE entdeckte im Dezember 2020 und im Januar 2021 zwei Sicherheitslücken in MS Exchange. Die Schwachstellen wurden von ihren Entdeckern „ProxyShell“ getauft und ermöglichten es in Kombination, Exchange Server aus der Ferne zu übernehmen.
- Die Schwachstellen wurden Microsoft im Januar 2021 mitgeteilt. Microsoft entwickelte entsprechende Patches und plante, diese im Zuge der monatlichen regulären Updates am 09.03.3021 auszurollen. Das Unternehmen entschloss sich dann kurzfristig, die Patches außerplanmäßig bereits am 03.03.2021 mitsamt einer eindringlichen Sicherheitswarnung zu veröffentlichen, da die Sicherheitslücken offenbar bereits aktiv ausgenutzt wurden.
- Eine mutmaßlich staatsnahe, aus China operierende Gruppe namens Hafnium nutzte ab dem 03.03.2021 ProxyShell, um eine großangelegte Angriffswelle durchzuführen. Die Gruppe suchte automatisiert nach verwundbaren Exchange Servern, nutze die Schwachstellen aus und platzierte auf ihnen ein Programm, mit dem die betroffenen Server jederzeit (also auch nach dem Einspielen der Updates) von ihnen ferngesteuert werden konnten („Backdoors“). Hafnium nutzte hierfür eine seit dem Jahr 2011 bekannte Backdoor die unter dem Namen „China Chopper Web Shell“ bekannt ist.
- Die platzierten Hintertüren wurden in den folgenden Tagen wiederum von verschiedenen Ransomware-Gruppen zielgerichtet gesucht und von diesen für eigene Zwecke verwendet.

RICHTIG! DA. WAR. WAS. HEFTIGES!

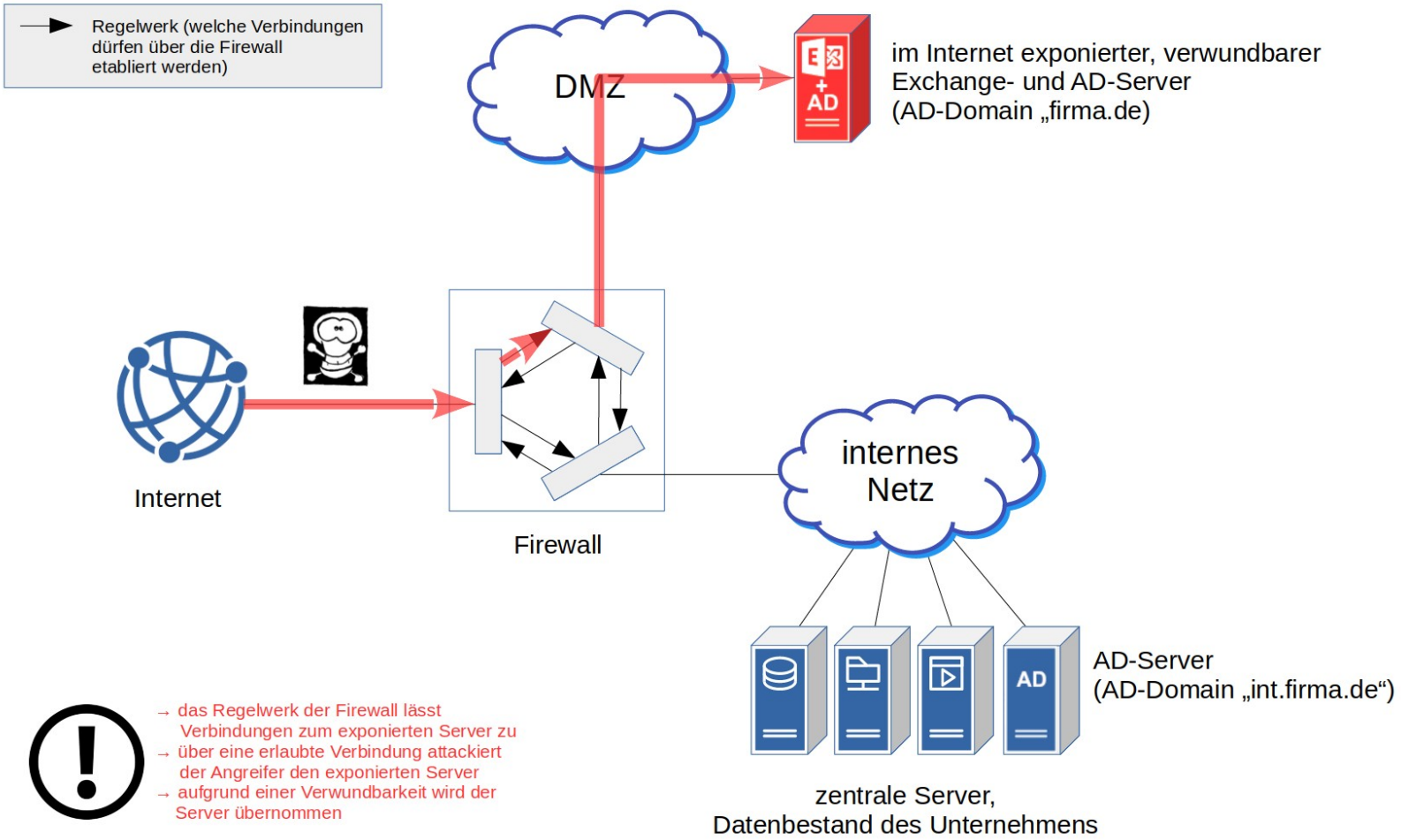


- LÖSUNG -

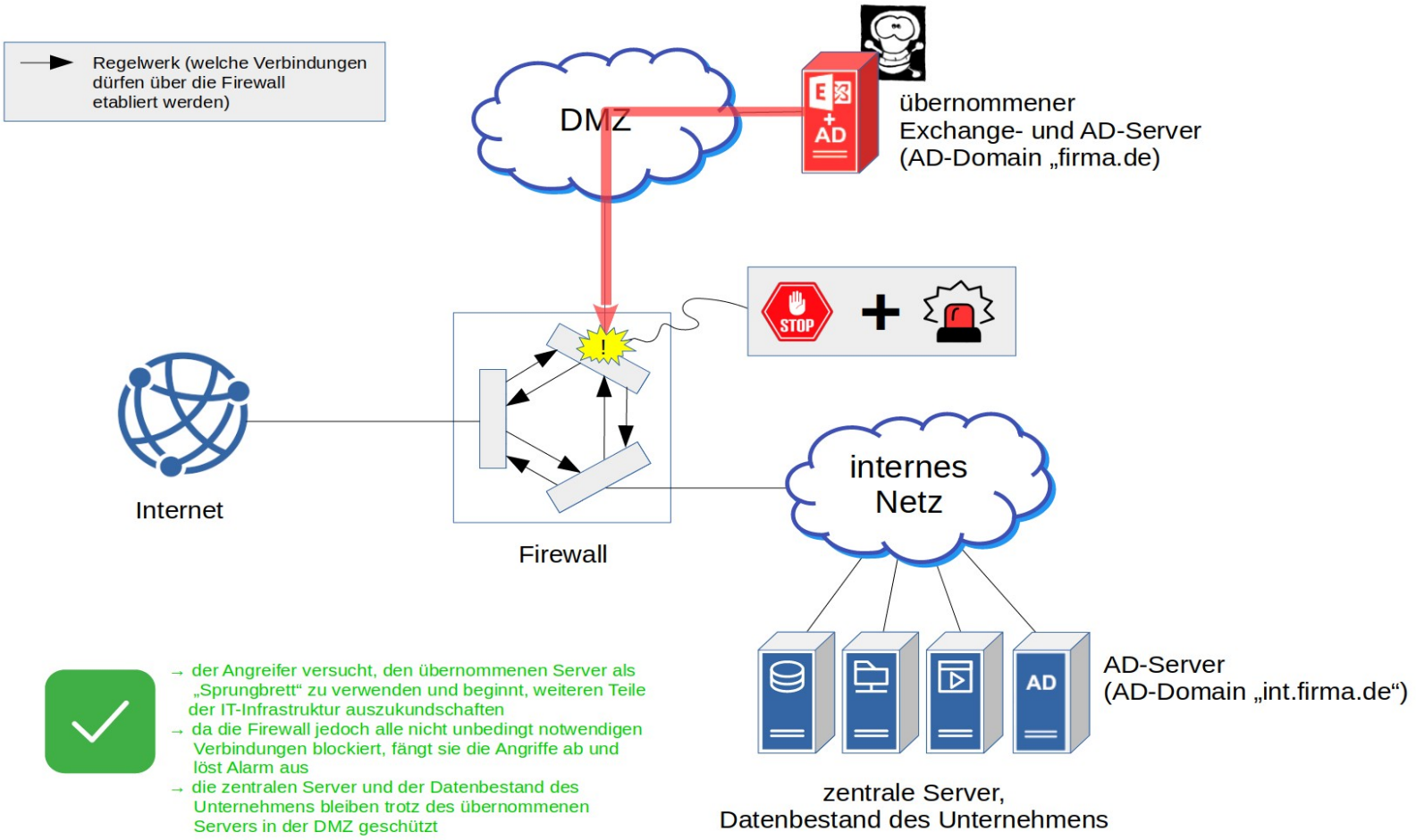
BETREIBEN SIE ZWEI UNABHÄNGIGE AD-SERVER

- Etablieren Sie eine zweite AD-Domain auf einem eigenen AD-Server.
- Platzieren Sie den zweiten AD-Server zusammen mit dem Exchange-Server in der DMZ (beide Dienste können z. B. auf dem gleichen IT-System untergebracht werden).
- Die zweite Domain beinhaltet alle Mail-Accounts des Unternehmens (<account>@firma.de) und ist von der eigentlichen AD-Domain komplett unabhängig (keine Vertrauensstellung o. ä.).

EXCHANGE + EIGENER AD-SERVER IN DER DMZ...



...SCHÜTZT DAS INTERNE NETZ

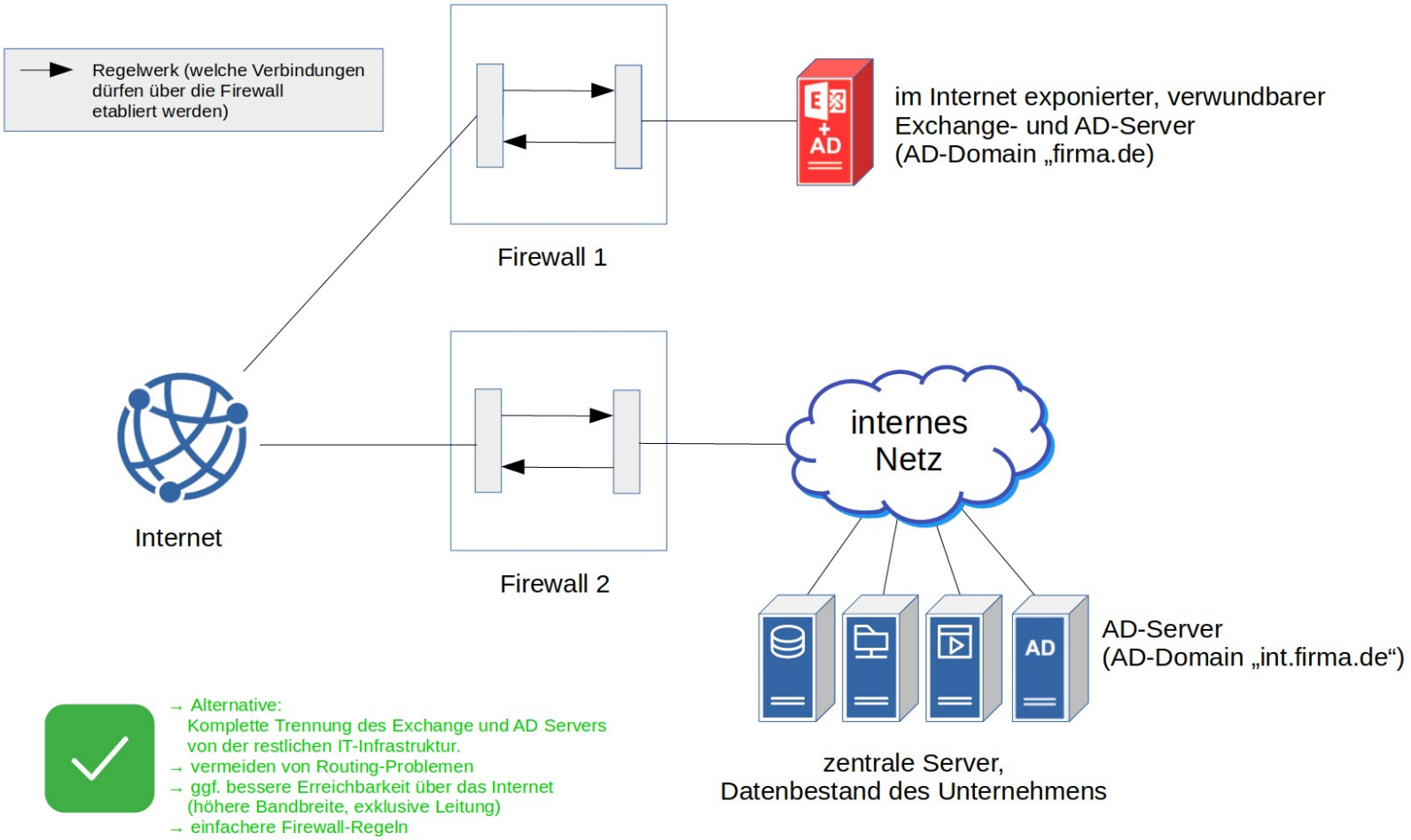


NACHTEILE DER LÖSUNG

- Erhöhter Installationsaufwand
  - Zusätzlicher AD-Server sowie Umzug des Exchange Servers in die DMZ.
  - Zusätzliche Regeln in der Firewall.
    - Internet → Exchange Server (Mail-Zustellung, Client-Access, ...)
    - internes Netz → Exchange Server (Mail-Zustellung, Client-Access, ...)
    - Exchange Server → Internet (ausgehende Mails, Updates, ...)
    - ~~Exchange Server → internes Netz~~ (Bitte nicht – das wollten wir doch gerade vermeiden!)
- Erhöhter Pflegeaufwand
  - Zusätzlicher AD-Server.
    - Updates
    - Monitoring
    - ...
  - Zusätzliche AD Domain.
    - Accounts
    - Passwörter
    - Monitoring
    - ...

- ALTERNATIVE -

KOMPLETTE TRENNUNG KANN VORTEILE BRINGEN



VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

-

FEEDBACK WILLKOMMEN!

MEINE KONTAKTDATEN

- Telefon: +49 163 732 74 75
- Mail: sicherheit [at] mark [minus] semmler [dot] de
- IM: Threema (ID: VTH4PXRW), Signal, Wire, Telegram
- Web: https://www.mark-semmler.de