

IT-Sicherheits-Studie

Zugang Externer Mitarbeiter zu Cloud-basiertem Austausch System
für NGOs (Non-Governmental Organisation)



System Situation externe Mitarbeiter und NGO

Domäne Fremd

Domäne NGO

Offenes Internet
(Private Netzwerke)

NGO Organisation
Netzwerk

NGO Firewall

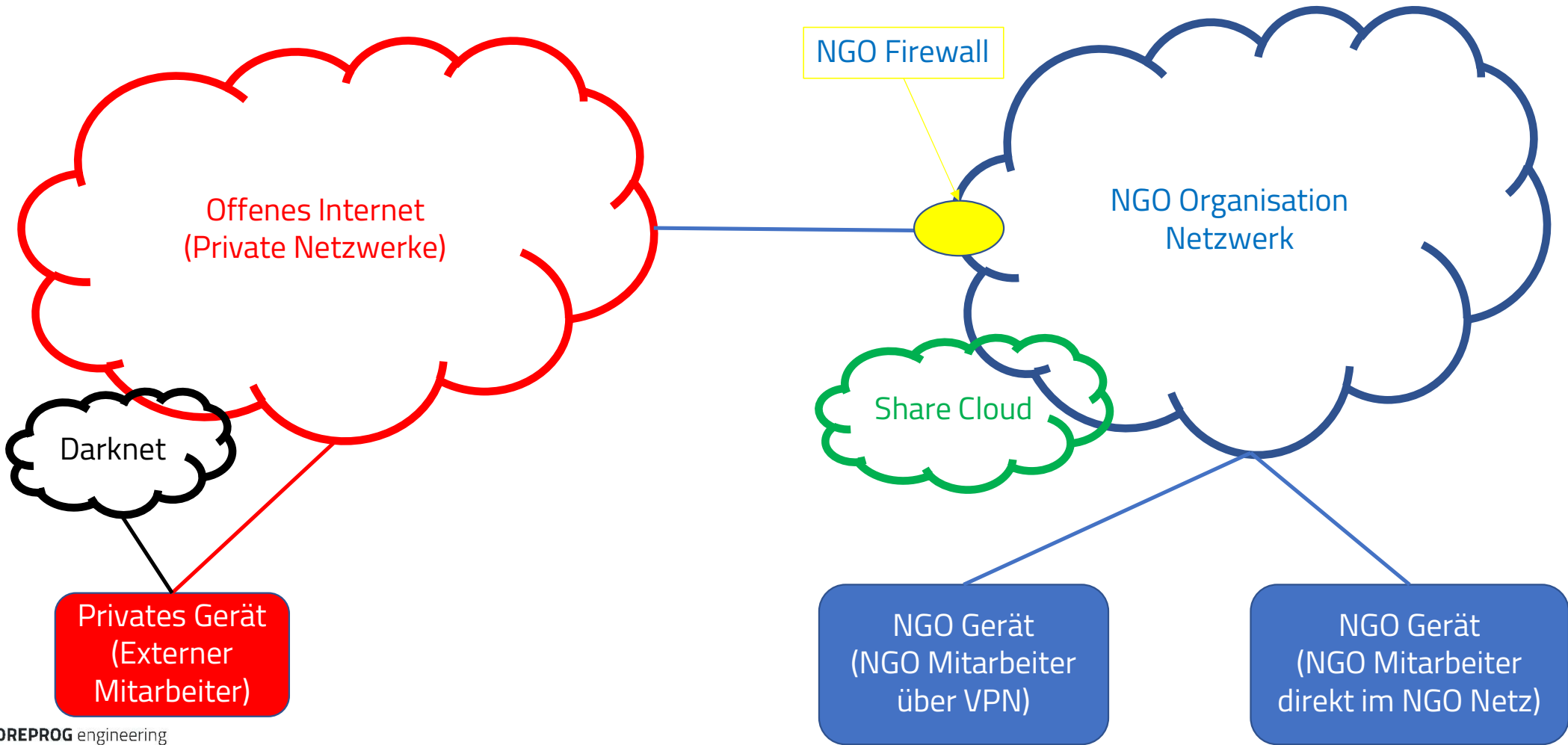
Share Cloud

Darknet

Privates Gerät
(Externer
Mitarbeiter)

NGO Gerät
(NGO Mitarbeiter
über VPN)

NGO Gerät
(NGO Mitarbeiter
direkt im NGO Netz)



Gefahren Situation

- Fremd Geräte
 - externer Mitarbeiter können nicht zertifiziert werden
 - werden nicht nur durch externe Mitarbeiter benutzt, z.B. auch durch Kinder des Mitarbeiters
 - haben unzureichenden Schutz
 - können absichtlich oder unabsichtlich Malware mitbringen
- Passive Malware (Skripting) kann sich über Standard-Kopiervorgänge (z.B. Verzeichnis-Kopie oder ZIP-Datei) im Netz von NGO verbreiten, z.B. bei automatischer Synchronisation lokaler Cloud-Caches
- Ein Trigger (z.B. über präparierte Internetseite, Werbung oder Email) kann die passive Malware aktivieren, was zu weiterer Installation von Ransomware, Botnetz, etc. führen kann



Technische Problem Definition

Privates
gerät

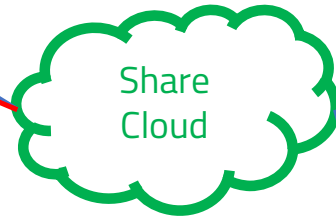
HTTPS Zugriff über Browser ist sicher, da HTTPS Zugriff aktive Aktion des Benutzers benötigt. In diesem Fall ist klar, dass die Aktion absichtlich ist und die File-Prüfung des Clouds kann sofort getriggert werden, wenn Update außerhalb des NGO Systems getriggert ist.

Cloud-Share Apps, z.B. Citrix FileShare App, ist Windows Mount, d.h. zwischen C: und S: Laufwerken kann auch per Skript kopiert werden. Externer Mitarbeiter weiß nichts davon, wenn sein Rechner infiziert ist.

Mount „S:“ hat auch Abbildung in „C:\user\username\AppData\Local\Citrix\Citrix Files\PartCache“, d.h. per Skript ist kopieren auf jeden Fall möglich.

Automatisierte Cloud-Updates externer und interner Rechner sind u.U. nicht unterscheidbar.

-> Dadurch kann passive Malware Skript in Cloud gelangen



Ein Trigger (z.B. über präparierte Internetseite, Werbung oder Email) kann die passive Malware aktivieren, was zu weiterer Installation von Ransomware, Botnetz, etc. führen kann

Copy oder Share über Cloud oder andere Systeme führt zu Malware Verbreitung

NGO Gerät
(VPN)

NGO Gerät
(direkt)



Technische Problem Lösung

