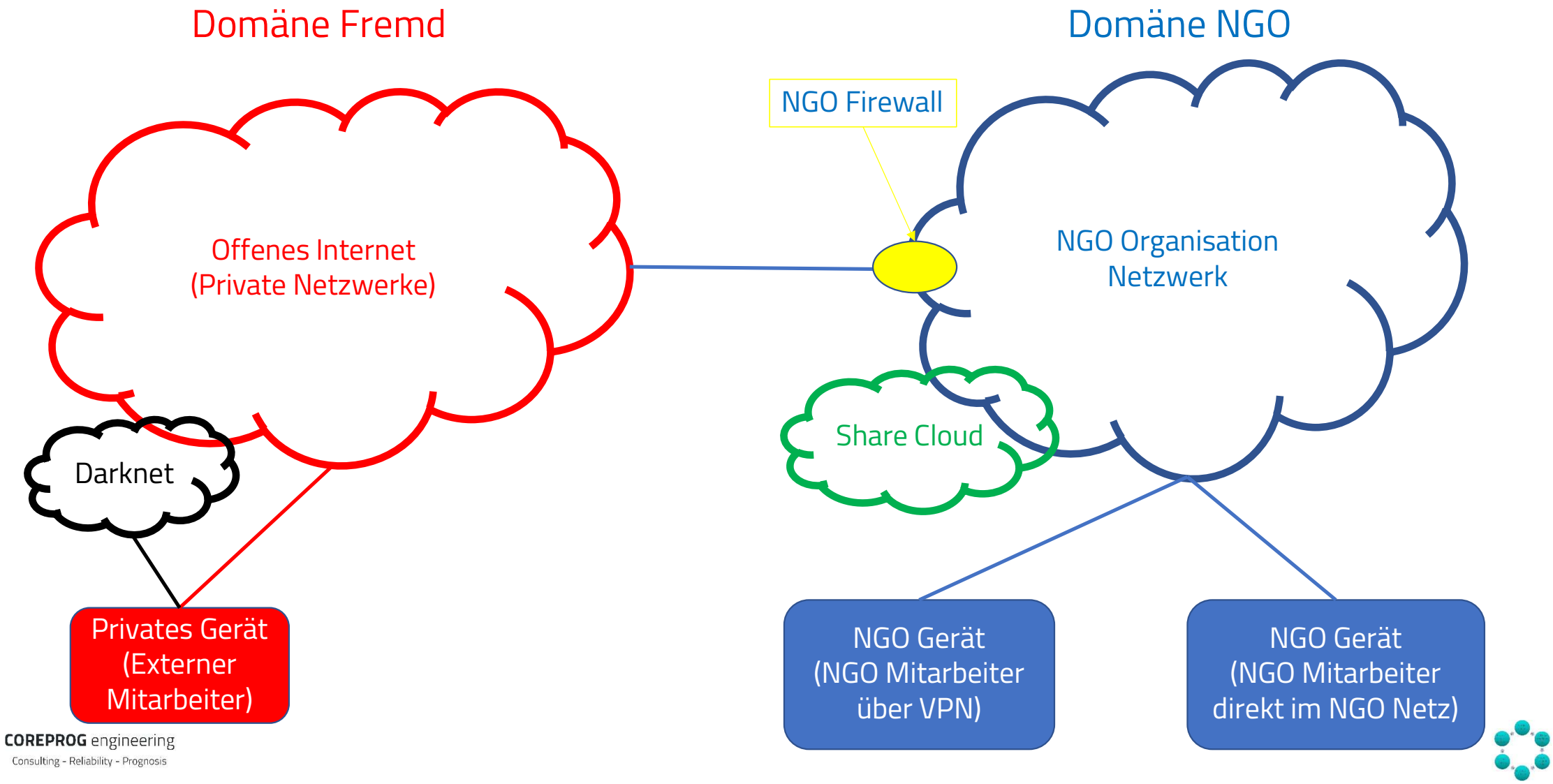
IT-Sicherheits-Studie

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

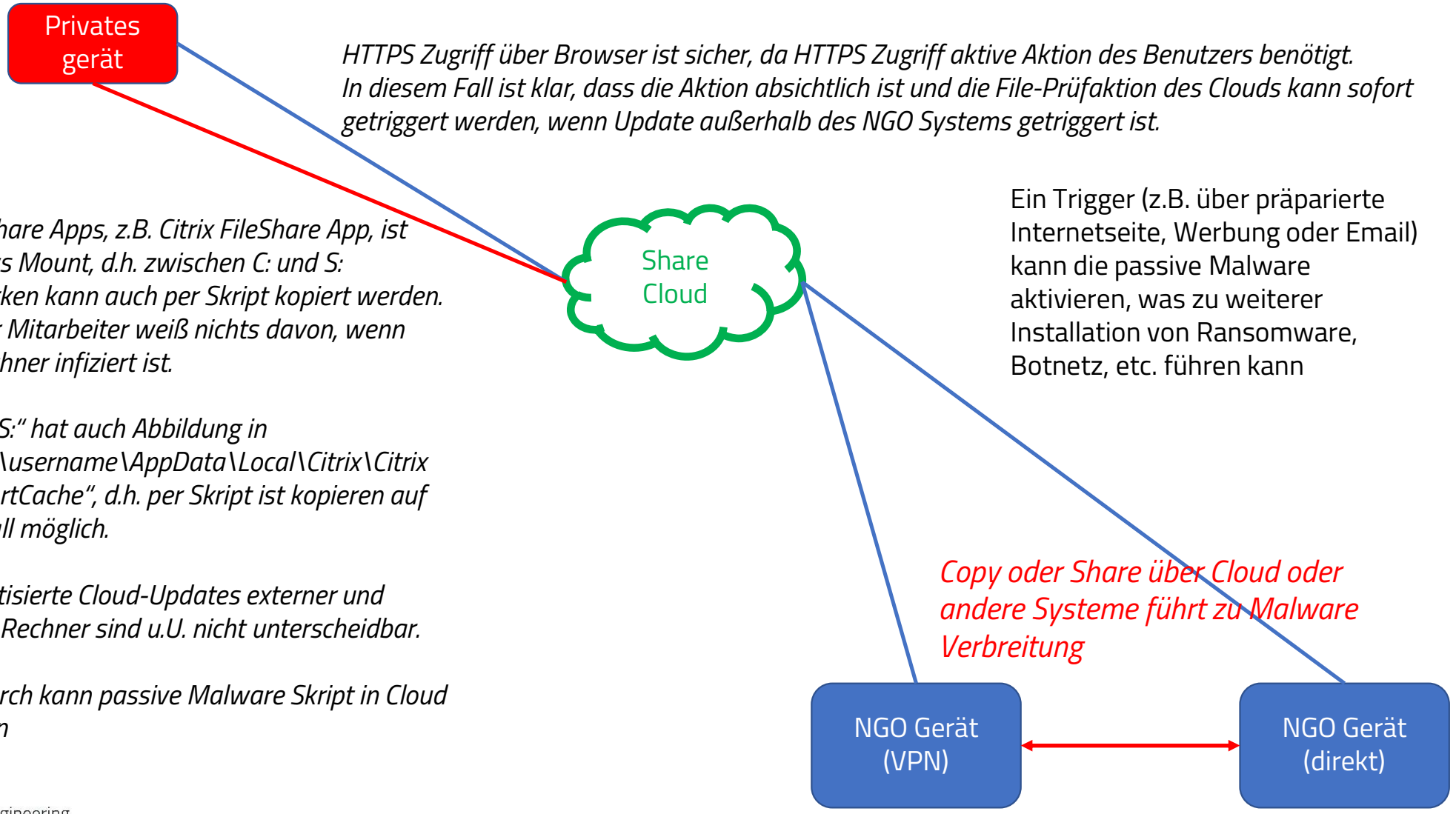
System Situation externe Mitarbeiter und NGO



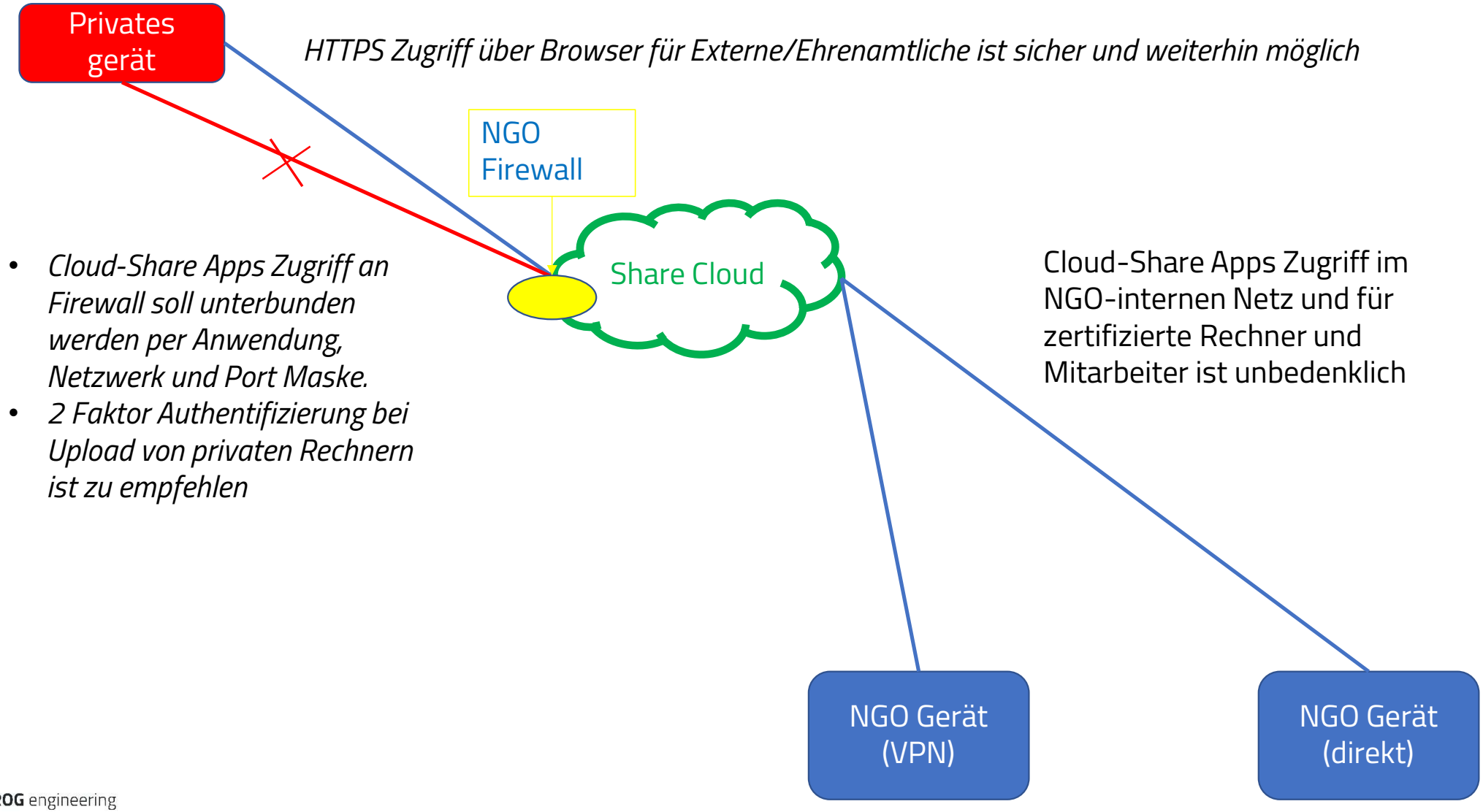
Gefahren Situation

- 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



Technische Problem Lösung



- *Cloud-Share Apps Zugriff an Firewall soll unterbunden werden per Anwendung, Netzwerk und Port Maske.*
- *2 Faktor Authentifizierung bei Upload von privaten Rechnern ist zu empfehlen*

Cloud-Share Apps Zugriff im NGO-internen Netz und für zertifizierte Rechner und Mitarbeiter ist unbedenklich