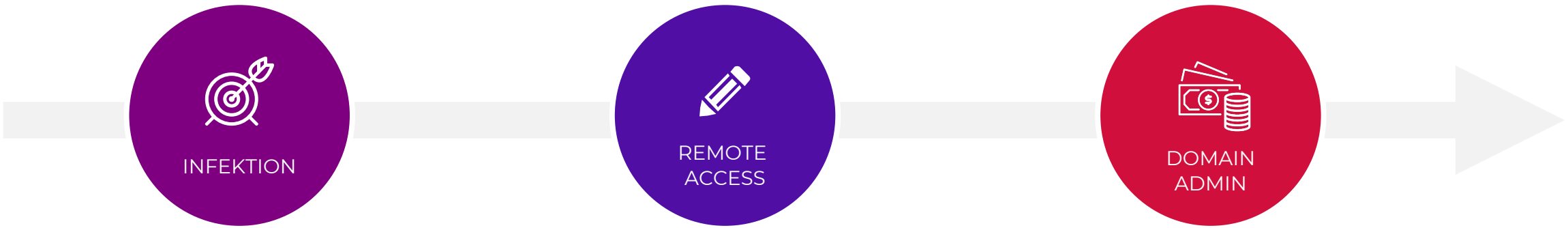
BEE SECURITY

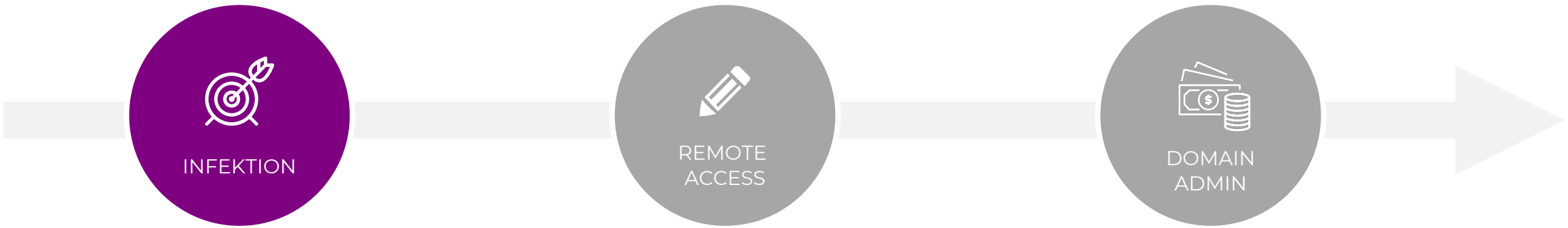
Dungeons and Domain Admins

Der etwas andere Live Hack...

Unsere Aufgabe



Unsere Aufgabe

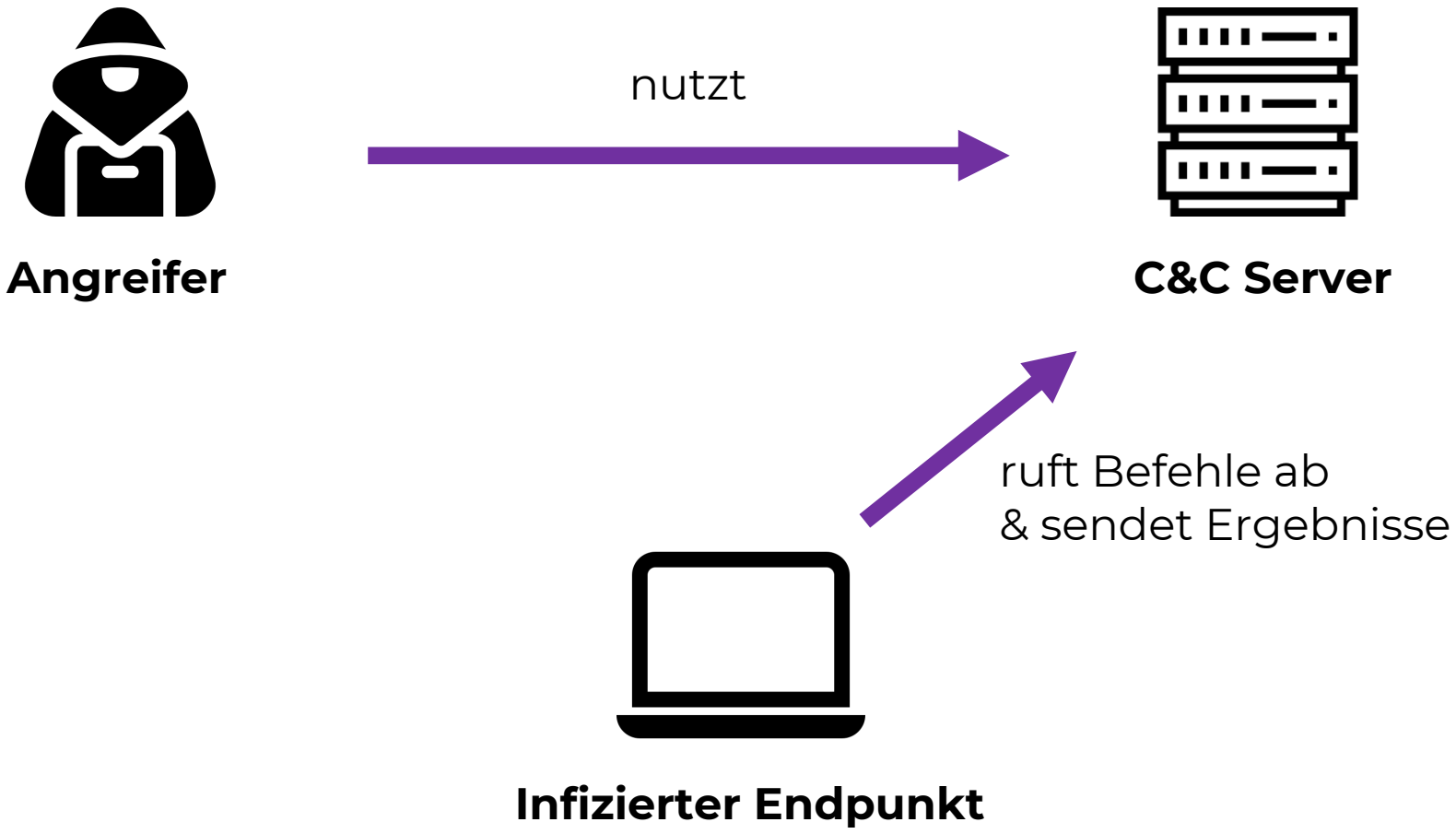


Infektion

Als Trojanisches Pferd im EDV-Jargon auch kurz Trojaner genannt, bezeichnet man ein Computerprogramm, das als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen des Anwenders eine andere Funktion erfüllt.

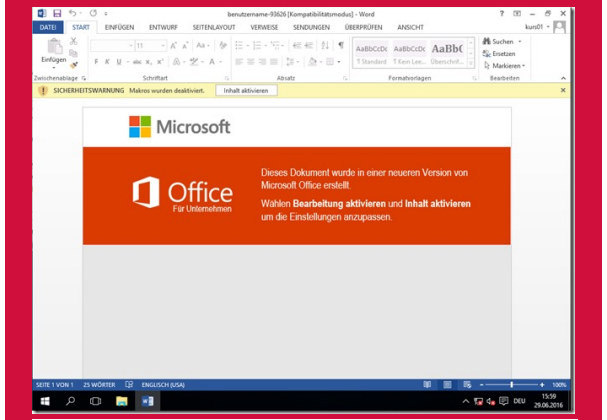
https://de.wikipedia.org/wiki/Trojanisches_Pferd_(Computerprogramm)

Infektion

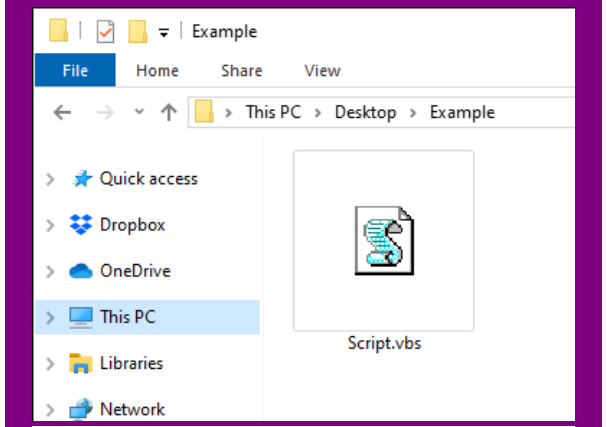

nutzt
Angreifer
C&C Server
ruft Befehle ab
& sendet Ergebnisse
Infizierter Endpunkt

Live Demo der BeeShell

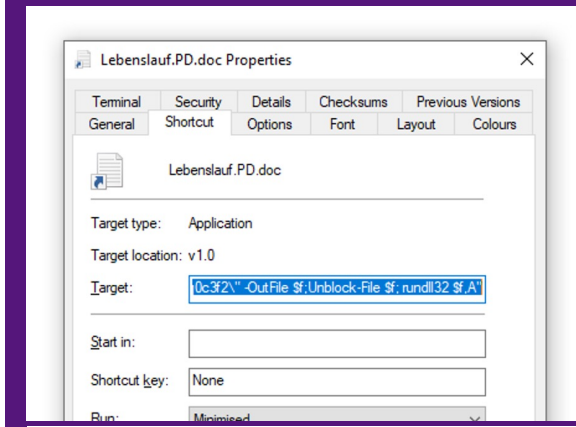
Infektion



Office Makros + Fileless
Infektion mittels AutoOpen Makro ohne eine Datei zu schreiben.

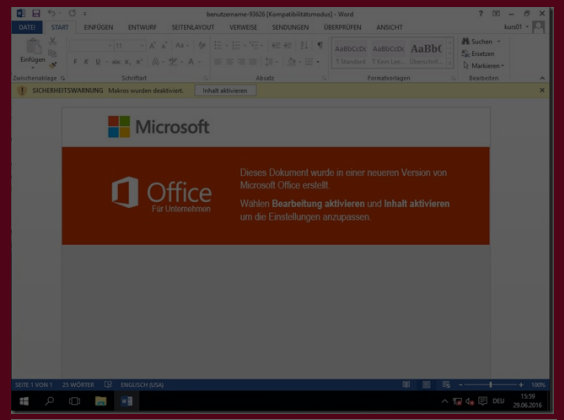


Skript + EXE
Gefährlicher Datentype (.js) lädt EXE Datei herunter, die BeeShell ausführt.

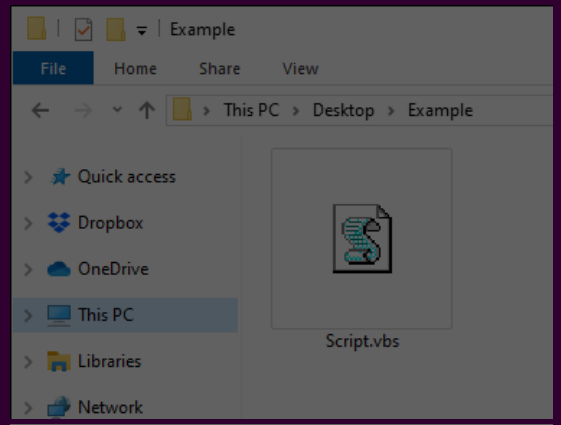


LNK + DLL
Link lädt per PowerShell eine DLL herunter, welche per rundll32.exe eine BeeShell startet.

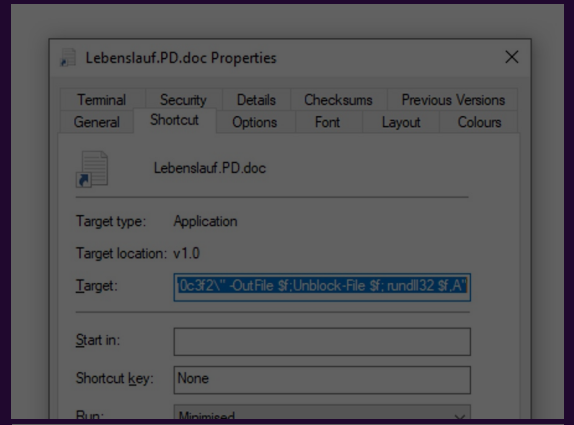
Infektion



Office Makros + Fileless
Infektion mittels AutoOpen Makro ohne eine Datei zu schreiben.



Skript + EXE
Gefährlicher Datentype (.js) lädt EXE Datei herunter, die BeeShell ausführt.



LNK + DLL
Link lädt per PowerShel
eine DLL herunter, welc
per rundll32.exe eine
BeeShell startet.

https://forms.office.com/e/dBxM80iVvS

Auswertung

BEE SECURITY

Insert Web Page

This app allows you to insert secure web pages starting with https:// into the slide deck. Non-secure web pages are not supported for security reasons.

Please enter the URL below.

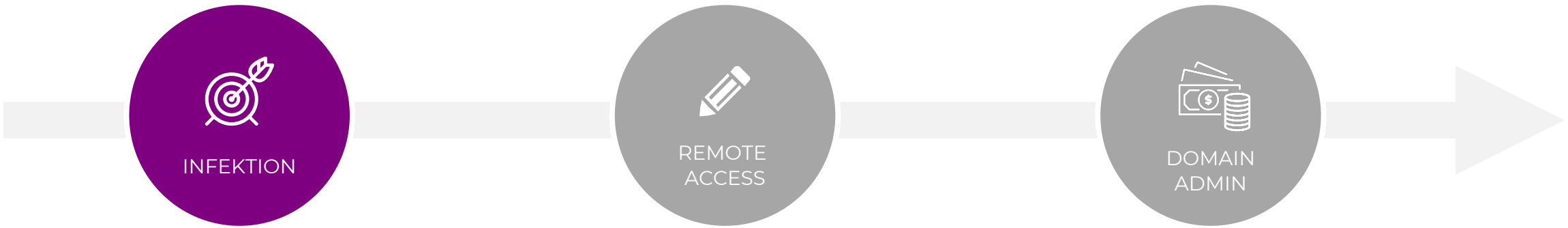
https:// tinyurl.com/2ka84tka

Note: Many popular websites allow secure access. Please click on the preview button to ensure the web page is accessible.

Web Viewer Terms | Privacy & Cookies Preview

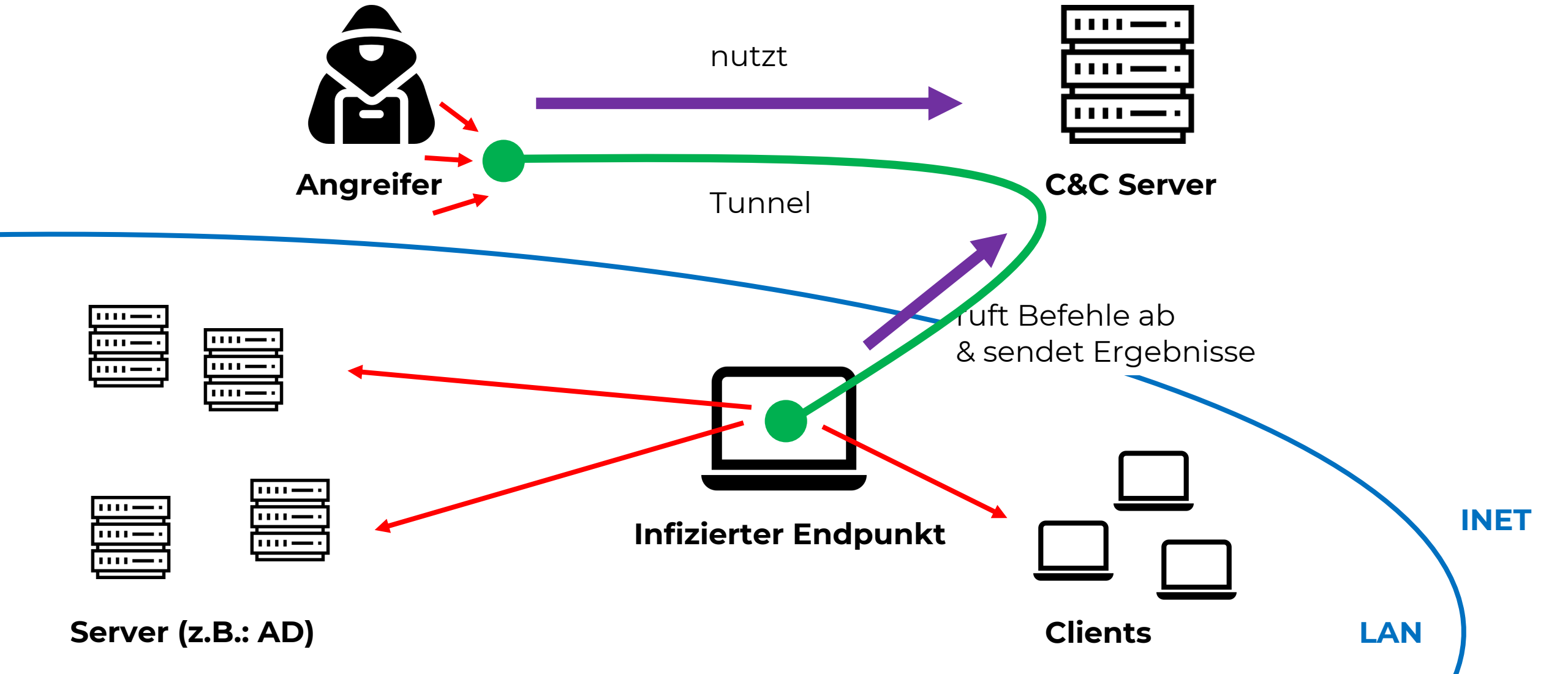
https://forms.office.com/e/dBxM80iVvS

Unsere Aufgabe

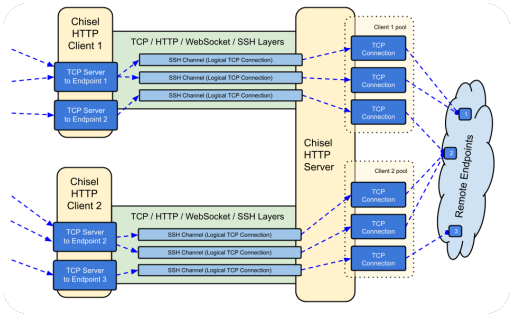


Unsere Aufgabe

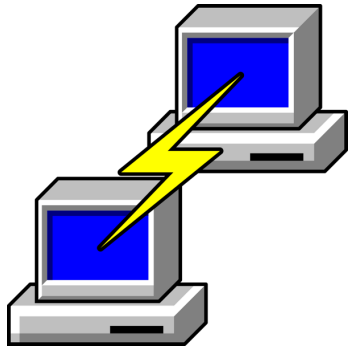
Infektion


nutzt
Angreifer
C&C Server
Tunnel
ruft Befehle ab
& sendet Ergebnisse
Infizierter Endpunkt
INET
Server (z.B.: AD)
Clients
LAN

Remote Access

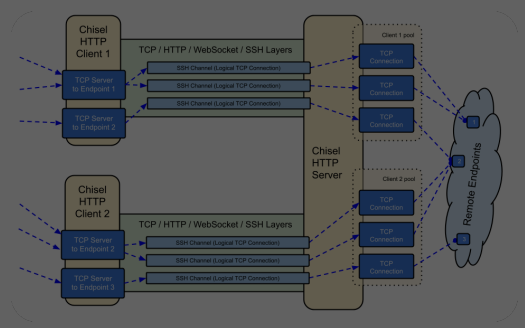


Chisel
Erlaubt es Tunnel basierend auf Basis von u.a. HTTP aufzubauen.
Nachteil: 3rd Party Tool!

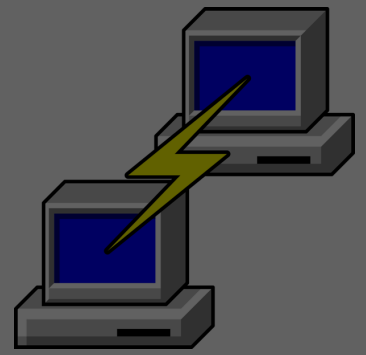


SSH Tunneling
Nutzung von OpenSSH um eine Verbindung herzustellen.
Nachteil: SSH ins Internet?

Remote Access



Chisel
Erlaubt es Tunnel basierend auf Basis von u.a. HTTP aufzubauen.
Nachteil: 3rd Party Tool!



SSH Tunneling
Nutzung von OpenSSH um eine Verbindung herzustellen.
Nachteil: SSH ins Internet?

https://forms.office.com/e/Sb13NNnHsN

Auswertung

Insert Web Page

This app allows you to insert secure web pages starting with https:// into the slide deck. Non-secure web pages are not supported for security reasons.

Please enter the URL below.

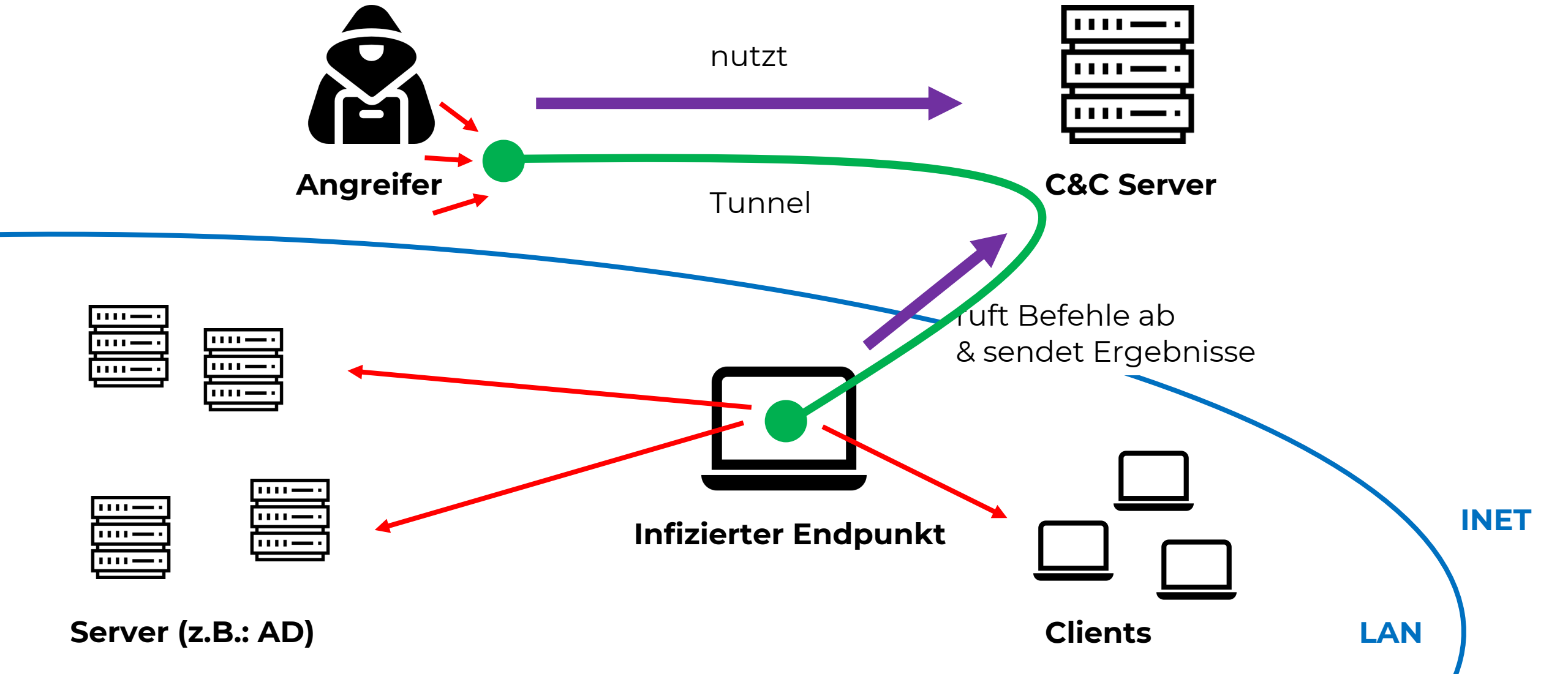
https:// tinyurl.com/5bjzh3pp

Note: Many popular websites allow secure access. Please click on the preview button to ensure the web page is accessible.

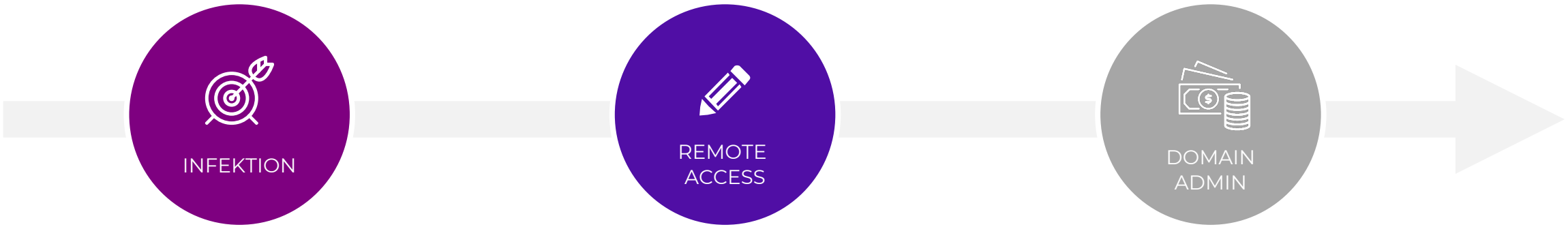
Web Viewer Terms | Privacy & Cookies Preview

https://forms.office.com/e/Sb13NNnHsN

Infektion


nutzt
Angreifer
Tunnel
C&C Server
ruft Befehle ab
& sendet Ergebnisse
Infizierter Endpunkt
Server (z.B.: AD)
Clients
INET
LAN

Unsere Aufgabe



Unsere Aufgabe

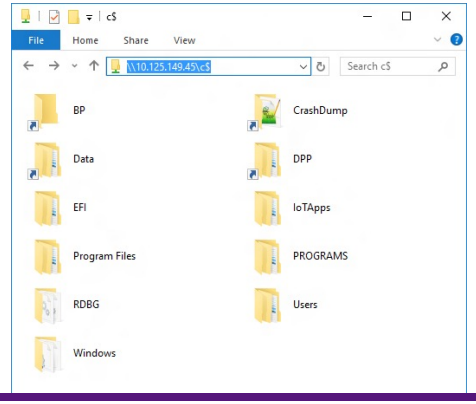
Domain Admin

Active Directory Certificate Services

Prüfung der CA
Nutzung von certipy um die ADCS auf Fehler zu prüfen.

BLOODHOUND

Bloodhound
Analyse des AD mit Bloodhound. Ist ein Lateral Movement möglich?



Sharefinder
Gibt es spannende Datei-Freigaben im internen Netzwerk?

Domain Admin

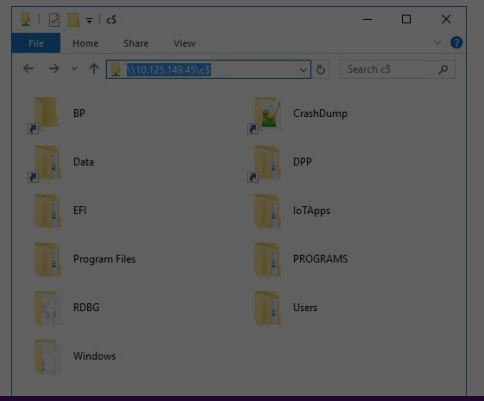
BEE SECURITY

Active Directory Certificate Services

Prüfung der CA
Nutzung von certipy um die ADCS auf Fehler zu prüfen.

BLOODHOUND

Bloodhound
Analyse des AD mit Bloodhound. Ist ein Lateral Movement möglich?



Sharefinder
Gibt es spannende Datei-Freigaben im internen Netzwerk?

https://forms.office.com/e/wg74NxVDrW

Auswertung

Insert Web Page

This app allows you to insert secure web pages starting with https:// into the slide deck. Non-secure web pages are not supported for security reasons.

Please enter the URL below.

https:// tinyurl.com/4b3rfxuc

Note: Many popular websites allow secure access. Please click on the preview button to ensure the web page is accessible.

Web Viewer Terms | Privacy & Cookies Preview

https://forms.office.com/e/wg74NxVDrW

BEE SECURITY

Florian Bogner

Information Security Experte

florian.bogner@beesecurity.at
+43 660 123 9 454
https://www.beesecurity.at