

# Zero Trust Network Access Enabler für die IT Modernisierung?



*Daniel Stutz, Co-Founder XplicitTrust*  
[xplicittrust.com](http://xplicittrust.com)

# Network Access



## Zentrale Frage:

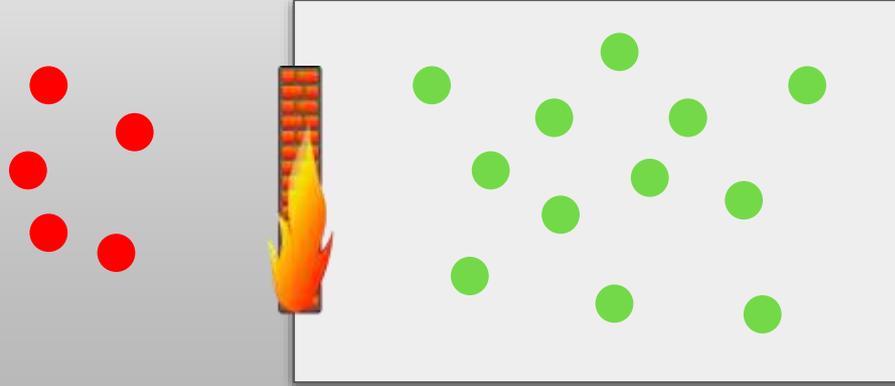
“Wer darf über das Netzwerk auf einen Dienst zugreifen?”

# Network Access



## Zentrale Frage:

“Wer darf über das Netzwerk auf einen Dienst zugreifen?”

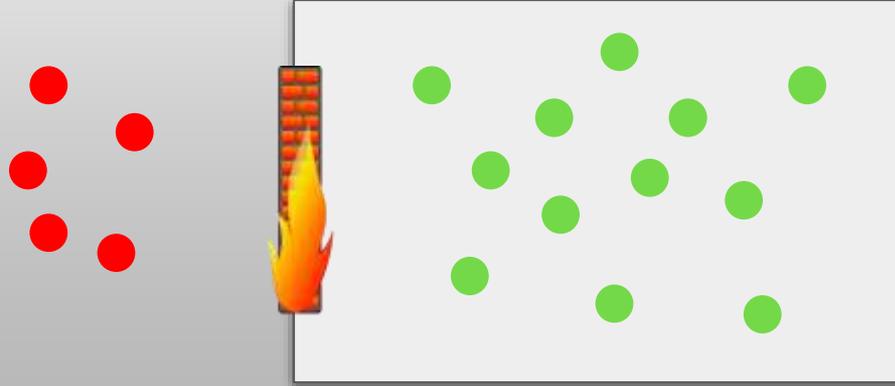


# Network Access



**Antwort:**

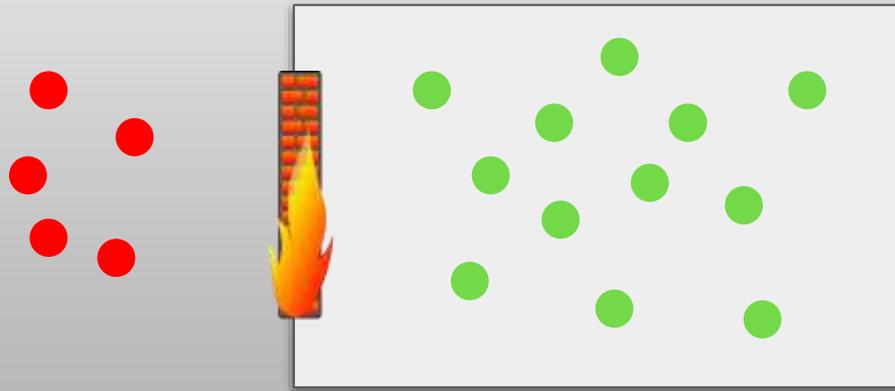
“Jeder, der sich im “privaten Netzwerk” befindet.”



# Network Access



Warum macht man es nicht sicherer?



# Network Access



## Sicherheit ist komplex

- ! Es gibt schon viele Ansätze für Teilprobleme:
  - Client-Zertifikate
  - Network Access Control
  - Application Firewalls
  - Point-to-Point VPNs
  - VLANs

**Unvollständig**

# Network Access



## Sicherheit ist komplex

- ! Es gab und gibt schon viele Ansätze
- ! Rollout und Management sind aufwändig:
  - Auf welche Dienste braucht ein Mitarbeiter Zugriff über das Netz?
  - Was muss bei Onboarding, Versetzung, Offboarding von Mitarbeitern passieren?
  - Was, wenn der Server ins Rechenzentrum soll?

**Aufwändig**

# Network Access



## Sicherheit ist komplex

- ! Es gab und gibt schon viele Ansätze
- ! Rollout und Management sind aufwändig
- ! Komplexität nimmt über die Zeit zu:
  - “Brauchen wir diese (VLANs, Firewall-Regeln, VPN-Tunnel) noch?”

**Unbeherrschbar**

# Zero Trust Network Access



## Zentrale Frage:

“Darf der **Nutzer** von diesem **Endgerät**, in seinem derzeitigen **Zustand**, an seinem derzeitigen **Standort** auf diesen **Dienst** zugreifen?”

# Zero Trust Network Access



## Zentrale Frage:

“Darf der **Nutzer** von diesem **Endgerät**, in seinem derzeitigen **Zustand**, an seinem derzeitigen **Standort** auf diesen **Dienst** zugreifen?”

**Wenn ja:**

Zugriff wird ermöglicht

**Wenn nein:**

Dienst auf **Netzwerkebene** nicht erreichbar

# Zero Trust Network Access



## Noch relevant?

- ? Wo steht der Dienst?
- ? Welche Firewalls stehen zwischen dem Endgerät und dem Server?
- ? Welche Konfiguration braucht der Client?
- ? Wann laufen die Zertifikate ab?
- ? Ist der Benutzer im Büro, auf Geschäftsreise, im Home Office?

# Zero Trust Network Access



## Noch relevant?

- ? Wo steht der Dienst?
- ? Welche Firewalls stehen zwischen dem Endgerät und dem Server?
- ? Welche Konfiguration braucht der Client?
- ? Wann laufen die Zertifikate ab?
- ? Ist der Benutzer im Büro, auf Geschäftsreise, im Home Office?

**Wir finden: Nein!**

# Xplicit Trust Network Access



## Zero Trust Network Access für den Mittelstand

### ✓ Einfach

- Zugriff auf Netzwerkdienste von überall aus
- ohne komplexe Konfiguration
- funktioniert immer

# Xplicit Trust Network Access



## Zero Trust Network Access für den Mittelstand

- ✓ Einfach
- ✓ Sicher
  - Identitätsbasiert
  - Multi-Faktor-Authentifizierung
  - automatische Schlüsselerwaltung

# Xplicit Trust Network Access



## Zero Trust Network Access für den Mittelstand

- ✓ Einfach
- ✓ Sicher
- ✓ Ganzheitlich
  - Dynamische Risikobewertung
  - Evaluation des Zustands der Endpunkte
  - Berücksichtigung des Zugriffskontexts

# Darum XplicitTrust



## Revolutionär einfache Bereitstellung und Betrieb

- ✓ **Always Connect**  
auch unter ungünstigen Netzbedingungen immer eine Verbindung
- ✓ **Zero Configuration**  
Identitätsbasierte, automatische Bereitstellung von Konfiguration
- ✓ **Actionable Insights**  
den Live-Status der Verbindungen jederzeit im Blick



# Darum XplicitTrust

## Revolutionär einfache Bereitstellung und Betrieb

- ✓ Always Connect
- ✓ Zero Configuration
- ✓ Actionable Insights

## Reduktion der Angriffsfläche exponierter Dienste

- ✓ Single Packet Authorization  
verhindert unbefugten Zugriff auf der Netzwerkebene
- ✓ Mikro-Segmentierung  
erschwert opportunistische Angriffe auf 0-Day Schwachstellen
- ✓ Handlungs- und Planungsspielraum für IT Verantwortliche

# Moderne IT

## Next Generation Network Access

- ✓ Benutzer erhalten anhand ihrer Gruppenmitgliedschaft Zugriff auf Dienste
  - ✓ Einfach: Onboarding, Abteilungswechsel, Offboarding
  - ✓ Multi-Faktor-Authentifizierung



# Moderne IT

## Next Generation Network Access

- ✓ Benutzer erhalten anhand ihrer Gruppenmitgliedschaft Zugriff auf Dienste
- ✓ Lokation der Dienste irrelevant
  - ✓ über Standorte verteilt
  - ✓ im Rechenzentrum
  - ✓ in der Cloud



# Moderne IT



## Next Generation Network Access

- ✓ Benutzer erhalten anhand ihrer Gruppenmitgliedschaft Zugriff auf Dienste
- ✓ Lokation der Dienste irrelevant
- ✓ Lokation der Nutzer irrelevant, aber kann eingeschränkt werden
  - ✓ im Außendienst oder auf Reisen
  - ✓ im Home Office
  - ✓ in einer Filiale
  - ✓ kein Zugriff aus dem Ausland

# Moderne IT

## Standortvernetzung

- ✓ Keine Site-to-Site Tunnel notwendig
  - ✓ Server werden direkt miteinander verbunden
  - ✓ für Benutzer spielt die Lokation keine Rolle



# Moderne IT



## Standortvernetzung

- ✓ Keine Site-to-Site Tunnel notwendig
- ✓ Kein Routing-/ und NAT-Problem bei Adressraumüberlappung
  - ✓ Dienste kommunizieren in eigenem Adressraum
  - ✓ Overlay-Netzwerk

# Moderne IT



## Standortvernetzung

- ✓ Keine Site-to-Site Tunnel notwendig
- ✓ Kein Routing-/ und NAT-Problem bei Adressraumüberlappung
- ✓ Benutzer können entweder
  - ✓ von allen Standorten den gleichen Zugang
  - ✓ oder je nach Standort eingeschränkten Zugang erhalten

# Moderne IT

## Rechenzentren und Multi-Cloud Szenarien

- ✓ Lokation der Dienste spielt keine Rolle
  - ✓ Server können beliebig platziert und migriert werden
  - ✓ Server sind immer vor Zugriffen aus dem Internet geschützt
  - ✓ erleichtert Migration in die Cloud, zwischen Clouds, oder aus der Cloud zurück



# Moderne IT

## Rechenzentren und Multi-Cloud Szenarien

- ✓ Lokation der Dienste spielt keine Rolle
- ✓ Vernetzung von Diensten untereinander über Cloud Grenzen hinweg
  - ✓ zur schrittweisen Re-Organisation von Cloud Diensten
  - ✓ um Lock-In bei Anbietern zu vermeiden



# Moderne IT

## Effektive Sicherung schwer patchbarer Systeme

- ✓ Auf engsten Nutzerkreis einschränkbarer Zugang
- ✓ Erweiterte Anforderungen an Lokation, Art und Zustand der Endgeräte
- ✓ Dokumentierbarer Berechtigtenkreis

- **zertifizierte Geräte**
- **Legacy-Systeme**
- **Individualsoftware**



# Moderne IT

## Industrie 4.0

- ✓ Sichere Anbindung von Maschinen und Geräten an Hersteller Clouds
  - ✓ Technologie funktioniert zuverlässig auch bei widrigen Bedingungen oder unvorhersehbaren Änderungen in den Kundennetzen
- ✓ Auf die Hardware des Herstellers eingrenzbare Wartungszugänge
- ✓ Gegenüber Kunden dokumentierbare Datenflüsse



**Interessiert an einer Live Demo?**



**Besuchen sie unseren  
Stand, an dem freundliche  
Mitarbeiter alle Fragen  
beantworten und  
XplicitTrust Network Access  
live demonstrieren!**