KOM SG

Netzwerksegmentierung

Informationen für Administratoren und Entscheidungsträger

Das vorliegende Dokument verwendet für eine einfache flüssigere Lesbarkeit ausschliesslich die männliche Schreibform.

1. Einleitung

In diesem Dokument wird das Thema Netzwerksegmentierung behandelt. Das Dokument ist sowohl als Referenz für Administratoren sowie als Wissensbasis für Entscheidungsträger zu verstehen.

1.1. Netzwerk ohne Segmentierung

Um die Netzwerksegmentierung besser zu verstehen hier eine Illustration eines Netzwerks ohne Segmentierung:

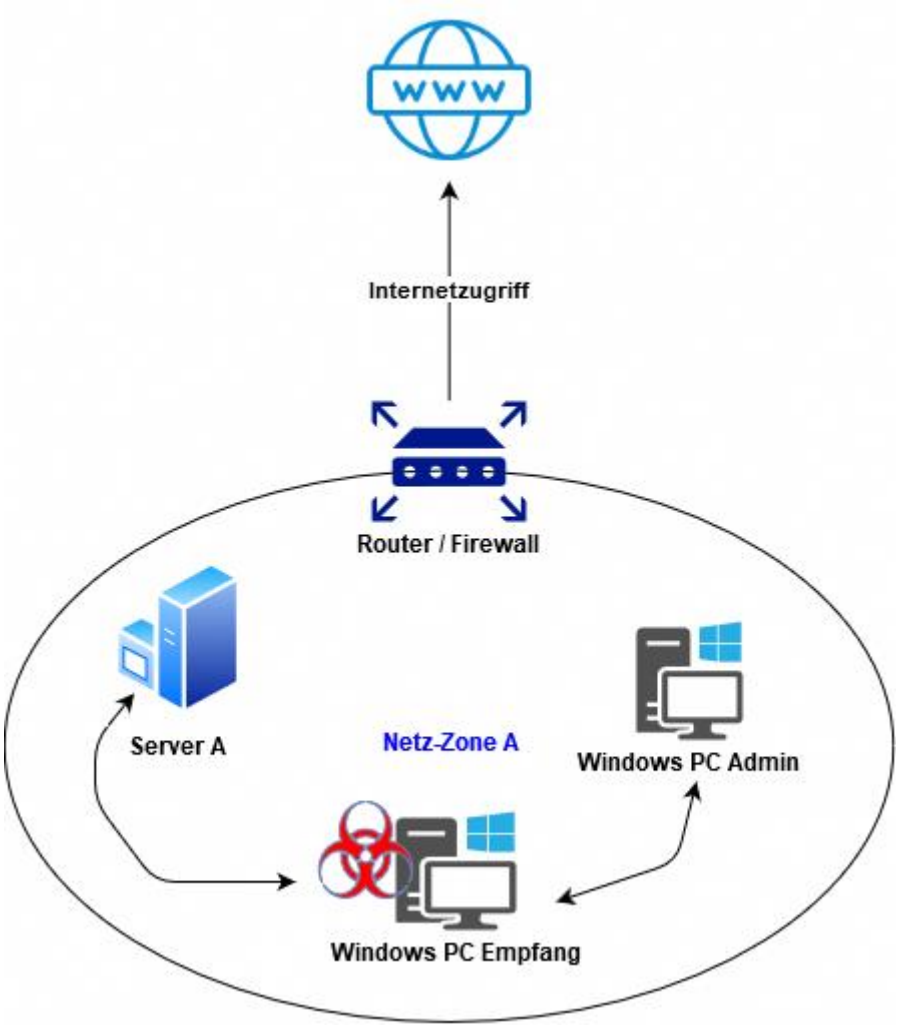


Abbildung 1 - Unsegmentiertes Netzwerk

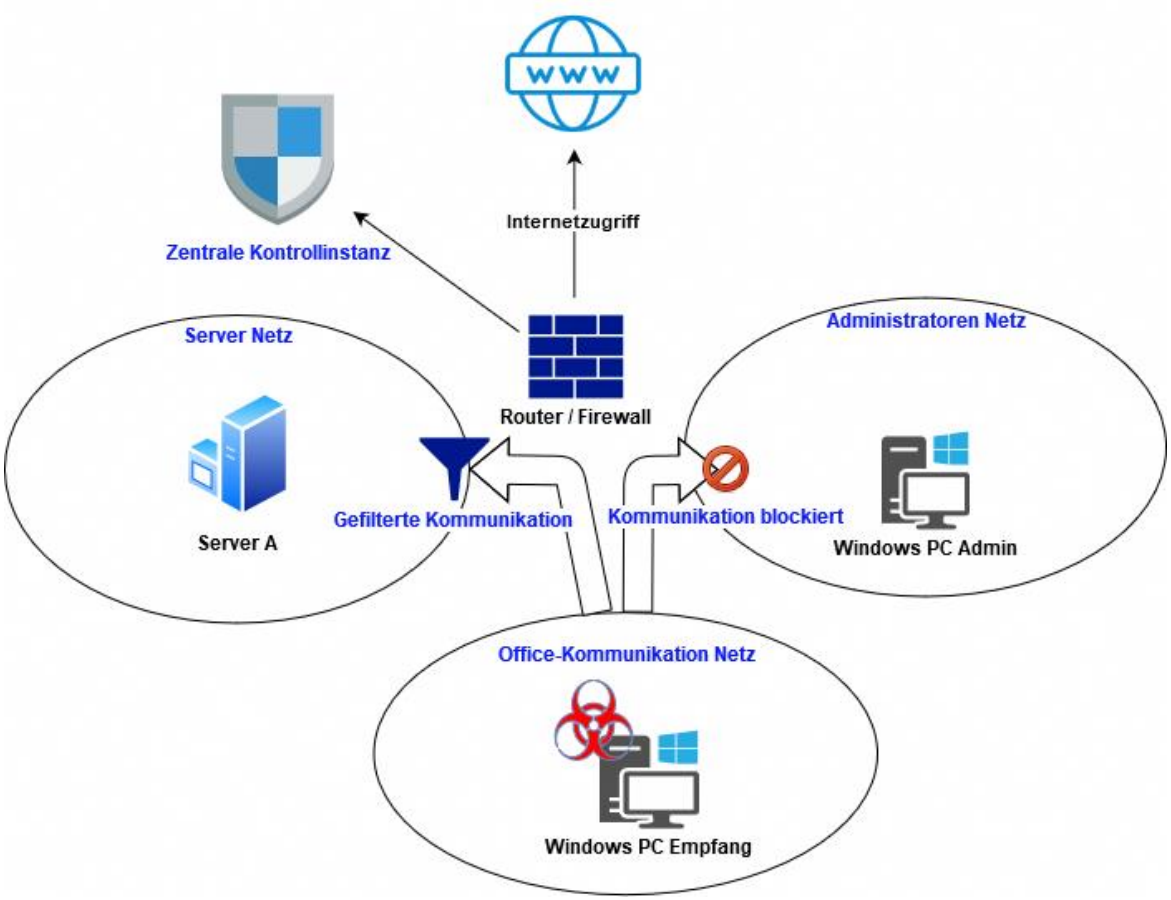
Sämtliche Geräte sind dabei in der gleichen Netz-Zone angesiedelt und können uneingeschränkt untereinander kommunizieren. Der 'PC Empfang' und 'PC Admin' können mit jeglichen Netzwerkprotokollen den Server A kontaktieren.

Wird ein einzelnes Gerät in der Netz-Zone kompromittiert (hier PC Empfang) gibt es für Angreifer keine netzwerktechnischen Hürden mehr zu überwinden, da alle Arbeitsstationen und Server ungefiltert kommunizieren.

Angreifer nun das gesamte Netzwerk beeinflussen. Denkbar sind Angriffe auf alle drei Schutzziele, (Vertraulichkeit, Integrität & Verfügbarkeit) je nach Motivation und Absichten der Angreifer.

1.2. Netzwerk mit Segmentierung

Im direkten Vergleich hier ein Netzwerk mit segmentierten Netz-Zonen:



Das Netzwerk wurde in 3 Netz-Zonen aufgeteilt. Computer von Office Mitarbeitenden befinden sich im 'Office-Kommunikation' Netz, während sich Geräte von Administratoren sowie Server im gesonderten 'Administratoren', resp. 'Server' Netz befinden.

Grundkommunikationsregeln für diese Architektur könnten z.B. wie folgt aussehen:

- Office-Kommunikation zu Administratoren: Alles Blockiert
- Office-Kommunikation zu Server: Nur spezifische Dienste erlaubt (gefiltert)

Wird nun das Gerät am Empfang wie bei Punkt 1.1 kompromittiert, befinden sich die Angreifer im Office-Kommunikation Netz. Von hier können Sie nicht wie zuvor direkt Geräte von Administratoren ansprechen/attackieren, da die Kommunikation vom Office-Netz zum Administratoren Netz komplett unterbunden wird. Simple Netzwerkangriffe (z.B. Layer 2 basierte Angriffe) oder administrative Zugänge zu den Servern (Remote Desktop) sind für Angreifer aus dem Office-Netz ebenfalls blockiert.

Mit dieser simplen Trennung und einigen Firewall Regeln wurde die Sicherheit für Komponenten in dieser Netzumgebung drastisch gesteigert.

Wichtig: Natürlich bringen diese Massnahmen keine 100% Sicherheit für das Netzwerk, dies ist nie erreichbar und soll auch nicht Ziel von Schutzmassnahmen sein. Ziel ist eine Risikominderung eines grösseren Vorfalls indem man versucht Angreifer zu verlangsamen, Ihnen viele Hürden zu stellen und dann diese Hürden zu überwachen, um etwaige Angriffe festzustellen.

2. Umsetzung

In diesem Abschnitt werden die beiden Hauptmethoden zur Segmentierung von Netzwerken kurz beschrieben. Diese Informationen sind eher technisch und daher vor allem für Netzwerk Administratoren von Interesse.

2.1. Logische Trennung (Empfehlung)

Eine Netzwerksegmentierung wird am einfachsten durch VLANs erreicht. Mit VLANs lassen sich mehrere logisch getrennte Netzwerke über die gleichen physischen Kanäle verwalten. Netzwerkpakete werden entsprechend des VLANs markiert (Tagging) und operieren getrennt zu Paketen mit anderer VLAN Markierung.

Um von einem VLAN ins nächste zu kommunizieren wird wie bei jedem Netzwerkübertritt ein Layer-3 Gerät (Router) benötigt. Die Übertritte resp. das Routing zwischen den VLANs sollte von einer Firewall behandelt werden. Dadurch können sämtliche Verbindungen unterhalb der VLANs in einer zentralen Kontrollinstanz geregelt werden.

Selbst wenn die Kommunikationsregeln nicht strikt konfiguriert werden, hat diese Konstellation den Vorteil, dass jegliche Zugriffe / Netzübergänge Paketlogs auf der Firewall hinterlassen die geprüft und analysiert werden können.

2.2. Physische Trennung

Eine weitere Methode zur Segmentierung von Netzwerken ist die weitaus aufwändigere (mehr Infrastruktur) physische Trennung. Durch separate Kabel und Netzkomponenten können so Systeme stark voneinander getrennt werden.

Meist ist eine solche Trennung nicht nötig, kann aber in gewissen Fällen auch simpler sein, Beispiel dafür ist z.B. ein zusätzlicher Internetanschluss, der für Gäste-WLAN genutzt wird und physikalisch komplett von der Umgebung der Verwaltung getrennt wurde.