BWCAMPUSNETZ

Zukunftsfähige Konzepte für die Campusnetze
an Universitäten und Hochschulen

Leitfaden Netzsegmentierung in Campusnetzen

Federführung bei der Erstellung dieses Dokuments: Karlsruher Institut für Technologie
Kontakt: team@bwcampusnetz.de

Inhalt

1 Einleitung

Netzsegmentierung ist der Prozess der Aufteilung eines Netzwerks in kleinere Segmente. In einem Campusnetz gibt es historisch oft große Broadcast-Domänen. In der Regel sind diese als VLANs realisiert, denen IP-Subnetze zugeordnet sind. In diesem Dokument wird beschrieben, welche Gründe für eine umfangreiche Segmentierung des Netzwerks und die Verkleinerung vorhandener Netzsegmente sprechen. Weiterhin wird besprochen, was bei der Netzsegmentierung zu beachten ist und wie die Segmentierung umgesetzt werden kann. Bei den Gründen für die Netzsegmentierung ist an erster Stelle die IT-Sicherheit zu nennen, was im folgenden weiter erläutert wird. In diesem Dokument werden die Begriffe Broadcast-Domäne und Netzsegment synonym verwendet.

In Campusnetzen gibt es häufig dezentrale Zuständigkeiten. Netzsegmente voller Altlasten werden von IT-Admininistratoren übernommen, oft ohne Übergabe durch den vorherigen Administrator, die sich dort erst einmal zurecht finden müssen. Es ist erforderlich, dass ein IT-Administrator den Überblick über alle Teilnehmer in den eigenen Netzsegmenten hat. Dies ist in akademischen Campusnetzen teilweise schwer zu verwirklichen, je nach physischer Zugänglichkeit von Netzwerkdosen, fehlender Authentifzierung und fehlenden organisatorischen Maßnahmen. Dennoch ist es auch zu beobachten, dass weniger Überblick besteht als möglich wäre. Generell ist aber für die IT-Administratoren von Organisationseinheiten eine gewisse Ordnung empfehlenswert, um aus administrativer Perspektive eine Gesamtübersicht zu behalten. Dieses Dokument soll eine Verbindung schaffen zwischen dem Schaffen von Ordnung und dem Umsetzen von IT-Sicherheit mittels Netzsegmentierung.

2 IT-Sicherheit

Zunächst soll erläutert werden, welche Vorteile eine weitreichende Netzsegmentierung für die IT-Sicherheit hat. Eine Broadcast-Domäne ist eine Vertrauens- und eine Fehlerdomäne. Das bedeutet, es gibt innerhalb der Broadcast-Domäne eine größere Angriffsfläche als über Netzsegmentgrenzen hinweg, d.h. es gibt Angriffe, die nur innerhalb einer Broadcast-Domäne möglich sind. Weiterhin dass es Fehlerbilder gibt, die alle Geräte in einer Broadcast-Domäne betreffen, die sich aber nicht über Subnetzgrenzen hinweg ausbreiten können.

Zu solchen Angriffen zählen IP-Spoofing, Rogue DHCP-Server, Rogue Router Advertisements und Neighbor Discovery DoS Attack sowie ARP-Spoofing. Als Fehlerbilder sind Schleifen, Broadcast-Stürme und IP-Adresskonflikte zu nennen. Die Fehlerbilder führen zu einer Verminderung der Verfügbarkeit und zur ungewollten Umleitung von Netzwerverkehr.

Durch gleichartige Systeme innerhalb der Broadcast-Domäne wird die Angriffsfläche verkleinert. Ist ein Gerät mit einem verwundbaren Gerät in derselben Broadcast-Domäne und selbst gegenüber dieser Verwundbarkeit nicht anfällig, steigt dennoch die eigene Verwundbarkeit, da einem Angreifer, der bereits in die eigene Broadcast-Domäne eingedrungen ist, mehr Angriffsmöglichkeiten innerhalb dieser zur Verfügung stehen.

Der Vorteil der Auftrennung in mehrere Broadcast-Domänen ist außerdem die Trennung des BUM-Traffics und die Reduzierung des Layer-2-Overheads. Hierdurch steigt die Verfügbarkeit des Netzwerks. Aufgrund von BUM-Traffics und der fehlenden Struktur in Layer-2-Segmenten, kann es in großen Broadcast-Domänen hingegen zu einem höheren Ressourcenverbrauch kommen, was Tabellen in der Data Plane von Netzkomponenten und Bandbreite betrifft.

Weiterhin findet Lateral movement durch einen Angreifer erfahrungsgemäß bevorzugt in der Broadcast-Domäne, d. h. im Subnetz, statt. Darüber hinaus ist bei vorhandener Netzsegmentierung das Einziehen einer Firewall zwischen den Segmenten zur weiteren Erhöhung der IT-Sicherheit einfach möglich.

2.1 Firewall-Freischaltungen

Normalerweise findet Firewalling auf Layer 3 und darüber statt. In diesem Fall kann Filterung nur zwischen Netzsegmenten und nicht innerhalb dieser stattfinden.

Auch bei Anwendung von Anti-Spoofing gemäß BCP38 [1] ist IP-Spoofing innerhalb der Broadcast-Domäne immer möglich. Insofern ist eine Freischaltung von einzelnen IP-Adressen nicht sinnvoll und bei IPv6 in der Regel auch nicht mehr möglich, da ausgehend meist temporäre Adressen verwendet werden. Ein Netzsegment soll eine einheitliche Security Policy haben und alle Geräte in dieser auf dieselben Ziele Zugriff haben. Spätestens bei IPv6 ist die Freischaltung des ganzen Netzsegments ohnehin notwenig aufgrund von unbekannten temporären Adressen der Geräte.

2.2 Zuständigkeit

Die IT-Administratoren eines Netzsegments müssen einen Überblick über die in ihr befindlichen Geräte haben. Je kleiner die Domäne ist, d. h. je weniger Geräte sich in ihr befinden, desto einfacher wird dies. Es muss eine klare administrative Zuständigkeit pro Netzsegment geben, wodurch auch die Administration selbst vereinfacht und die IT-Sicherheit gesteigert wird.

Auch bei der Nachverfolgbarkeit, gerade bei temporären zufälligen IPv6-Adressen, ist dies von Vorteil, auch wenn hier weitere Mechanismen wie die Auswertung des Neighbor Caches angewandt werden können, die auch bei großen Broadcast-Domänen funktional bleiben. Hiermit können IP-Adressen durch das Mapping auf MAC-Adressen rückverfolgt werden, indem das Gerät bzw. der Nutzer durch die MAC-Adresse identifiziert wird. Allerdings wird hier vorausgesetzt, dass das Gerät eine statische MAC-Adresse hat und diese bekannt ist. Bei dynamischen MAC-Adressen, ist es wiederum hilfreich, wenn aus dem Netzsegment klar wird, welches System dieses benutzt zur Kommunikation. Weitere Möglichkeiten der Rückverfolgbarkeit von IP-Adressen ergeben sich bei authentifzierten Netzzugängen.

3 Design von Netzsegmenten

Bei dem Design von Netzsegmenten haben sich die folgende Prinzipien für die Zusammenfassung von Geräten in einem Netzsegment als sinnvoll erwiesen:

- Geräte gleichartigen Typs: Clients, Server, Peripheriegeräte, IoT-Geräte
- Teilnehmer, die dieselbe Anwendung bereitstellen
- Geräte mit demselben Schutzbedarf
- Geräte mit denselben Administratoren

Beispiele für Netzsegmente:

- Arbeitsplatz-PCs einer Abteilung oder eines Teams
- Arbeitsplatz-PCs der IT-Administratoren
- Server in einem Projekt
- Virtuelle Maschinen, die einen RADIUS-Dienst bereitstellen
- Drucker im Gebäude 123

Grundsätzlich sind Clients und Server voneinander zu trennen und in eigenen Netzsegmenten anzubinden. Clients bieten oft größere Einfallstore als Server und Server haben oft einen höheren Schutzbedarf.

Die Anzahl der Endgeräte (MAC-Adressen) in einem Netzsegment sollte nicht zu groß sein. Ein Erfahrungswert ist, in einem Netzsegment nicht mehr als 30 Endgeräte (/27 IPv4) und im Ausnahmefall bis 254 (/24 IPv4) Teilnehmer anzubinden. Eine weitere Metrik für die Größe eines Netzsegments ist die Zahl der Netzkomponenten, auf denen das Segment aufliegt. Auf je mehr Komponenten es aufliegt, desto mehr Komponenten sind betroffen von den oben beschriebenen Fehlerszenarien, die die Verfügbarkeit des Netzwerks einschränken. Dadurch beeinträchtigte Netzkompenten können Störungen in weiteren Netzsegmente verursachen. Daher sollte darauf geachtet werden, ein Netzsegment auf möglichst wenige Netzkomponenten zu beschränken.

Generell spricht nichts gegen sehr kleine Netzsegmente mit sehr wenigen Geräten. Sollten VLANs als Technologie eingesetzt werden und die Anzahl der VLAN-IDs knapp weden, ist der Einsatz von VXLAN ein Ausweg, siehe auch *Architekturbausteine für moderne und virtualisierte Netze* [2]. Bezüglich des Verschnitts und der Knappheit von IPv4-Subnetzen, kann über IPv6-only nachgedacht werden, siehe auch das Dokument *IPv6-only in Campusnetzen* [3].

Sind Netzwerkdosen physisch zugänglich für unbekannte Personen und nicht weiter abgesichtert (siehe auch *LAN-Zugang für Benutzer, Geräte und IoT-Devices* [4]), sollten diese einem Netzsegment für Gäste zugeordnet werden, was keine Zugriffe außer einem Internetzugang bereitstellt. Keinesfalls soll eine solche Dose einem regulären Netzsegment für Angehörige der Organisationseinheit zugeordnet werden.

4 Netzsegmentierung in der Praxis

Prinzipiell ist die Netzsegmentierung sehr arbeits- und zeitaufwendig. Es ist also wichtig, dass die Akteuere von dem Vorhaben überzeugt sind. Neben den Argumenten der IT-Sicherheit, die bereits dargestellt wurden, wird im folgenden Abschnitt Analyse nochmals auf den Inventarisierungscharakter der Vorbereitung auf die Netzsegmentierung hingewiesen.

4.1 Analyse

Für die Analyse des Ist-Zustands ist der erste Schritt, dass der IT-Administrator alle Netzsegmente in seiner Zuständigkeit sammelt und sich einen Überblick über diese verschafft. Wir sprechen hier insbesondere über Netzsegmente, in die sich Nutzer im LAN verbinden. Weitere Beispiele sind Hardware-Server, die an Switchports angeschlossen sind, virtuelle Maschinen oder WLAN-Clients.

Der IT-Administrator muss sich im LAN über die Verbereitung des Segments informieren können, d.h. wo Geräte in diesem Segment angeschlossen sind. Hierbei ist es hilfreich, wenn der IT-Administrator diese Informationen selbst einsehen kann. Wenn es sich um einen dezentralen IT-Administrator handelt, wie es sie in akademischen Campusnetzen häufig gibt, sind mandantenfähige Portale oder Tools notwendig, die die zentrale IT zur Verfügung stellt oder – wenn dies nicht gegeben ist – sollten die Daten für den denzentralen IT-Administrator durch die zentrale IT ausgelesen und ihm zur Verfügung gestellt werden. Außerdem sind die Kommunikationsbeziehungen der Teilnehmer in der Organisationseinheit zu ermitteln, um die entsprechenden Freischaltungen einrichten zu können, wenn die Teilnehmer in verschiedene Netzsegmente separiert werden.

Generell ist für dezentrale IT-Administratoren eine gute Zusammenarbeit mit der zentralen IT sehr wichtig, um Verständnis für notwendige Änderungen und Anpassungen zu schaffen. Hierbei sind oft ausführliche Einzelgespräche notwendig. Schulungen für ein größeres Publikum tragen auch oft zum Verständnis bei. Derartige Umstellungen können inklusive Analyse, Planung und Vorbereitung viele Monate in Anspruch nehmen und stellen eine hohe Arbeitsbelastung für die dezentralen IT-Administratoren dar.

Hierbei ist der Inhalt des Neighbor Caches des Routers eine hilfreiche Information sowie hiernach die Lokalisierung der enthaltenen MAC-Adressen an Netzwerkports oder Netzwerkdosen. In einigen Fällen wird der dezentrale Netzwerkadministrator nicht umhin kommen, die Netzwerkdosen physisch aufzusuchen, um zu sehen, was für ein Gerät dort angeschlossen ist. Da nicht alle Geräte, die sich potentiell im Netzwerk befinden, immer eingeschaltet sind, ist dafür zu sorgen, dass dennoch alle Geräte identifiziert werden.

Die Erlangung der Übersicht kann man auch als Inventarisierung der durch den IT-Administrator betreuten Geräte bezeichnen. Die Idee ist, dass dies ohnehin in seinem Aufgabenbereich liegt und sich so die Segmentierung oder zumindest die Vorbereitung auf die Segmentierung fast nebenbei erledigen lässt.

4.2 Planung und Vorbereitung

Hat der IT-Administrator die Übersicht über die Geräte in seinen Netzsegments erlangt, kann die zukünftige Umsetzung der Netzsegmente in seinem Bereich geplant werden.

Die Kriterien, welche Geräte in einem Netzsegment zusammen gefasst werden, wurden im Abschnitt Design von Netzsegmenten bereits genannt. Es werden Geräte gleichartigen Typs, mit demselben Schutzbedarf und mit denselben Administratoren zusammengefasst. Für jedes geplante Netzsegment muss der Schutzbedarf und so die Positionierung innerhalb des gesamten Netzwerks definiert werden. Weiterhin muss bei der Verwendung von IPv4 die benötigte Anzahl der IPv4-Adressen festgelegt werden, die der Anzahl der Teilnehmer in dem Netzsegment entspricht. Die weiteren Hinweise im Abschnitt Design von Netzsegmenten sind zu beachten. Zu empfehlen ist, die Arbeitsplatz-PCs der IT-Administratoren in der Organisationseinheit in einem eigenen Netzsegment zusammenzufassen, wodurch auch die Firewall-Freischaltungen für den erweiterten Zugriff der IT-Administratoren eingerichtet werden können.

Im Rahmen der Netzsegmentierung ist Renumbering an verschiedenen Stellen nötig. Dies betrifft die IP-Adressen der Teilnehmer inklusive Subnetzmaske und Default-Gateway und weiterhin zum Beispiel DHCP-Konfigurationen und DNS-Einträge, insbesondere für Serverdienste. Auch kann es hierdurch notwendig sein, die Konfiguration von Anwendungen anzupassen. Zu empfehlen ist, bei IPv4 vor der Umstellung – sofern noch nicht geschehen – für

möglichst viele Geräte DHCP einzuführen, damit die Umstellung möglichst einfach durchgeführt werden kann. Andernfalls sind umfangreiche manuelle Konfigurationen notwendig, die dann auch zumeist direkt am Gerät durchgeführt werden müssen. Bei IPv6 erleichtert analog zu DHCP bei IPv4 die zustandlose Autokonfiguration die Umstellung.

Falls es sich anbietet, ein vorhandenes großes Netzsegment bzw. Subnetz in mehrere kleine aufzuteilen und stattdessen nicht ganz neue Netzsegmente bzw. Subnetze anzulegen, kann bei statischer IPv4-Konfiguration, wie in Servernetzen üblich, auch zunächst für eine Übergangszeit Proxy ARP auf dem Router eingeschaltet werden, um so eine sanfte Migration zu ermöglichen.

4.3 Umsetzung

Für jedes neue Netzsegment muss ein Umstellungstermin festegelegt werden, an dem die Zuordnung der Netzwerkports zum Netzsegment geändert werden. An einem Termin kann auf mehrere neue Netzsegmente gleichzeitig umgestellt werden. Bei dem Termin konfiguriert der Netzwerkadministrator die Netzwerkports um und die betroffenen Geräte müssen sich im Anschluss eine neue IP-Adresse im neuen Netzsegment konfigurieren durch Erneuern des DHCP-Leases bzw. des Sendens einer Router Solication. Im Zweifelfsfall kann dies durch einen Neustart des Geräts erreicht werden. Es empfiehlt sich als IT-Administrator an dem Termin vor Ort zu sein, um notfalls lokal an den Geräten eingreifen zu können. Gibt es statische IP-Konfigurationen und keinen Baseboard Management Controller (BMC) beim entsprechenden Gerät, muss die IP-Konfiguration ohnehin vor Ort geändert werden.

5 Abgrenzung zur Mikrosegmentierung

Mikrosegmentierung meint eine weitere Unterteilung der Netzsegmente in einzelne Abschnitte, über deren Grenzen hinweg sich eine Bedrohung nicht weiter ausbreiten kann. Hierzu werden oft einzelne Nutzer isoliert und Firewall-Regeln basierend auf Nutzer-ID oder eines zugeordneten Gruppen-Tags umgesetzt. Mikrosegmentierung, auch Zero-Trust-Segmentierung ist unbedingte Voraussetzung für Zero Trust (siehe auch *Grundlagen des Zero-Trust-Ansatzes und Fallstudie am Beispiel des Netzwerks der Universität Mannheim* [5]). Oft wird die Mikrosegmentierung mittels sogenannter Next-Generation-Firewalls (NGFWs) durchgeführt.

6 Versionsverlauf

Version	Datum	Änderungen
1.0	6.10.2025	Initiale Veröffentlichung

Literaturverzeichnis

[1] *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*, 2000. Adresse: https://www.rfc-editor.org/info/bcp38.

[2] *Architekturbausteine für moderne und virtualisierte Netze*, 2025. Adresse: https://bwcampusnetz.de/page/publications/.

[3] *IPv6-only in Campusnetzen*, 2025. Adresse: https://bwcampusnetz.de/page/publications/.

[4] *LAN-Zugang für Benutzer, Geräte und IoT-Devices*, 2025. Adresse: https://bwcampusnetz.de/page/publications/.

[5] *Grundlagen des Zero-Trust-Ansatzes und Fallstudie am Beispiel des Netzwerks der Universität Mannheim*, 2025. Adresse: https://bwcampusnetz.de/page/publications/.