BWCAMPUSNETZ

Zukunftsfähige Konzepte für die Campusnetze
an Universitäten und Hochschulen

Blueprint Firewall-Architektur für kleinere Hochschulen oder Universitäten

Federführung bei der Erstellung dieses Dokuments: Universität Mannheim
Kontakt: team@bwcampusnetz.de

Inhalt

1 Einführung **3**

2 Netzwerkarchitektur **4**

2.1 Erstellen einer Netzwerkarchitektur in Anlehnung an IT BSI-Grundschutz . . 4

2.1.1 Weitere Segmentierung 5

2.2 Anforderungen aus BSI IT-Grundschutz, die nicht realisiert wurden 6

3 Die Firewalls **7**

3.1 Architektur der Firewalls 7

3.2 Installation und Konfiguration der Firewalls 8

4 Benötigte Prozesse **10**

5 Versionsverlauf **11**

Literaturverzeichnis **12**

1 Einführung

Historisch gewachsen wird an kleineren Hochschulen oder Universitäten gerne aus Kostengründen nur über Access Control Listen (ACLs) auf Netzwerkkomponenten wie Switches und Routern gefiltert. Das ist jedoch nicht ausreichend gemäß BSI IT-Grundschutz, da es sich hierbei um eine stateless (zustandslose) Firewall handelt, jedoch immer stateful (zustandsbehaftete) Firewalls gefordert werden. Deswegen ist es hiermit nicht möglich, ein ISO27001-Zertifikat basierend auf BSI IT-Grundschutz zu erreichen. Dieses Dokument beschreibt die Ergebnisse einer Umstellung eines flachen Campusnetzes mit stateless Firewalls in Form von ACLs auf den Routern zu einer möglichst einfachen, Firewall-basierten Lösung. Vor dem Hintergrund von wenig Geld und einer dünnen Personaldecke wurde hier eine möglichst einfache und rentable Lösung gefunden. Diese beinhaltet eine mächtige, redundante Next Generation Application Level Firewall und eine vorgeschaltete, günstige stateful Firewall.

2 Netzwerkarchitektur

2.1 Erstellen einer Netzwerkarchitektur in Anlehnung an IT BSI-Grundschutz

Das Wichtigste ist, zunächst eine Netzwerkarchitektur zu erstellen, die die notwendigen und gefordertenSicherheitsanforderungen erfüllt. Generell benötigt man ein Konzept, das den Schutzbedarf und benötigten Berechtigungen im Campusumfeld abbildet. Im BSI-Standard 200-2 (IT-Grundschutz-Methodik) ist das Vorgehen bei der Schutzbedarfsfeststellung so definiert, dass zunächst der Schutzbedarf der Geschäftsprozesse ermittelt wird. Daraus wird dann der Schutzbedarf der weiteren Assets abgeleitet. Hier wird davon ausgegangen, dass ein solches Konzept vorliegt, mit einer Einschätzung eines durchschnittlichen Campusnetzes. Ein Campusnetz ist weder ein komplett offenes Netzwerk noch ein Hochsicherheitsnetz. Die meisten Bereiche sind relativ unkritisch. Es gibt jedoch auch Netzsegmente, wie die der Verwaltung, die mit finanz- oder personenbezogenen Daten arbeitet, die einen höheren Schutzbedarf haben. Um einen solchen, relativ üblichen Schutzbedarf zu realisieren, kann eine der einfachsten Netzwerkarchitekturen verwendet werden. Außerhalb des Campusnetzes ist das Internet, abgetrennt durch eine Perimeter-Firewall. Danach folgen in einer demilitarisierten Zone (DMZ) sämtliche Server, die aus dem Internet erreichbar sind. Im Zentrum, geschützt hinter einer weiteren Firewall, befindet sich dann das Intranet, in diesem Fall das Campusnetz oder dessen größter Teil. Diese Architektur stellt gleichzeitig die Minimalkonfiguration oder auch die Standardkonfiguration des BSI IT-Grundschutzes dar, mit der eine Zertifizierung zu erreichen ist. Sie wird in Abbildung 2.1 dargestellt.

Für eine kleine Universität oder Hochschule ist es ausreichend, eine einfache DMZ für alle Services, die von außen erreichbar sein müssen, zu haben. Eine Besonderheit stellt der VPN-Zugang dar. Man kann den VPN-Server entweder in die DMZ stellen oder parallel dazu ansiedeln und mit einer eigenen Firewall ausstatten. Beides ist aus Sicherheitsgründen möglich und zu empfehlen. Zwischen DMZ und Intranet, in dem Fall dem Campusnetz, platziert man eine weitere stateful Firewall. Im Intranet können dann verschiedene Lehrstühle, Bereiche etc. oder auch vor allem besonders schutzbedürftige Bereiche wie die Verwaltung oder

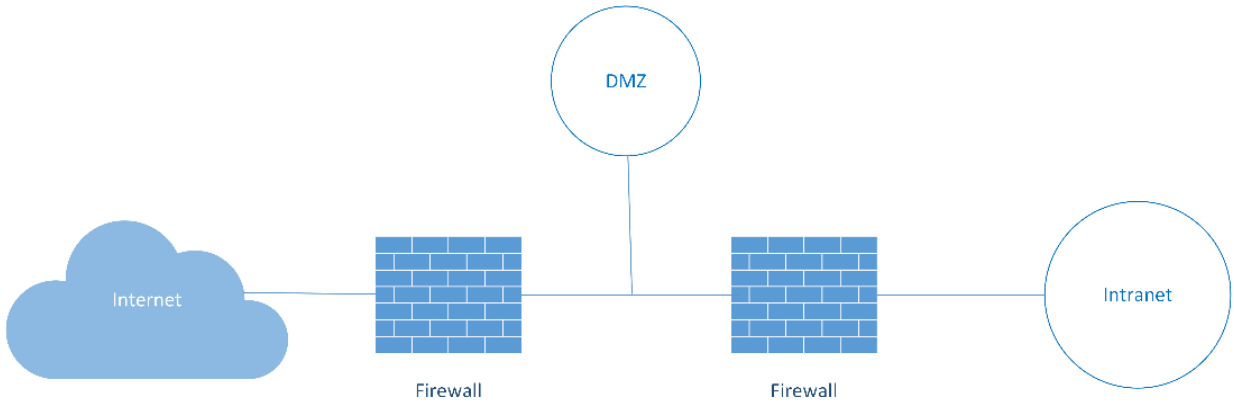

Abb. 2.1: Typische Netzarchitektur mit DMZ

Gebäudeleittechnik durch weitere Schutzmechanismen, wie Firewalls und separate Netzwerksegmente, voneinander getrennt werden. Schwer zu schützende Bereiche, die keinen Internetzugang benötigen (wie bspw. Teile der Gebäudeleittechnik) dürfen weder Zugriff auf das Internet haben noch vom Internet aus erreichbar sein. Empfehlenswert ist auch ein eigenes Netzwerksegment, um Netzkomponenten managen zu können. Dies wird nach Schutzbedarf entschieden, hier wird nicht weiter darauf eingegangen. Ganz selten kann es sinnvoll sein, bestimmte Netze ohne nennenswerten Schutzbedarf an der DMZ vorbei mehr oder weniger ungefiltert auf das Internet zu lassen. Dies ist z.B. für Gastnetze, für Netze mit geringen Sicherheits- aber dafür hohen Performanceanforderungen oder für Studierendenwohnheime möglich. Dieser Sonderfall wird in der unten beschriebenen Architektur behandelt.

2.1.1 Weitere Segmentierung

Innerhalb des Campusnetzes muss sinnvoll, nach Betriebs- und Sicherheitsgrundsätzen, segmentiert werden. Dies muss in diesem Kontext überprüft und ggf. ein derartiges Konzept erstellt werden. Speziell sind verschiedene Bereiche nach Nutzung zu separieren. So sollte ein Segment nur Geräte eines ähnlichen Schutzbedarfs beinhalten (bspw. nie Clients und Server in einem Segment sein) und ein wechselseitiger Schutz unterschiedlicher Organisationseinheiten berücksichtigt werden. Das BSI fordert ebenfalls ein eigenes Management-Netzwerk, um die Sicherheit beim Zugriff auf sicherheitsrelevante Komponenten zu erhöhen.

2.2 Anforderungen aus BSI IT-Grundschutz, die nicht realisiert wurden

Zu erwähnen ist in diesem Kontext noch, dass vom BSI IT-Grundschutz zusätzlich Security Proxies gefordert werden; diese sind in dieser Architektur nicht berücksichtigt. Ein Aufbrechen des verschlüsselten Verkehrs wird durch die meisten Universitäten abgelehnt. Ebenso sind die (entbehrlichen) Anforderungen, eine P-A-P-Struktur für die Internet-Anbindung zu schaffen, nicht umgesetzt worden, vgl [1]. Last not least ist der Umgang des BSI IT-Grundschutzes mit virtualisierten Netzwerkkomponenten, konkret mit dem Betrieb verschiedener Netzsegmente und Sicherheitskontexte auf der gleichen Hardware, aktuell in einer Phase des Umbruchs und muss, sobald die Weiterentwicklung des BSI IT-Grundschutzes abgeschlossen ist, noch betrachtet werden.

3 Die Firewalls

3.1 Architektur der Firewalls

Für die Firewall-Architektur wurde die in Abbildung 2.1 beschriebene Netzwerkarchitektur geringfügig verändert, siehe Abbildung 3.1.

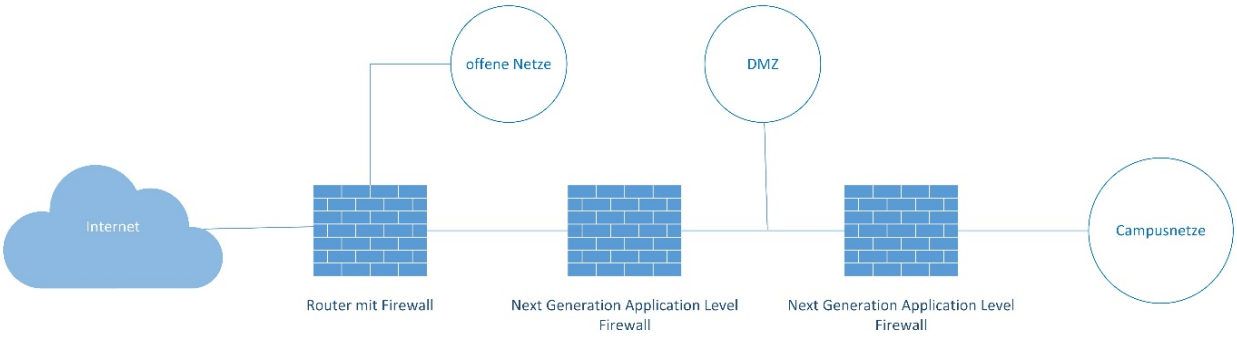

Abb. 3.1: Realisierte Netzarchitektur mit DMZ

Die in Abbildung 1 beschriebene Netzwerkarchitektur sieht zwei stateful Firewalls vor, die sich zwischen Internet und DMZ sowie zwischen DMZ und Intranet befinden. Dieser Ansatz wurde hier durch eine weitere, vorgelagerte Firewall ergänzt. Genau genommen wurden als Router, die das Internet mit dem Netz der Universität verbinden (Border-Router), redundante Switche mit Firewall-Funktionalität gewählt. Diese eingehenden (stateful) Firewalls sind preislich nur geringfügig teurer als Border-Router ohne Firewall-Funktionalität. Ihre Aufgabe ist es, fehlerhaften Traffic , bspw. Pakete mit fehlerhaftem Headern, overlapping Fragments oder Noise, auszusortieren und bestimmte, dahinter liegende Bereiche, zu schützen. Hier wird größtenteils noch nicht portgenau gefiltert, IP-Bereiche reichen aus. Auf die Art und Weise wird alles, was dahinter liegt, grundlegend geschützt und Angriffe auf die innen liegenden, die DMZ „umschließenden“ Firewalls verhindert. Zu erwähnen ist noch, dass einzelne Netzwerke ohne nennenswerten Schutzbedarf, wie bspw. Gastnetze oder Studierendenwohnheime, direkt über diese Router mit Firewall-Funktionalität angebunden sind. Diese Netze werden im Folgenden nicht weiter betrachtet. Dahinter wurde die übliche Firewall-Architektur umgesetzt; die hier eingesetzten Firewalls sind moderne Next Generation Application Level Firewalls.

Eine derartige Firewall untersucht den Traffic bis auf Layer 7. Sie enthält ebenfalls IDS- und IPS-Funktionalitäten. Diese sollten zur Erhöhung der Sicherheit genutzt werden.

Für die Dimensionierung der Firewall ist es wichtig zu wissen, welchen Datendurchsatz man zwischen Campusnetz und Internet hat. Oft wird der Internetanschluss nur partiell ausgelastet, daher sollte die Firewall auf Basis des tatsächlich anfallenden Datendurchsatzes und deren voraussichtlicher Entwicklung dimensioniert werden, und nicht basierend auf der theoretischen maximalen Bandbreite.

3.2 Installation und Konfiguration der Firewalls

Bei der Installation können die äußeren Router mit Firewallfunktionalität (Border-Router) und die dahinterliegenden Firewalls um die DMZ zeitlich getrennt in Betrieb genommen werden. Es erleichtert die Fehlersuche, wenn nur an einer Stelle neue Komponenten eingefügt werden. Für die Border-Router wurden einfache Regeln, größtenteils analog zu den vorherigen ACLs, ergänzt, um Regeln zum Schutz der dahinter liegenden Firewalls und gegen fehlerhaften Traffic , zu realisieren. Die beiden Next Generation Application Level Firewalls wurden zunächst „offen“ in das Netz eingebunden. Das bedeutet, dass erstmal sämtlicher Traffic durch sie laufen gelassen wurde, ohne dass Regeln diesen einschränkten. Die Analyse dieser Datenflüsse unterstützte die Erstellung von Firewall-Regeln. Ebenfalls hilfreich waren die Portscans durch das DFN, diese wiesen offene Ports der Server aus. Dieser Ansatz wurde gewählt, um ein möglichst passgenaues Regelwerk erstellen zu können. Wichtig ist hierbei auch, dass vom BSI ein Whitelisting gefordert wird. Das heißt, zunächst muss sämtlicher Traffic verboten und dann einzelne Verbindungen erlaubt werden. Hier konnten die ACLs aus den Switches, die bisher bis auf Layer 3 (stateless) gefiltert haben, nicht direkt übernommen werden. Sie boten jedoch Anhaltspunkte, was man durchlassen möchte und was nicht. Zusammen mit den gesammelten Verkehrsdaten und den Ergebnissen der DFN-Scans ließ sich herausarbeiten, welche Ports wirklich benötigt werden. Diese Ports konnten dann einzelnen Anwendungen zugeordnet und entsprechend freigeschaltet werden. Je nach Ausgangslage kann hier unterschiedlich vorgegangen werden, wichtig ist, dass am Ende ein möglichst genaues Regelwerk vorliegt. Vor der Inbetriebnahme der Firewall ist es wichtig, alle Administratoren und Lehrstühle zu kontaktieren und hierüber zu informieren. Ebenso muss der Service Desk mit eingebunden werden. Die Inbetriebnahme der Firewall-Regeln

sollte in einer Zeit ohne geplante Prüfungen oder Ähnliches stattfinden, da es sich nicht vollständig ausschließen lässt, dass durch Fehler in der Konfiguration Probleme mit benötigten Verbindungen auftreten.

4 Benötigte Prozesse

Generell benötigt der Betrieb einer Firewall Prozesse, die im Wesentlichen denen von sicherheitsrelevanten Komponenten entsprechen und sich in die normalen betrieblichen Prozesse integrieren. Einige wichtige sind im Folgenden exemplarisch aufgelistet. Damit die Firewall nicht selbst zum angreifbaren Ziel wird, muss sie regelmäßig überprüft und aktualisiert werden, alle Sicherheitsupdates müssen schnellstmöglich installiert werden. Die Firewall-Regeln müssen ebenfalls regelmäßig überprüft und ggf. angepasst werden, um die aktuelle Situation korrekt abzubilden und um neue Bedrohungen und Sicherheitsanforderungen zu berücksichtigen. Regelmäßige Audits erhöhen die Sicherheit und helfen, Sicherheitslücken zu identifizieren. Auch die Auswertung von Logfiles ist in diesem Zusammenhang wichtig. Sicherheitslücken müssen schnellstmöglich geschlossen werden. Generell ist Dokumentation (inkl. Sicherheitspolicies und -Vorgaben) wichtig und muss gepflegt und auf den neusten Stand gehalten werden. Alle Administratoren und relevanten Mitarbeiter müssen regelmäßig geschult werden, um sicherzustellen, dass sie über die neuesten Sicherheitspraktiken und Anforderungen informiert sind.

5 Versionsverlauf

Version	Datum	Änderungen
1.0	30.09.2025	Initiale Veröffentlichung

Literaturverzeichnis

[1] *Kommentare zur Anwendbarkeit und Umsetzung des BSI IT-Grundschutzes in Campusnetzen an Hochschulen*, 2025. Adresse: `https://bwcampusnetz.de/page/publications/`.