BWCAMPUSNETZ

Zukunftsfähige Konzepte für die Campusnetze
an Universitäten und Hochschulen

Kommentare zur Anwendbarkeit und Umsetzung des BSI IT-Grundschutzes in Campusnetzen an Hochschulen

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

Inhalt

1 Einleitung

In diesem Papier sollen die IT-Grundschutzbausteine [1] für Datennetze des IT-Grundschutzkompendium [2] des BSI kommentiert werden in Bezug auf Anwendbarkeit und Umsetzung in Campusnetzen an Hochschulen aus Sicht von Netzbetreibern an Hochschulen in Baden-Württemberg. Im Rahmen des Projekt bwCampusnetz wurden moderne Netzarchitekturen evaluiert und Architekturbausteine in einem Kompendium veröffentlicht.[3] Weiterhin wurde das Thema Firewall als zentraler Baustein einer sicheren Netzarchitektur behandelt. Betrachtet wurden daher die Bausteine NET.1.1 (Netzarchitektur und -design), NET.3.2 (Firewall) und teilweise NET.3.1 (Router und Switches).

Im Folgenden wird auch eine kleine Einführung in die relevanten Begrifflichkeiten und Prozesse des IT-Grundschutz gegeben, die notwendig sind, um zu verstehen, wie die Bausteine zu betrachten sind.

Die in diesem Dokument ausgesprochenen Empfehlungen und Einschätzungen bzgl. Konformität von Maßnahmen mit dem BSI IT-Grundschutz stammen allesamt von Netzbetreibern an Hochschulen in Baden-Württemberg, sind also insbesondere keine Aussagen des BSI.

2 Schutzbedarf im IT-Grundschutz

Zentrale Schutzziele: Vertraulichkeit, Integrität, Verfügbarkeit

Schutzbedarf von Zielobjekten

- „normal“ : Die Schadensauswirkungen sind begrenzt und überschaubar.
- „hoch“ : Die Schadensauswirkungen können beträchtlich sein.
- „sehr hoch“ : Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

An einer Hochschule besteht größtenteils normaler Schutzbedarf, teilweise erhöhter Schutzbedarf. Zur Schutzbedarffeststellung siehe IT-Grundschutz-Methodik (200-2). [4]

Eine Kommunikationsverbindung/Netz bedient im Regelfall mehrere Services, das Maximum der Schutzbedarfe dieser Services ist der Schutzbedarf der Kommunikationsverbindung bzw. des Netzes. Insofern erhalten wir bei Netz-/Kommunikationsverbindungen meist den Schutzbedarf hoch. (Maximumsprinzip)

3 IT-Grundschutzbausteine in der Schicht NET

Ein IT-Grundschutz-Baustein wird auf ein Zielobjekt aus dem Informationsverbund angewendet. Die Zielobjekte in der Schicht NET (Netze und Kommunikation) sind Netzkomponenten (Router, Firewalls etc.), Netz-Clients, Netzverbindungen, Netzmanagement-Systeme und die Netze selbst. Die Schicht NET enthält System-Bausteine, keine Prozess-Bausteine.

> „Die Schicht NET betrachtet die Vernetzungsaspekte, die sich nicht primär auf bestimmte IT-Systeme, sondern auf die Netzverbindungen und die Kommunikation beziehen. Dazu gehören zum Beispiel die Bausteine Netz-Management, Firewall und WLAN-Betrieb.“ BSI-Standard 200-2: IT-Grundschutz-Methodik [4]

Für die Bausteine gibt es verschiedene Typen von Anforderungen.

- B = Basis-Anforderung
  - Fundamental und stets umzusetzen, sofern nicht gravierende Gründe dagegen sprechen.
- S = Standard-Anforderung
  - Für den normalen Schutzbedarf grundsätzlich umzusetzen, sofern sie nicht durch mindestens gleichwertige Alternativen oder die bewusste Akzeptanz des Restrisikos ersetzt werden.
- H = Anforderung bei erhöhtem Schutzbedarf
  - Exemplarische Vorschläge, was bei entsprechendem Schutzbedarf zur Absicherung sinnvoll umzusetzen ist.

Sind die Anforderungen aus dem Baustein beim Zielobjekt umgesetzt?
Mögliche Antworten: ja / teilweise / nein / entbehrlich

4 Begriffe in NET.1.1 und NET.3.2

Im IT-Grundschutz-Kompendium des BSI werden viele Begriffe verwendet, ohne dass sie definiert werden. Daher wurde versucht, Definitionen in anderen Dokumenten des BSI oder ähnlichen Dokumenten zu finden. Wenn dies auch nicht möglich war, wurde versucht, selbst eine Definition zu erstellen, die sich mit der Verwendung im IT-Grundschutz deckt.

4.1 Netzwerksegment

Ein Netzwerksegment ist in der Regel ein Layer-2-separiertes Netz, eine Broadcastdomain. Die Segmente sind durch Router voneinander getrennt. Sie müssen jedoch noch nicht zwangsweise durch eine Firewall voneinander getrennt sein. Wenn im IT-Grundschutz von der Notwendigkeit physischer Trennung gesprochen wird, sind die Netze bereits auf Layer-1 zu separieren.

4.2 Zone

In einer Netzzone werden Systeme gesammelt, die einen ähnlichen Schutzbedarf haben. Dieser Begriff soll mangels klarer Definition durch Zitate aus dem IT-Grundschutz beschrieben werden.

4.2.1 Physische Separierung in drei Zonen

> „Das Gesamtnetz MUSS mindestens in folgende drei Zonen physisch separiert sein: internes Netz, demilitarisierte Zone (DMZ) und Außenanbindungen (inklusive Internetanbindung sowie Anbindung an andere nicht vertrauenswürdige Netze). Die Zonenübergänge MÜSSEN durch eine Firewall abgesichert werden.“ (NET.1.1.A4)

4.2.2 Eigenschaften von Zonen

> „Jedoch müssen allgemeine Anforderungen an die Architektur und das Design, z. B. dass Zonen gegenüber Netzsegmenten immer eine physische Trennung erfordern, für alle Netztechniken beachtet und erfüllt werden.“ (NET1.1, Beschreibung 1.3)

Zonen können segmentiert werden. (NET.1.1.A1)

4.2.3 DMZ (Demilitarisierte Zone)

DMZ ist ein weit verbereiteter Begriff, eine eindeutige Definition fehlt.

Im Rahmen dieses Dokuments beschreibt der Begriff DMZ ein Netzwerksegment, in dem Dienste bereitgestellt werden, die sowohl von außen als auch von innen erreicht weden sollen. Durch die Erreichbarkeit von außen ist die Angriffsfläche erhöht, somit sollen die entsprechenden Server nicht ohne weiteren Schutz das interne Netz erreichen. Auch gegenüber dem Internet soll die DMZ geschützt sein. Daher bietet es sich bei einem zweistufigen Firewallkonzept an, die DMZ zwischen den beiden Perimeter-Firewalls zu plazieren.

4.2.4 Internes Netz / Intranet

„Intranet“ ist vermutlich deckungsgleich mit „internes Netz“. In NET.1.1 wird der Begriff in folgender Weise genutzt: „Das Gesamtnetz MUSS mindestens in folgende drei Zonen physisch separiert sein: internes Netz, demilitarisierte Zone (DMZ) und Außenanbindungen“ (NET.1.1.A4)

> „Nicht vertrauenswürdige Netze (z. B. Internet) und vertrauenswürdige Netze (z. B. Intranet) MÜSSEN mindestens durch eine zweistufige Firewall-Struktur, bestehend aus zustandsbehafteten Paketfiltern (Firewall), getrennt werden.“ (NET.1.1.A4)

4.2.5 Extranet

Das Extranet befindet sich außerhalb des Intranets außerhalb der externen Firewall. Im Extranet befinden sich Systeme und Anwender, die nicht zur Einrichtung gehören. Hier bzw. angrenzend befinden sich auch die Außenanbindungen inklusive Internetanbindung.

4.3 Firewall

Eine Firewall ist ein Paketfilter, durch den Netzwerkverkehr geleitet wird. Verschiedene Zonen dürfen nach BSI-Grundschutz nur über eine Firewall verbunden werden. Netzsegmente derselben Zone können per Firewall oder Router verbunden werden. Eine Firewall kann zustandsbehaftet oder zustandslos sein. Ein Beispiel für eine zustandslose Firewall sind Router-ACLs. Eine Host-Firewall ist eine Firewall auf einem Endgerät.

4.3.1 Application-Layer-Gateway (ALG) / Sicherheits-Proxy

Paketfilter, Firewall und Application Level Gateway (ALG) sind unterschiedliche Dinge. Die Begriffe Application-Layer-Gateway (ALG) und Sicherheits-Proxy werden synonym vewendet.

- Paketfilter / Firewall
  - Filterung auf Vermittlungsschicht (Layer 3) und Transportschicht (Layer 4)
  - Firewall wird meist synonym mit zustandsbehafteter Firewall verwendet. Paketfilter meint meist einfache zustandslose Router-ACLs.
- Application Level Gateway / Sicherheits-Proxies
  - Filterung auf Anwendungschicht (Layer 7)
  - Payload wird gefiltert
  - Verbindungen werden vom ALG entkoppelt

5 Betrachtung der IT-Grundschutzbausteine in der Schicht NET

Es wurden die Anforderungen in den Bausteinen NET.1.1 und NET.3.2 untersucht. Anforderungen, die Richtlinien, Dokumentationen, Planungen, Spezifikationen oder Maßnahmen enthalten, wurden nur am Rande betrachtet und werden hier auch nicht aufgelistet. Der Fokus lag auf den Anforderungen, die konkrete Eigenschaften der Netzarchitektur enthalten.

5.1 NET.1.1: Netzarchitektur und -design

In diesem Baustein ist das Zielobjekt das Gesamtnetz der Institution:

> „Der Baustein NET.1.1 Netzarchitektur und -design ist auf das Gesamtnetz einer Institution inklusive aller Teilnetze anzuwenden. Der Baustein enthält grundsätzliche Anforderungen, die zu beachten und erfüllen sind, wenn Netze geplant, aufgebaut und betrieben werden. Anforderungen für den sicheren Betrieb der entsprechenden Netzkomponenten, inklusive Sicherheitskomponenten wie z. B. Firewalls, sind nicht Gegenstand des vorliegenden Bausteins. Diese werden in der Bausteingruppe NET.3 Netzkomponenten behandelt.“ NET.1.1 1.3 Abgrenzung und Modellierung

Zielsetzung: Etablierung der Informationssicherheit als integralen Bestandteil der Netzarchitektur und des Netzdesigns. Gewünschtes Ergebnis: Sichere Netzarchitektur.

Die Verfügbarkeit des Netzes spielt auch eine Rolle, siehe NET.1.1 „2.1. Ausfall oder unzureichende Performance von Kommunikationsverbindungen“ .

Sicherheitsrelevante Aspekte:

- sichere Trennung verschiedener Mandanten und Gerätegruppen auf Netzebene

- Kontrolle ihrer Kommunikation durch eine Firewall
- Netzzugangskontrolle für Clients

5.1.1 Basisanforderungen

- NET.1.1.A4: Netztrennung in Zonen
- NET.1.1.A5: Client-Server-Segmentierung
- NET.1.1.A6: Endgeräte-Segmentierung im internen Netz
- NET.1.1.A7: Absicherung von schützenswerten Informationen
- NET.1.1.A8: Grundlegende Absicherung des Internetzugangs
- NET.1.1.A9: Grundlegende Absicherung der Kommunikation mit nicht vertrauenswürdigen Netzen
- NET.1.1.A10: DMZ-Segmentierung für Zugriffe aus dem Internet
- NET.1.1.A11: Absicherung eingehender Kommunikation vom Internet in das interne Netz
- NET.1.1.A12: Absicherung ausgehender interner Kommunikation zum Internet

5.1.2 Standardanforderungen

- NET.1.1.A18: P-A-P-Struktur für die Internet-Anbindung
- NET.1.1.A19: Separierung der Infrastrukturdienste
- NET.1.1.A20: Zuweisung dedizierter Subnetze für IPv4/IPv6-Endgerätegruppen
- NET.1.1.A21: Separierung des Management-Bereichs
- NET.1.1.A23: Trennung von Netzsegmenten
- NET.1.1.A24: Sichere logische Trennung mittels VLAN

5.1.3 Anwendbarkeit und Umsetzung für Campusnetze

Die Anforderungen, die die Segmentierung von Netzen und die Absicherung von schützenswerten Informationen betreffen, sind unstrittig und in den Zielarchitekturen aller Partner umsetzbar. Die Netztrennung in drei Zonen ist zwar prinzipiell bei den Zielarchitekturen aller Partner umsetzbar, aber Begrifflichkeiten wie z. B. „DMZ“ sind auch beim BSI nicht genau definiert.

Die Umsetzung der physischen Separierung wird derzeit aus Gründen der Skalierbarkeit, Flexibilität und Unwirtschaftlichkeit nicht angestrebt. Vom BSI haben wir die Aussage erhalten, dass sie das Thema (stark) virtualisierte Netzarchitekturen im bestehenden IT-Grundschutz gar nicht mehr behandeln werden, sondern im IT-Grundschutz++ (noch nicht veröffentlichte Weiterentwicklung des IT-Grundschutz).

Die Absicherung ausgehender interner Kommunikation zum Internet wird mehrheitlich nicht angestrebt, da ein Aufbrechen des verschlüsselten Verkehrs durch uns als Universitäten grundsätzlich abgelehnt wird. Außerdem hat unsere Rückfrage an das BSI keine konkreten Anforderungen an die Eigenschaften eines Sicherheits-Proxies ergeben. Es sind dahingehend keine geeigneten Produkte bekannt.

Eine P-A-P-Struktur für die Internet-Anbindung wird mehrheitlich nicht angestrebt, dies kann aber als entbehrliche Anforderung entsprechend begründet werden, was weiter unten ausgeführt wird.

5.2 NET.3.2: Firewall

> „Der Baustein NET.3.2 Firewall ist immer auf jede Firewall des Informationsverbunds anzuwenden.“ NET.3.2 1.3 Abgrenzung und Modellierung

Der Baustein baut auf den Baustein NET.1.1 Netz-Architektur und -design auf und enthält konkrete Anforderungen, die zu beachten und zu erfüllen sind, wenn netzbasierte Firewalls beschafft, aufgebaut, konfiguriert und betrieben werden.

5.2.1 Basisanforderungen

- NET.3.2.A2: Festlegen der Firewallregeln
- NET.3.2.A3: Einrichten geeigneter Filterregeln am Paketfilter
- NET.3.2.A4: Sichere Konfiguration der Firewall
- NET.3.2.A6: Schutz der Administrationsschnittstellen
- NET.3.2.A7: Notfallzugriff auf die Firewall
- NET.3.2.A8: Unterbindung von dynamischem Routing
- NET.3.2.A9: Protokollierung
- NET.3.2.A10: Abwehr von Fragmentierungsangriffen am Paketfilter

5.2.2 Standardanforderungen

- NET.3.2.A16: Aufbau einer „P-A-P„-Struktur
- NET.3.2.A17: Deaktivierung von IPv4 oder IPv6
- NET.3.2.A18: Administration über ein gesondertes Managementnetz
- NET.3.2.A19: Schutz vor TCP SYN Flooding, UDP Paket Storm und Sequence Number Guessing am Paketfilter
- NET.3.2.A20: Absicherung von grundlegenden Internetprotokollen
- NET.3.2.A21: Temporäre Entschlüsselung des Datenverkehrs
- NET.3.2.A22: Sichere Zeitsynchronisation

5.2.3 Anwendbarkeit und Umsetzung für Campusnetze

In NET.3.2 sind grundsätzlich nur Anforderungen umsetzbar, die durch die eingesetzte Firewall unterstützt werden. Teilweise sind daher Anforderungen nicht umsetzbar, die aber auch nicht als kritisch gesehen werden.

Zwei Punkte wurden identifiziert, die aus unserer Sicht Campusnetze nicht passend sind: Das ist einerseits die Unterbindung des dynamischen Routings. Moderne Routingprotokolle sind abgesichert und Anforderungen wie Anycast-Redundanz in einem großen und dynamischen Netz können ohne dynamisches Routing nicht erfüllt werden. Das BSI konnte die Frage nicht abschließend beantworten, da derzeit eine Überarbeitung des IT-Grundschutzes stattfindet. Die zweite Anforderung, die von uns als Universitäten wie bereits oben erwähnt nicht umgesetzt wird, ist die temporäre Entschlüsselung des Datenverkehrs.

6 „P-A-P“-Struktur

Eine P-A-P-Struktur besteht aus Paketfilter – Application Layer Gateway – Paketfilter.

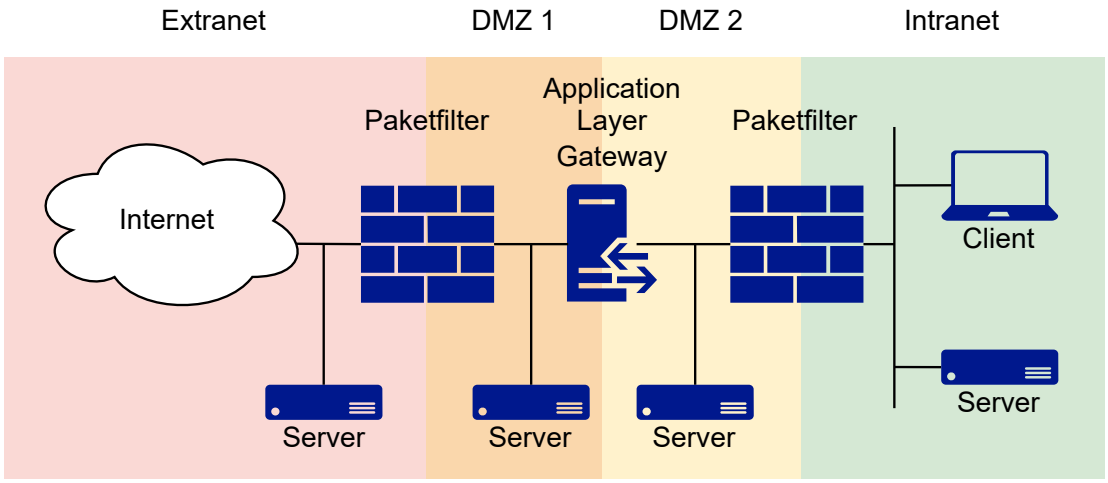

Abb. 6.1: P-A-P: Application Layer Gateway zwischen zwei Paketfiltern

Application Level Gateways (ALGs) bzw. Sicherheits-Proxies haben grundsätzlich das Problem, dass das Ende-zu-Ende-Prinzip verletzt wird, da die ALGs per Definition auf der Anwendungsebene (Layer 7) und nicht in der Netzwerkschicht (Layer 3) agieren. Darüberhinaus leidet in vielen Fällen die Performance, da die ALGs Datenverkehr bis zur Anwendungsschicht verarbeiten müssen, was sich nicht, wie z.B. die reine Weiterleitung von Paketen, in Hardware implementieren lässt. In akademischen Campusnetzen werden jedoch viele Anwendungen genutzt, welche eine hohe Performance oder geringe Latenz erfordern. Weiterhin handelt es sich um eine weitere mögliche Fehlerquelle, die das Debugging erschwert: Die strikte Trennung zwischen Netzwerk und Anwendung wird verletzt, bei der netzseitigen Fehlersuche muss auch die Anwendungsebene betrachtet werden, was in vielen Fällen Spazialwissen erfordert. Auch ist die Erkennung von „schadhaftem Verkehr“ gar nicht immer möglich, da Tunnel-Techniken dies verhindern können. Schon aus diesen Gründen ist genau abzuwägen, ob man einen Sicherheits-Proxy einsetzen möchte oder nicht.

In akademischen Campusnetzen kommen weitere Gründe hinzu, die gegen einen Sicherheits-Proxy sprechen: Grundsätzlich steht das Konzept eines Sicherheits-Proxies der Freiheit von Forschung und Lehre entgegen, insbesondere da ein Sicherheits-Proxy das Aufbrechen von Verschlüsselung erfordert. Auch könnten sich rechtliche Probleme bei Privatnutzung durch Mitarbeitende oder Studierenden ergeben.

7 Segmentierung von Netzen

Die Netzsegmentierung ist eine ganz zentrale Sicherheitsmaßnahme, die aus unserer Sicht auch für Campusnetze uneingeschränkt anzuwenden ist. Einige Bausteine beziehen sich auf dieses Thema, die umgesetzt werden müssen. Schon die Layer-2-Segmentierung ohne Trennung durch Firewalls auf Layer-3 bringt einen Sicherheitszuwachs, da sich Angreifer oft in der Layer-2-Domain ausbreiten. Weitere Sicherheit erlangt man durch die Trennung der Netzsegmente durch eine Firewall. Zum Thema Netzsegmentierung in Campusnetzen wurde im Projekt ein Leitfaden [5] verfasst.

8 Best Practice

Das Ziel ist eine Netzarchitektur zu entwerfen, mit der die Informationssicherheit gemäß IT-Grundschutz umgesetzt werden kann. Neben der Netzsegmentierung innerhalb des ganzen Netzes ist die Unterteilung in Zonen und die Umsetzung der Trennung von Systemen verschiedenen Schutzbedarfs zentral.

Eine möglichst zustandsbehaftete Firewall zur Trennung des Internets vom internen Netz ist zu verwenden. Die vom BSI geforderte Zweistufigkeit kann in verschiedenen Ausprägungen je nach Größe des Netzes umgesetzt werden.

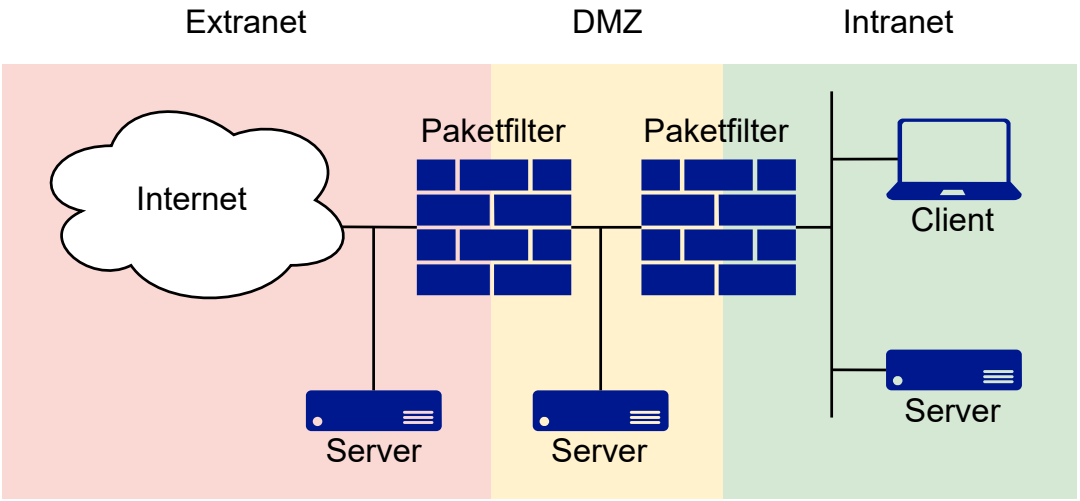

Abb. 8.1: Klassisches Netzdesign mit DMZ

8.1 Kleinere Netze

Für kleinere Netze bietet sich das klassische, auch vom BSI vorgeschlagene Design mit einer DMZ zwischen zwei Perimeter-Firewalls an, in der alle Systeme angebunden werden, die aus dem Internet erreichbar sein sollen. Im internen Netz können dann alle Systeme frei kommunizieren, sollten aber dennoch in Layer-2-Segmente separiert sein. Gegebenfalls können

Systeme mit besonders hohem Schutzbedarf wie in der Verwaltung durch eine separate Firewall noch weiter geschützt werden. Hier geht man von der Vertrauenswürdigkeit der Systeme im internen Netz aus.

8.2 Größere akademische Campusnetze

In größeren Netzen und insbesondere großen akademischen Campusnetzen, die unterschiedlichste Teilnehmer beherbergen, kann man allerdings von vorneherein nicht davon ausgehen, dass sich im Intranet nur vertrauenswürdige Systeme befinden, da die verwendeten Systeme oft nicht zentral verwaltet werden und auch zumeist keine allumfassende Kontrolle über den Zugang zum Netz (LAN-Dosen) besteht. Darüber hinaus werden auch oft private Geräte verwendet (BYOD), z. B. von Studierenden. Daher sollten zumindest Systeme mit hohem Schutzbedarf, wie z. B. die Systeme der Verwaltung mit personenbezogenen Daten, durch eine Firewall vor den restlichen Netzsegmenten im internen Netz geschützt werden.

In akademischen Campusnetzen gibt es außerdem meist dezentrale Netzwerkadministratoren, die die Anforderungen der Forschenden an ihrem Institut umsetzen müssen. Das bedeutet auch die Möglichkeit, Systeme aus dem Internet erreichbar zu machen. Daher benötigt man die Flexibilität, beliebige Netzsegmente zu definieren, die aus dem Internet erreichbare Systeme enthalten. Statt diese nun alle in der DMZ anzusiedeln, ist eine Möglichkeit, prinzipiell jedes Netzsegment gegenüber den anderen Netzsegmenten – auch im internen Netz – durch eine Firewall zu schützen. Hierdurch wird das Netz in noch mehr Zonen unterteilt und man schafft einen Schutz auch innerhalb des internen Netzes. Da jedes interne Netzsegment selbst noch einmal geschützt ist, sind eventuelle Freischaltungen aus dem Internet ohne Weiteres zu begründen. Diese Lösung adressiert auch die oben beschriebene Situation, dass in akademischen Campusnetzen generell nicht davon ausgegangen werden kann, dass sich im Intranet nur vertrauenswürdige Systeme befinden. Jedes System im internen Netz ist hiermit nicht mehr davon abhängig, dass sich der Rest des Netzwerks vorschriftsmäßig verhält, sondern ist in jedem Fall geschützt.

Dieses Konzept ersetzt vollständig das Konzept der DMZ. Aus der Basis-Anforderung NET.1.1.A4 „Netztrennung in Zonen“ : Nicht vertrauenswürdige Netze (z. B. Internet) und vertrauenswürdige Netze (z. B. Intranet) MÜSSEN mindestens durch eine zweistufige Firewall-Struktur, bestehend aus zustandsbehafteten Paketfiltern (Firewall), getrennt

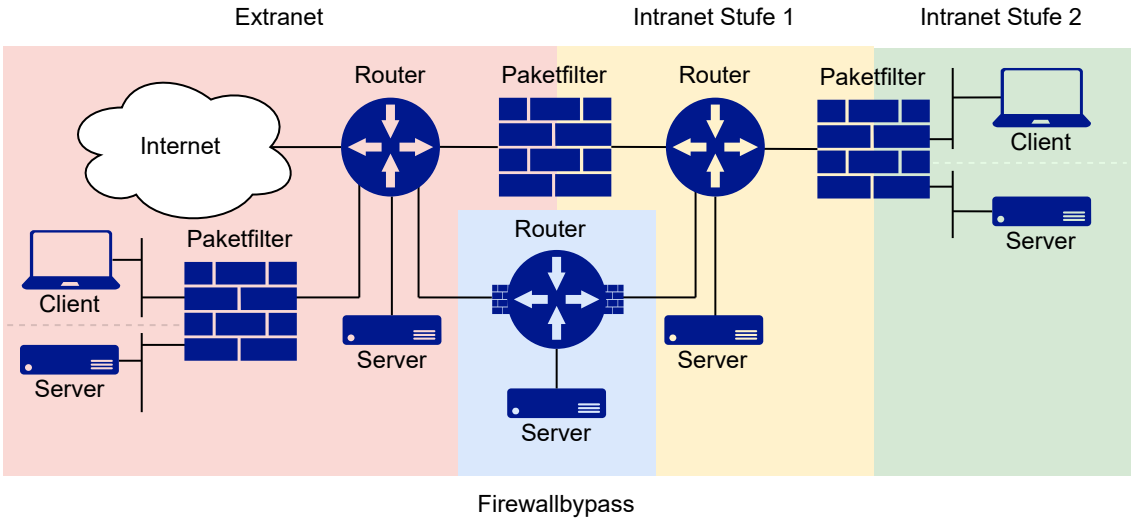

Abb. 8.2: Alternatives Netzdesign ohne DMZ

werden. Um Internet und externe DMZ netztechnisch zu trennen, MUSS mindestens ein zustandsbehafteter Paketfilter eingesetzt werden.

In der beschriebenen alternativen Umsetzung sind sowohl die aus dem Internet erreichbaren Systeme als auch die Systeme im internen Netz vor dem Internet und vor den Systemen in anderen Segmenten des internen Netzes durch eine oder mehrere Firewalls geschützt. Sie sind somit aus dem Internet selbst und vor allen aus dem Internet erreichbaren Systemen geschützt. Auch die Anzahl der Firewalls entspricht der in der DMZ-Achitektur. Vor dem Internet schützen zwei Firewalls und vor aus dem Internet erreichbaren Systemen schützt eine Firewall. Von der Netzarchitektur her gesehen könnte man die DMZ als diejenigen Netzsegmente bezeichnen, die nur vor dem Internet durch eine Firewall geschützt sind, und wie oben beschrieben dann aber vor anderen Systemen im internen Netz z. B. durch Hostfirewalls oder auch zustandlose Router-ACLs geschützt sind. Die DMZ wäre dann so etwas wie die Zone für Systeme, die untereinander ohne Firewall kommunizieren können sollen, aus Gründen wie z. B. hohe Anforderungen an Bandbereite, Latenz und Jitter.

Weiterhin ist eine praktikable Möglichkeit, eine Netzarchitektur aufzubauen, die die hier beschriebene Lösung ermöglicht, aber dennoch zunächst die Netzsegmente mit hohem Schutzbedarf zusätzlich durch eine zweite Firewall und somit vor den restlichen Segmenten im internen Netz zu schützen. Sukzessive ist es dann möglich, weitere Netzsegmente ebenfalls hinter die zweite Firewall umzuziehen.

Folgend werden zwei weitere Netzwerkzonen erläutert, die in Campusnetzen oftmals Anwendungsfälle haben.

8.2.1 Firewallbypass

Besteht Bedarf an Netzsegmenten, die nicht durch eine Firewall geschützt werden, ist dies entsprechend zu begründen und es müssen Vorkehrungen durch andere Maßnahmen getroffen werden, etwa durch den Einsatz von Hostfirewalls. In akademischen Campusnetzen gibt es Systeme, die mit hohen Bandbreiten oder niedriger Latenz bzw. Jitter sowohl mit dem Internet als auch mit dem Intranet kommunizieren müssen. Dazu ist es erforderlich, dass der Verkehr keine zustandsbehaftete Firewall passiert. Das Netzsegment wird hierfür über einen sogenannten Firewallbypass-Router angebunden, der sich ohne Firewall zwischem dem Intranet und dem Internet befindet. Für diese Form der Anbindung ist es unbedingte Voraussetzung, dass die Systeme über eine Hostfirewall und die Serveradministratoren über sehr gute Kenntnisse in diesem Bereich verfügen. Der Firewallbypass-Router muss so implementiert sein, dass Systeme im Intranet über diesen Weg nicht aus dem Extranet/Intranet erreichbar sind, so dass das normale Schutzkonzept für die Systeme im Intranet weiter greift. Zusätzlich ist die Konfiguration von zustandlosen Router-ACLs für die Netzsegment im Firewallbypass durch die Netzwerkadministatoren möglich.

8.2.2 Extranet

Externe Teilnehmer im Netz der Einrichtung, wie z. B. Gäste im WLAN, sollten wie das Internet behandelt werden und direkt am Internetrouter angeschlossen werden und somit zwei Firewalls passieren, um das Intranet zu erreichen. In akademischen Campusnetzen ist als Beispiel Education Roaming (eduroam) zu nennen. Hierbei handelt es sich um eine Initiative, die Mitarbeitern und Studierenden von partizipierenden Hochschulen und Organisationen einen Internetzugang gewährt. Weitere Beispiele für eine Anbindung im Extranet können Projekte mit externen Partnern sein. Es ist sehr zu empfehlen, diese Netzsegmente für Gäste ebenso mit einer Firewall gegenüber dem Internet abzusichern. Es kann im Extranet aber auch Netzsegmente geben, die man nicht mit einer Firewall der Organisation absichern will, da sie beispielsweise ihre eigene Firewall verwenden möchten.

9 Fazit

Vieles aus dem BSI IT-Grundschutz ist auch in akademischen Campusnetzen gut anzuwenden. Anderes ist nicht für diese Größenordnung und nicht für das Wesen von akademischen Campusnetzen mit dem Grundsatz der Freiheit von Forschung und Lehre gedacht. In diesem Dokument wurde eine Architektur vorgestellt, die den Anforderungen, die Forschung und Lehre an große Campusnetze stellen, genügt, und gleichzeitig möglichst viele der im BSI IT-Grundschutz beschriebenen Sicherheitsanforderungen abdeckt.

10 Versionsverlauf

Version	Datum	Änderungen
1.0	6.10.2025	Initiale Veröffentlichung
1.1	7.10.2025	Kapitel zu P-A-P überarbeitet.

Literaturverzeichnis

[1] *IT-Grundschutz-Bausteine*, 2023. Adresse: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html.

[2] *IT-Grundschutz-Kompendium*, 2023. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf.

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

[4] *BSI-Standard 200-2: IT-Grundschutz-Methodik, Version 1.0*. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html.

[5] *Leitfaden Netzsegmentierung in Campusnetzen*, 2025. Adresse: https://bwcampusnetz.de/page/publications/.