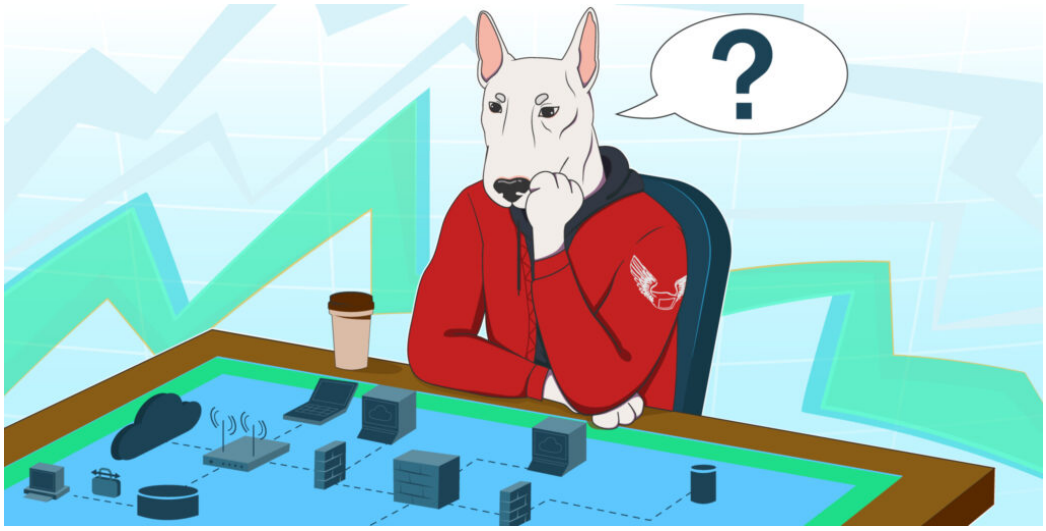


Netzwerksegmentierung und IT-Sicherheit

Inhalt



# Netzwerksegmentierung – Ein unterschätztes Instrument in der IT-

# Sicherheit Teil 2

Nachdem wir im ersten Teil die Basics der Netzwerksegmentierung erläutert haben, möchten wir im zweiten Teil mehr in die technische Tiefe gehen. Dazu haben wir unseren Sicherheits-Experten Nox eingeladen. Nox sind die BSI IT-Grundschutz Bausteine schon länger ein Begriff. Während der Zeit im Homeoffice hatte Nox Zeit sich mit dem Punkt „NET – Netzwerke und Kommunikation“ beschäftigt. Der Auszubildene Paul ist an dieser Thematik ebenso interessiert und sucht das Gespräch mit Nox.

## BSI Grundschutz NET.1.1: Netzarchitektur und –design

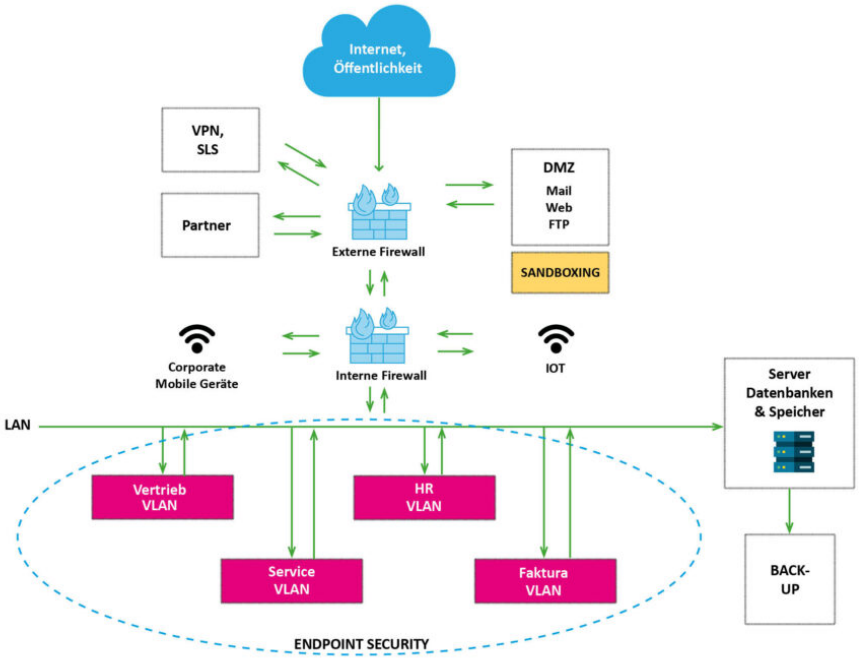
Besonders interessant für die Netzwerksegmentierung hält Nox den Punkt NET.1.1. Hier steht:

*„Um ein hohes Sicherheitsniveau zu gewährleisten, sind zusätzliche sicherheitsrelevante Aspekte zu berücksichtigen. Beispiele hierfür sind eine sichere Trennung verschiedener Mandanten und Gerätegruppen auf Netzebene und die Kontrolle ihrer Kommunikation durch Firewall-Techniken. Ein weiteres wichtiges Sicherheitselement, speziell im Client-Bereich, ist außerdem die Netzzugangskontrolle.“*

Das hat Paul schon einmal gehört und hängt Nox an den Lippen.

Dieser geht weiter ins Detail. Das BSI fordert darin pauschal die strikte Trennung von Clients und Servern, siehe Anforderung NET.1.1.A5 Client-Server-Segmentierung: „Clients und Server müssen in unterschiedlichen Sicherheitssegmenten platziert

werden. Die Kommunikation zwischen diesen Segmenten muss mindestens durch eine Firewall kontrolliert werden.“ Außerdem wird eine bedarfsorientierte weitere Unterteilung des Netzes in Sicherheitssegmente empfohlen, die sich am Schutzbedarf der IT-Systeme orientiert. Nox zückt einen Stift und stellt die Segmentierung schematisch dar.




Netzwerksegmentierung “Sicherer Perimeter” mit zweistufiger Firewall

Das Ergebnis ist eine Separierung unterschiedlicher Gruppen im Netz mit den Mitteln von beispielsweise VLANs. Die Übergänge zwischen den so geschaffenen Segmenten (Sicherheitszonen) werden meist durch Firewalls gebildet, die den ein- und ausgehenden Verkehr kontrollieren können.

Paul versteht nur Bahnhof, sodass Nox nochmal einen Schritt zurückgeht.

# Die Basics der

# Netzwerksegmentierung

Bei der Segmentierung werden dem Unternehmensnetzwerk sprichwörtlich Türen und Wände eingebaut. Aus technischer Sicht wird das gesamte Netzwerk in einzelne Netzwerksegmente, also IP-Subnetze, unterteilt. Technisch und auch organisatorisch bedingt kann dies eine große Zahl Segmente ergeben, jedoch ist nicht für jedes einzeln eine Schutzbedarfs-Abklärung nötig. Kriterien können zum Beispiel sein, ob die enthaltenen Systeme unmittelbar mit dem Internet verbunden sind, ob die Geräte direkt im Benutzerzugriff stehen oder ob im Segment sogar unkontrollierbare Fremdgeräte platziert werden können.

## In welche Netzwerkzonen kann man pauschal segmentieren?

Die wichtigsten Stereotypen und Grundgedanken seien aber erwähnt:

### «Trusted» Zonen:

Sind Zonen, in welchen ausschliesslich verwaltete Geräte mit bekannter Konfiguration und bekanntem Gesundheitszustand zu finden sind. Ein Bespiel wäre ein gut geschütztes Client-Netz. In unserer Grafik in Magenta dargstellt. Jener Zonentyp garantiert implizit, dass keine Gefahr für die Nutzer der Zone durch Fremdgeräte herrscht. Für Netzwerksegmente, welche Server/Services beinhalten, ist dies leicht zu garantieren. Die einzige Schnittstelle ist der Zonenübergang an der Firewall. Alle Systeme darin werden von Administratoren bereitgestellt und betrieben. Eine Herausforderung hingegen sind die

Clientnetzwerksegmente. Einerseits sitzen hinter den Clients Benutzer, welche bei unzureichender Schutzkonfiguration aus Unwissenheit oder Absicht Unfug mit ihren Endgeräten betreiben können. Andererseits sind Netzwerkports und WLAN-Zugänge häufig Dritten (Kunden, Passanten, Lieferanten) oder sogar der Öffentlichkeit zugänglich. Für vertrauenswürdige Zonen gilt deshalb: Nebst einem durchdachten Firewall-Regelset ist auch der Zugriff auf das Netzwerk durch eine «Network Access Control»-Lösung (NAC-Lösung) zu implementieren. Damit sind die Übergänge geschützt. Diese sogenannten Endpoint-Clients sind nochmals durch eine Endpoint Security abgesichert. (Siehe hier), welche die Zweckentfremdung der Endgeräte weitgehend unmöglich macht.

## «DMZ»-Zonen:

Sind Zonen, welche den Austausch mit dem Internet in kontrollierter Art und Weise ermöglichen, um Dienste wie E-Mail, Webzugang, Authentisierung (Federation), etc. bereitzustellen. Jene Zonen exponieren sich im Internet. Dabei sollte darauf geachtet werden, dass die Systeme darin weitest möglich auf Netzwerkebene geschützt sind, sprich, die Systeme stehen hinter einer Perimeter-Firewall (externe Firewall), welche den Zugriff nur auf den nötigsten IPs und Ports erlaubt. Ein häufiges Missverständnis sei noch erwähnt: DMZs erlauben zwar den Zugriff aus dem Internet, jedoch ist zu keiner Zeit ein Zugriff direkt auf dem Medium (Einstecken eines Endgeräts) zu erlauben. Netzwerktechnisch handelt es sich um besonders gekapselte Zonen, in welchen keine Benutzerendgeräte anzutreffen sind. Die im besteht lediglich auf Netzwerkebene und durch eine Firewall.

## «Management»-Zonen:

Sie beinhalten ausschließlich Systeme, welche zur Bereitstellung und Verwaltung der IT-Infrastruktur dienen und werden nur von privilegierten Administratoren genutzt. Die Systeme darin sollten stets als äusserst sensitiv betrachtet werden, da mit ihnen die Steuerung der IT-Infrastruktur möglich ist. Als Grundregel beim Erstellen der Zonenmatrix und beim Implementieren der Firewall-Regeln gilt: Aus Management-Zonen darf in verschiedene Zonen zugegriffen werden (Source), jedoch sind Zugriffe in Management-Zonen (Destination) weitestgehend zu vermeiden. Medienzugriff aus dem Access-Bereich ist strikt untersagt.

**Wichtig ist, dass alle Systeme innerhalb der Zone ähnliche Anforderungen an den Schutzbedarf stellen. Gradmesser und Taktgeber ist jenes System, welches die höchsten Anforderungen stellt.**

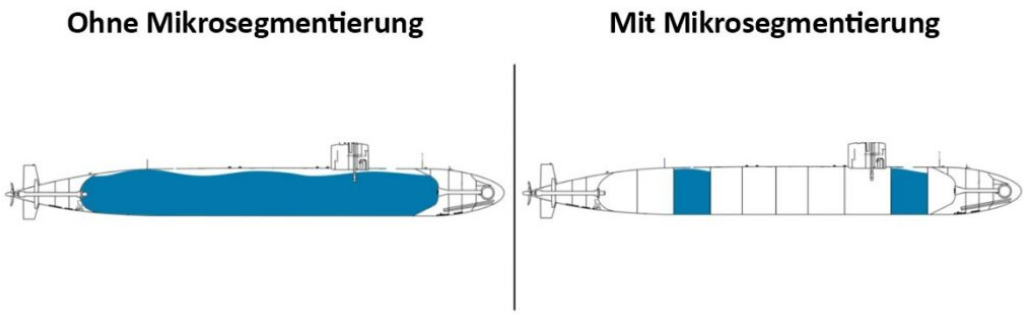
## Was bedeutet Mikrosegmentierung ?

Das leuchtet Paul ein und fragt wie die Kommunikation innerhalb der groben Segmente gesichert wird ?

Aus der Erfahrung heraus wird die Kommunikation auf Ebene des Netzes oft nicht weiter eingeschränkt und genau hier liegt ein interessantes Problem.

Nehmen wir das oben skizzierte Beispiel einer strikten Client- und Serversegmentierung. Die Server sind so vor unberechtigten Zugriffen von Clients in einem gewissen Rahmen geschützt. Nehmen wir außerdem an, dass die Server, die besonders kritische Daten verarbeiten, in einem zusätzlichen eigenen Sicherheitssegment für den hohen Schutzbedarf abgetrennt werden. Auf den ersten Blick scheint dies eine passable Lösung zu

sein, die einmal aufgebaut wird und dann ein solides Sicherheitsniveau liefern kann.




Vorteile der Mikrosegmentierung in der IT-Sicherheit

Leider gibt es da noch die ausgesprochen dynamische Welt der Schwachstellen. Es kann nämlich durchaus sein, dass (vielleicht sogar von den Servern mit hohem Schutzbedarf) gewisse Server als unsicher zu werten sind, da z.B. die Betriebssysteme auf Grund der laufenden Anwendungen nicht geregelt (oder gar nicht) gepatcht werden dürfen oder die Anwendungen selbst Schwachstellen aufweisen, die auf absehbare Zeit nicht beseitigt werden können. Diese Server stellen dann natürlich grundsätzlich eine Bedrohung dar.

Schwachstellen könnten von einem Angreifer ausgenutzt werden, um die betroffenen Systeme zu kompromittieren und Daten zu entwenden bzw. zu manipulieren oder von dieser Angriffsbasis aus die anderen Server unter Beschuss zu nehmen.

## Endgeräte-Segmentierung im internen Netz

Das BSI IT-Grundschutz-Kompendium sagt dann auch folgerichtig in Anforderung NET.1.1.A6 Endgeräte-Segmentierung im internen Netz: „Es dürfen nur Endgeräte in einem Sicherheitssegment positioniert werden, die einem ähnlichen Sicherheitsniveau

entsprechen.“
Die Antwort darauf ist klar: Mit den Mitteln der Netzsegmentierung wird weiteres Sicherheitssegment als Käfig aufgebaut, in dem unsichere Systeme (in unserem Beispiel sind es IOT Geräte) gelagert werden. Hier werden beispielsweise alle Sprachassistenten, Live-Kameras, … in separate Netze gepackt. Der Verkehr von und zu dem Käfig kann dann z.B. durch ein besonders strenges Regelwerk und durch Intrusion-Prevention-Techniken genauestens kontrolliert werden.

Mit den Mitteln einer Mikrosegmentierung könnte beispielsweise durch den Einsatz der Distributed Firewall ein solcher zielgerichteter Schutz von VMs bedarfsweise geschaffen werden. Diese Lösung ist hier auch deshalb interessant, weil die Distributed Firewall für das Netz transparent ist und das System netztechnisch nicht in ein anderes Sicherheitssegment umgezogen werden müsste.

## Netzwerksegmentierung aus Sicht der IT-Sicherheit ist ein dynamischer Prozess

In der Praxis zeigt sich immer wieder, dass Netzsegmentierungen auch stets den Umgang mit unsicheren Systemen berücksichtigen müssen und damit nie statischer Natur sind. Ohne ein Konzept für den Aufbau von Giftschränken und den Umgang mit ihnen ist eine Netzsegmentierung nicht besonders sinnvoll. Eine Netzsegmentierung muss also dynamisch und schnell genug auf neue Schwachstellen in den Systemen reagieren und flexibel einen zusätzlichen Schutz für betroffene Systeme schaffen können. Wenn dieser Schutz nicht mehr benötigt wird (weil vielleicht ein Patch die

Schwachstellen beseitigt hat) muss er außerdem auch genauso flexibel wieder entfernt werden können. Der Schutz muss also hier möglichst nah an den betroffenen Endgeräten liegen und für Layer 3 transparent sein. Eine traditionelle Netzsegmentierung auf Basis von VLANs kann dies nicht leisten und SDN-basierte Lösungen werden vermehrt diese Lücke schließen.

# Weiterführende Links

BSI Grundschutz NET 1.1 – Hier klicken

Peter, IT-Leiter, und die Netzwerksegmentierung – Teil 1 – Hier klicken

## Neueste Beiträge

Was bringt ein SOC (Security Operation Center)

Trends IT Sicherheit im Jahr 2022

Hacking als Geschäftsmodell – Erfolg von Ransomware as a Service steigt

5 Gründe warum Pentests in jedes Sicherheitskonzept gehören

Wie Unternehmen sich vor Ransomware-Forderungen schützen können

.

Deutsch