controlware

Controlware
Security Day
22. - 23. September 2022
Congress Park Hanau

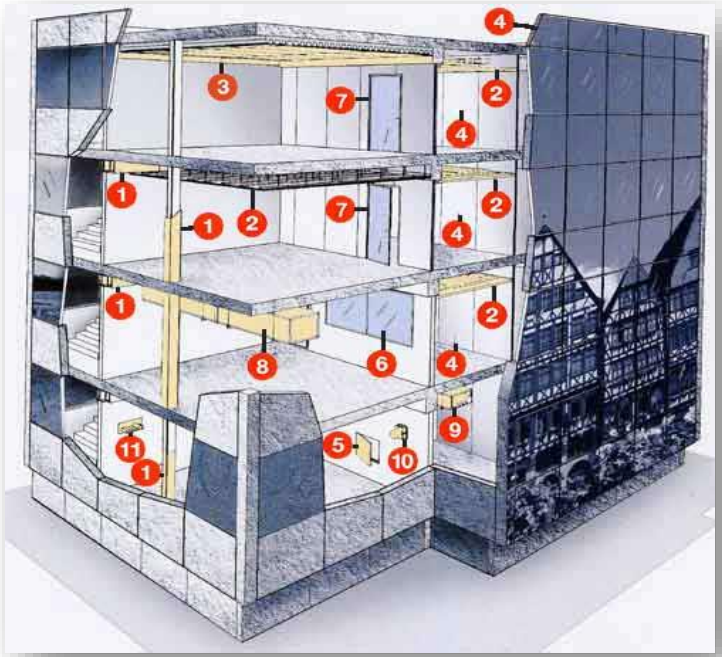
„Kompass-Security“ im modernen Data Center

Workloads mit aktuellen Technologien in die Zero Trust-Ära überführen

Jens Katzwinkel, Controlware GmbH, Senior Consultant Data Center Infrastruktur
Christoph Schmidt, Controlware GmbH, Lead Consultant Information Security

Entwicklung einer Sicherheitsarchitektur

Segmentierung – Begriffe



Quelle: Feuerschutz MOHR

Meta Group White Paper – Securing Internal Networks

„Die zunehmende Anzahl alternativer Kommunikationspfade in eine Unternehmensinfrastruktur, Angriffe auf der Applikationsebene und die immer vernichtendere Wirkung von Würmern lassen nur eine Schlussfolgerung zu: Die klassische Perimeterabsicherung muss um eine umfassende Reihe interner Sicherheitsmechanismen ergänzt werden.“

Entwicklung einer Sicherheitsarchitektur

Segmentierung – Begriffe

Network **Compartmentalization**

- Aufteilen des Netzwerks in Abteilungen oder Zonen (Bsp. Buchhaltung, Personal, F & E, Produktion,…)
- Schutzklassen / Schutzzonen

Network **Segmentation**

- Trennung des Netzwerktraffics in einzelne Bereiche
- Hintergrund: „Collision Domains“

Network **Virtualization**

- Logische Trennung von Netzwerken auf einer physikalischen Infrastruktur
- VLANs
- virtuelle Netzwerkkomponenten
- virtuelle Systeme (Hosts, Server, Desktops, usw.)

Micro Segmentation

- Trennung auf Funktionsebene
- Im DC: Zugriffe auf Services bzw. Zugriffe von Services untereinander

Segmentierung – „Mythos“

Microsegmentierung
=
Zero Trust

Entwicklung einer Sicherheitsarchitektur

Segmentierung – „Don‘t boil the Ocean“

How Network Segmentation Projects Fail

Separate Zoning Design From Implementation. Build your zoning strategy separate from the specific implementation constraints of the environment. Design first, pick the tool second. Don’t let the tool drive the design. Picking the tool first, then creating the design is the canary in the coal mine of a doomed-to-fail network segmentation project.

Gartner

Aufbau von internen Sicherheitszonen / Segmentierung

Typische Anforderungen

- **Schutz kritischer Daten vor unberechtigten Zugriffen**
  - Vertraulichkeit
  - Verfügbarkeit
  - Integrität
- **Trennung von schutzbedürftigen IT-Systemen und ganzen Netzbereichen**
  - Data Center (Mikrosegmentierung) → Kann per Definition auch im z.B. OT Bereich sein
  - Campus
- **Sichere IT-Administration (Managementnetz)**

Aufbau von internen Sicherheitszonen / Segmentierung

Kleiner Exkurs

Aufbau von internen Sicherheitszonen / Segmentierung

Beispiel: BSI Zonenkonzept

Das Netz ist in separate Bereiche zu untergliedern, welche jeweils durch ein eigenes Sicherheitsgateway oder einen Paketfilter abgesichert werden.

NET.1.1.A4 Netztrennung in Sicherheitszonen (B)

Das Gesamtnetz muss mindestens in folgende drei Sicherheitszonen **physisch** separiert sein: internes Netz, demilitarisierte Zone (DMZ) und Außenanbindungen (inklusive Internetanbindung sowie Anbindung an andere nicht vertrauenswürdige Netze).

NET.1.1.A5 Client-Server-Segmentierung

Clients und Server müssen in unterschiedlichen Sicherheitssegmenten (getrennt durch einen zustandsbehafteten Paketfilter (Firewall)) platziert werden.

NET.1.1.A19 Separierung der Infrastrukturdienste

Server, die grundlegende Dienste für die IT-Infrastruktur bereitstellen, sollten in einem dedizierten Sicherheitssegment positioniert und die Kommunikation durch einen zustandsbehafteten Paketfilter (Firewall) kontrolliert werden.

Das Zonenkonzept unterscheidet in der Folge verschiedene Sicherheitszonen mit unterschiedlichen Sicherheitseigenschaften.

Sicherheitszonen unterscheiden sich u. a. durch:

- den Eigentümer der Prozesse und Daten,
- die Klassifizierung und den Schutzbedarf der zu verarbeitenden Informationsobjekte,
- die Benutzergruppen und Komponenten, die auf diese Informationsobjekte zugreifen dürfen,
- die Bedrohungen und die umgesetzten Sicherheitsmaßnahmen.

Alle eingesetzten IT-Systeme sind genau einer Zone des Zonenkonzeptes zuzuordnen.

Es gilt das Prinzip des Verbots zonenübergreifender Zugriffe.

Ziel: Wird ein IT-System kompromittiert, dann können lediglich die IT-Systeme aus der selben Zone angegriffen werden.

Test- und Entwicklungsumgebungen sind hinreichend von Produktivumgebungen abzuschotten.

Aufbau von internen Sicherheitszonen / Segmentierung

Entscheidungskriterien zur Einsortierung (Container/Zone/Gerätegruppe)

- Zuordnung zu erbrachten/genutzten Diensten
- Art, Umfang und Richtung der benötigten Kommunikation (Bsp. Backup)
- Technische Eigenschaften und Beschränkungen
- organisatorische Zugehörigkeit
- Schutzbedarf

Aufbau von internen Sicherheitszonen / Segmentierung

Schutzbedarf

Bestimmung des „Risikos“:

Bsp: Personal

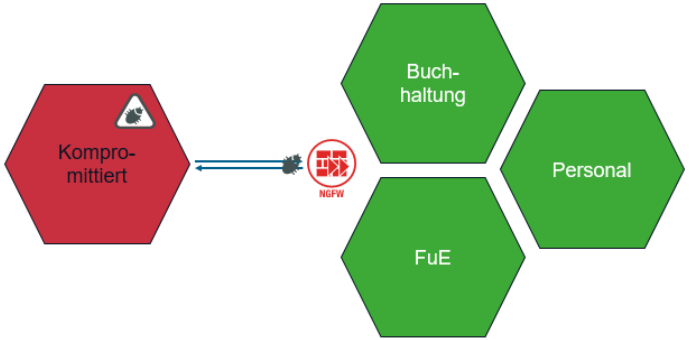
- Schutz **für** Personal (Vertraulichkeit & Zugriffe)
- Schutz **vor** Personal (Exponiertheit (Ransomware))

Weitere Beispiele: Lab, Produktion

Aufbau von internen Sicherheitszonen / Segmentierung

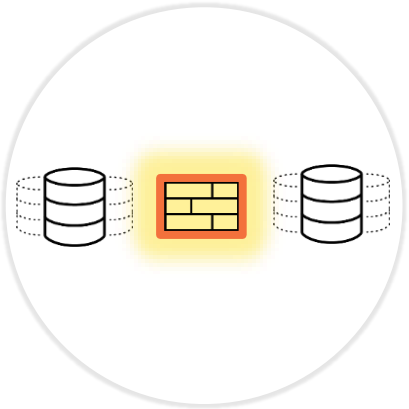
Aufbau von internen Sicherheitszonen / Segmentierung

- **Trennung von Systemen mit spezifischen Sicherheitsanforderungen**
- **Isolation von Systemen mit hohem Schutzbedarf**
  - Filter am Übergang in eine Ebene
  - Keine direkten IP-Zugriffe aus nicht oder eingeschränkt vertrauenswürdigen Bereichen
- **Bedarfsorientierte netztechnische Trennung in mehrere Zonen**

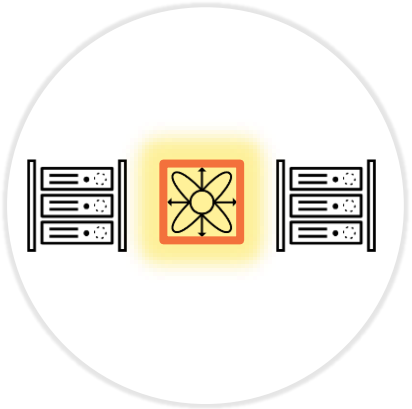


Aufbau von internen Sicherheitszonen / Segmentierung

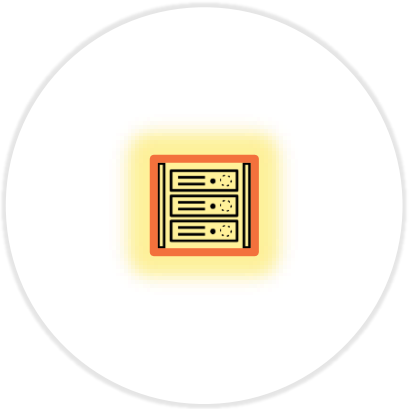
Verwirrung – Begriffe & Definitionen



North-South (Perimeter)
DC Edge firewalls
User to DC, Inter DC
VRF, VLAN, IP Subnet



East-West (Fabric)
Course level (Network)
Network Overlay (EPG, Macro-segment, VXLAN)

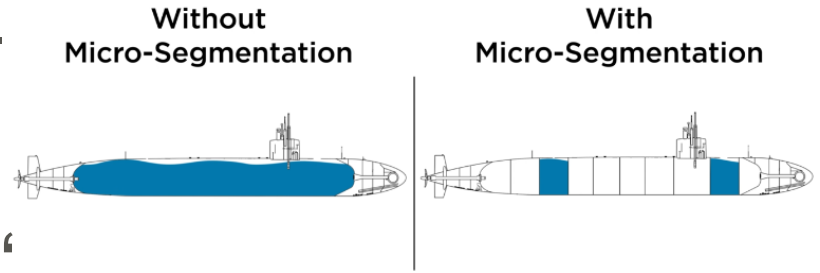


East-West (Host)
Granular (Workload)
Port groups, Hypervisor
Micro-segment

Microsegmentierung – Zusammenfassung

Was ist das und warum brauche ich das?

- Reduktion der Angriffs-fläche
- Verhindert „Ausbrüche“
- Erfüllt regulatorische Compliance Anforderungen
- Ist Basis für eine Zero Trust Strategie ☺



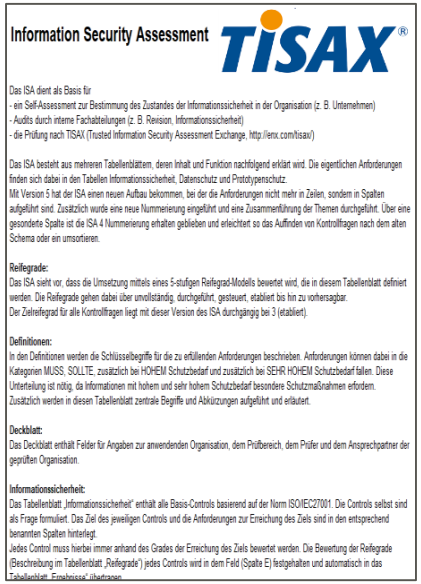
Aufbau von internen Sicherheitszonen / Segmentierung

Anforderungen aus Normen und Standards (beispielhaft)


INTERNATIONAL STANDARD

ISO/IEC 27001

Information technology — Security techniques — Information security management systems — Requirements


Information Security Assessment TISAX®

Das ISA dient als Basis für
- ein Self-Assessment zur Bestimmung des Zustandes der Informationssicherheit in der Organisation (z. B. Unternehmen)
- Audits durch interne Fachabteilungen (z. B. Revision, Informationssicherheit)
- die Prüfung nach TISAX (Trusted Information Security Assessment Exchange, http://enx.com/tisax/)

Das ISA besteht aus mehreren Tabellenblättern, deren Inhalt und Funktion nachfolgend erklärt wird. Die eigentlichen Anforderungen finden sich dabei in den Tabellen Informationssicherheit, Datenschutz und Prototypenschutz.
Mit Version 5 hat der ISA einen neuen Aufbau bekommen, bei der die Anforderungen nicht mehr in Zeilen, sondern in Spalten aufgeführt sind. Zusätzlich wurde eine neue Nummerierung eingeführt und eine Zusammenführung der Themen durchgeführt. Über eine gesonderte Spalte ist die ISA 4 Nummerierung erhalten geblieben und erleichtert so das Auffinden von Kontrollfragen nach dem alten Schema oder ein umsortieren.

Reifegrade:
Das ISA sieht vor, dass die Umsetzung mittels eines 5-stufigen Reifegrad-Modells bewertet wird, die in diesem Tabellenblatt definiert werden. Die Reifegrade gehen dabei über unvollständig, durchgeführt, gesteuert, etabliert bis hin zu vorhersagbar.
Der Zielreifegrad für alle Kontrollfragen liegt mit dieser Version des ISA durchgängig bei 3 (etabliert).

Definitionen:
In den Definitionen werden die Schlüsselbegriffe für die zu erfüllenden Anforderungen beschrieben. Anforderungen können dabei in die Kategorien MUSS, SOLLTE, zusätzlich bei HOHEM Schutzbedarf und zusätzlich bei SEHR HOHEM Schutzbedarf fallen. Diese Unterteilung ist nötig, da Informationen mit hohem und sehr hohem Schutzbedarf besondere Schutzmaßnahmen erfordern.
Zusätzlich werden in diesen Tabellenblatt zentrale Begriffe und Abkürzungen aufgeführt und erläutert.

Deckblatt:
Das Deckblatt enthält Felder für Angaben zur anwendenden Organisation, dem Prüfbereich, dem Prüfer und dem Ansprechpartner der geprüften Organisation.

Informationssicherheit:
Das Tabellenblatt „Informationssicherheit" enthält alle Basis-Controls basierend auf der Norm ISO/IEC27001. Die Controls selbst sind als Frage formuliert. Das Ziel des jeweiligen Controls und die Anforderungen zur Erreichung des Ziels sind in den entsprechend benannten Spalten hinterlegt.
Jedes Control muss hierbei immer anhand des Grades der Erreichung des Ziels bewertet werden. Die Bewertung der Reifegrade (Beschreibung im Tabellenblatt „Reifegrade") jedes Controls wird in dem Feld (Spalte E) festgehalten und automatisch in das Tabellenblatt „Ergebnisse" übertragen.

Aufbau von internen Sicherheitszonen / Segmentierung

Unterschiedliche Ansätze für die Mikrosegmentierung

Network/Firewall-based

Hypervisor-based

Host-based

Cloud (CWPP)

Cisco ACI

Extreme networks

vmware NSX

Microsoft Hyper-V

Guardicore

Cisco Secure

illumio

Prisma™ Cloud

McAfee

Security am Übergang

Check Point Software Technologies

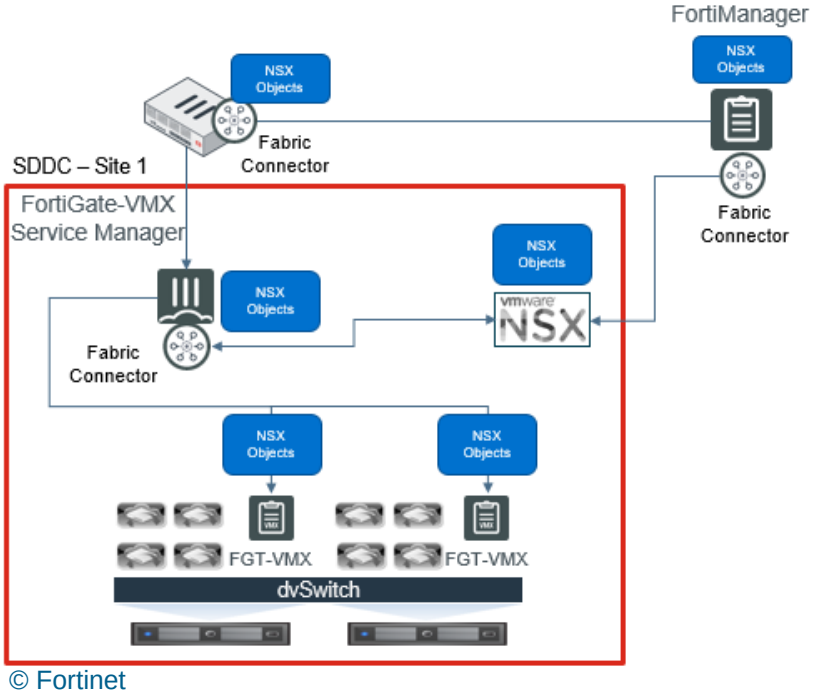
Fortinet

paloalto Networks

Aufbau von internen Sicherheitszonen / Segmentierung

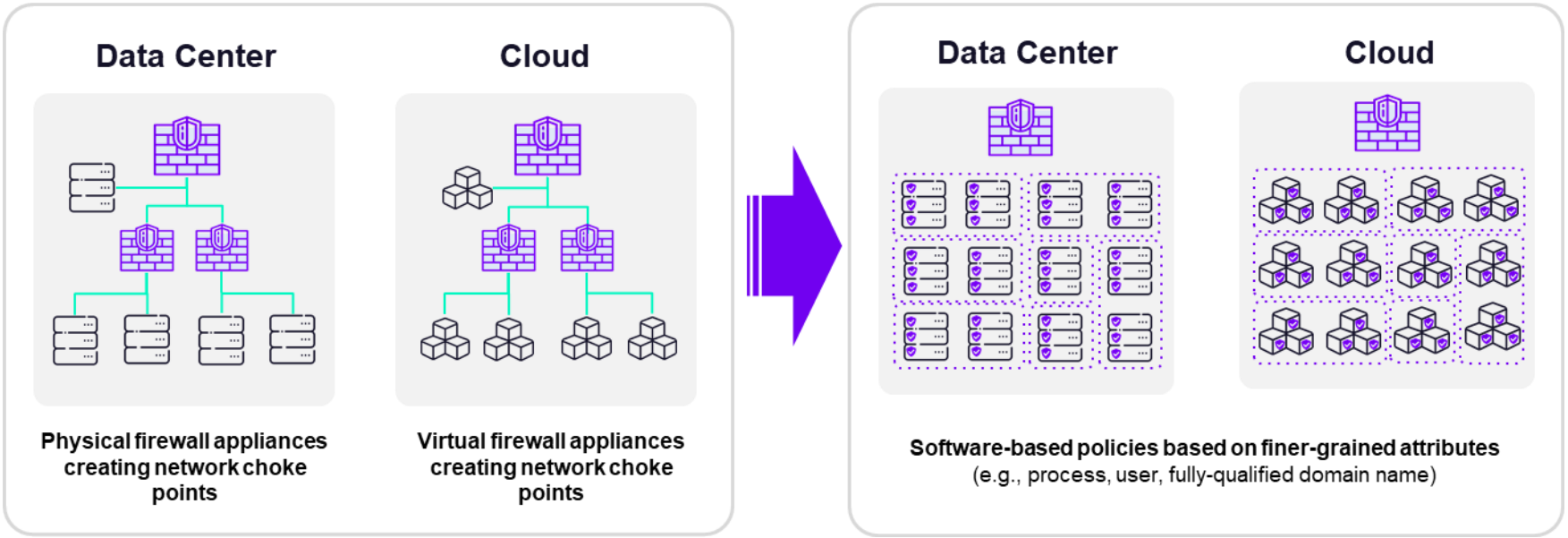
Virtuelle Firewall Appliances zur Mikrosegmentierung

- Virtuelle VM-attached FW
- Vmware NSX Service Insertion
- Integration vCenter und NSX Manager mit Firewall-Management (z.B. Fortinet, Check Point, Palo Alto)
  - IDS/IPS
  - App Control
  - Identity Awareness
  - …



Aufbau von internen Sicherheitszonen / Segmentierung

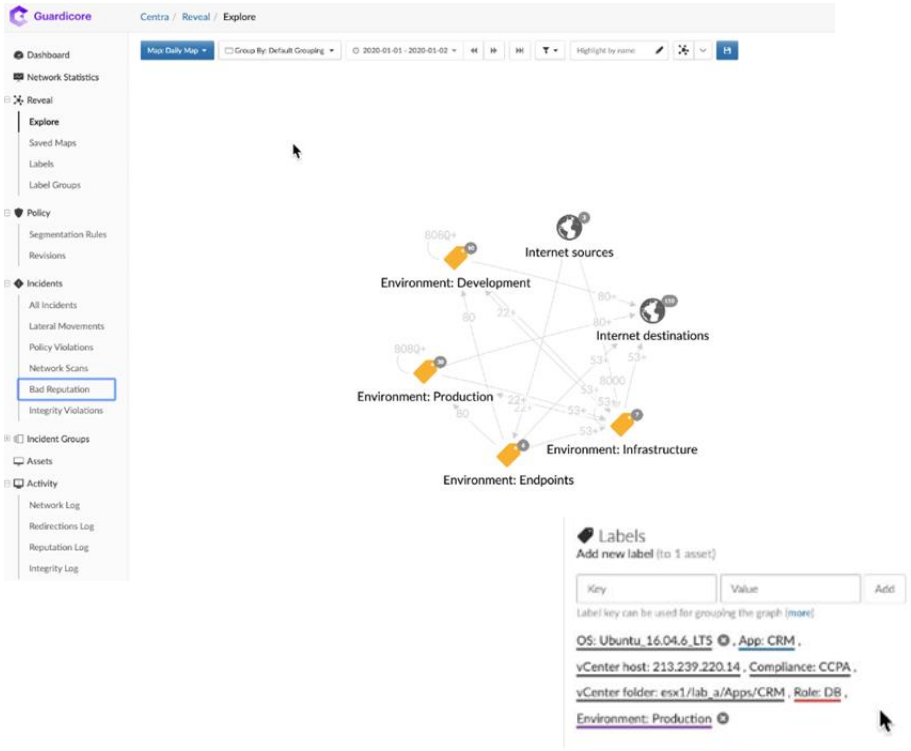
Hostbasierte Mikrosegmentierung



Aufbau von internen Sicherheitszonen / Segmentierung

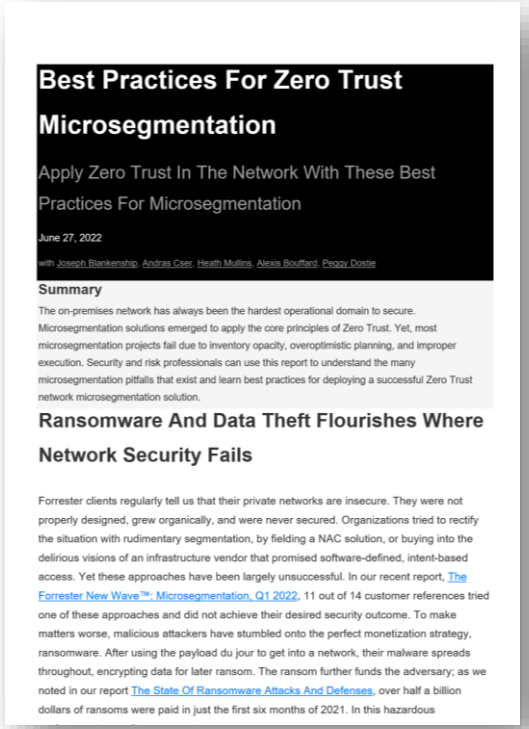
Hostbasierte Mikrosegmentierung

- **Environment Segmentation**
  - Entwicklung
  - Test
  - Produktion
- **Application Segmentation**
  - „Ring-Fencing“ – kritische Applikationen abkapseln
- **Tier Segmentation**
  - Webserver
  - Applikation-Server
  - Datenbank
- **Label bzw. Tags statt IP-Adressen**



Microsegmentierung

Vorgehen und Next Steps?



Best Practices For Zero Trust Microsegmentation

Apply Zero Trust In The Network With These Best Practices For Microsegmentation

June 27, 2022

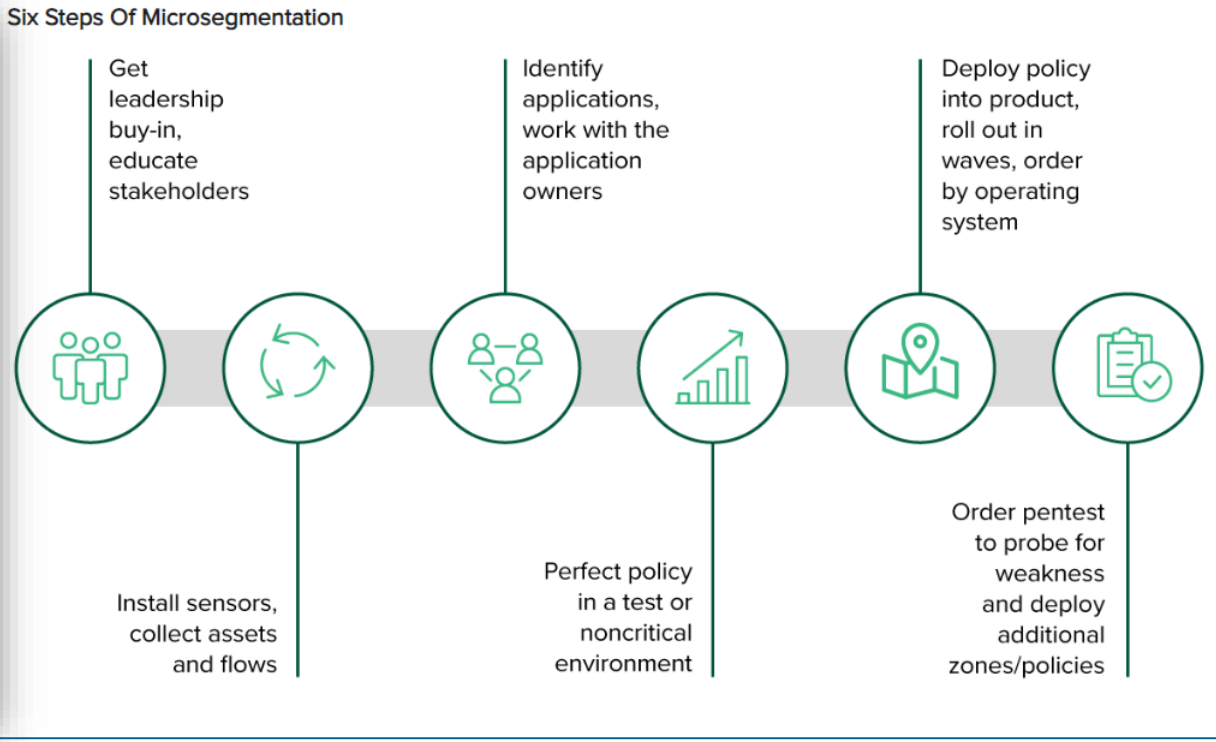
with Joseph Blankenship, Andras Cser, Heath Mullins, Alexis Bouffard, Peggy Dostie

Summary

The on-premises network has always been the hardest operational domain to secure. Microsegmentation solutions emerged to apply the core principles of Zero Trust. Yet, most microsegmentation projects fail due to inventory opacity, overoptimistic planning, and improper execution. Security and risk professionals can use this report to understand the many microsegmentation pitfalls that exist and learn best practices for deploying a successful Zero Trust network microsegmentation solution.

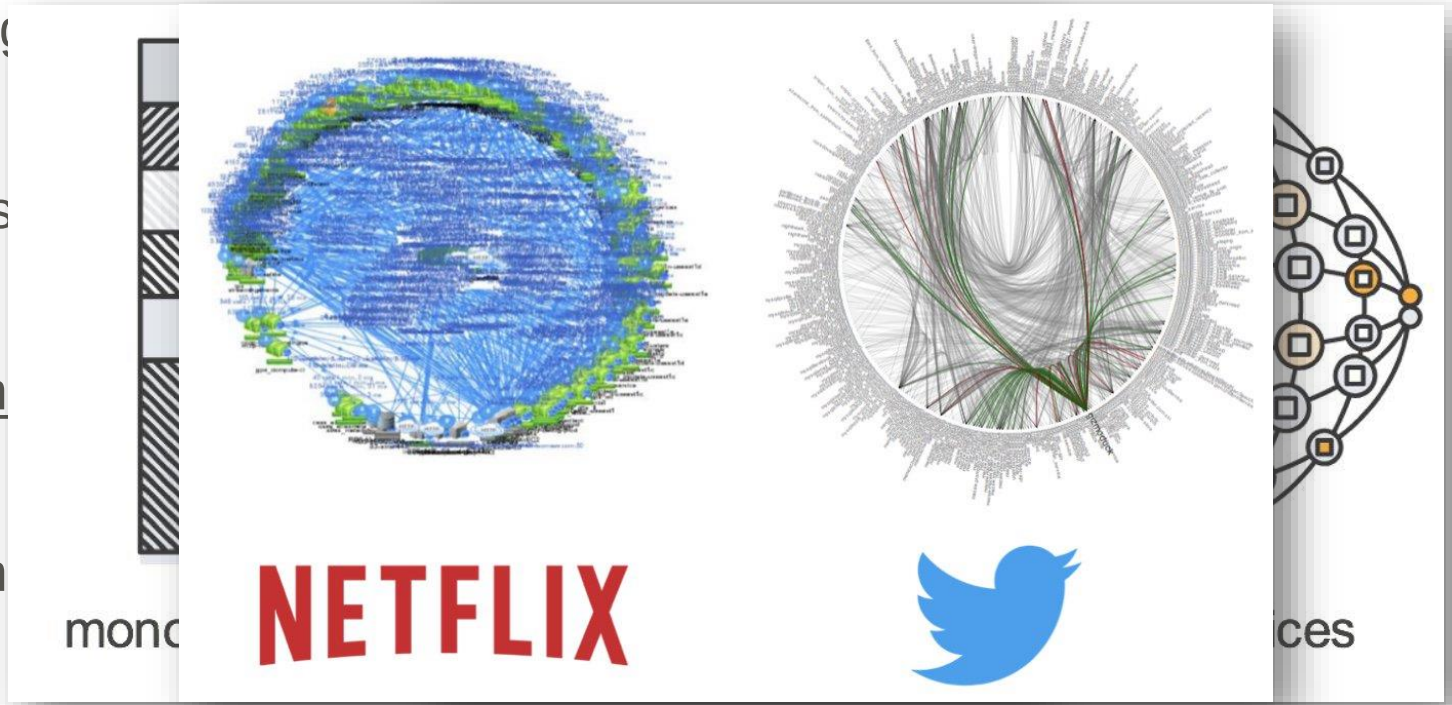
Ransomware And Data Theft Flourishes Where Network Security Fails

Forrester clients regularly tell us that their private networks are insecure. They were not properly designed, grew organically, and were never secured. Organizations tried to rectify the situation with rudimentary segmentation, by fielding a NAC solution, or buying into the delirious visions of an infrastructure vendor that promised software-defined, intent-based access. Yet these approaches have been largely unsuccessful. In our recent report, The Forrester New Wave™: Microsegmentation, Q1 2022, 11 out of 14 customer references tried one of these approaches and did not achieve their desired security outcome. To make matters worse, malicious attackers have stumbled onto the perfect monetization strategy, ransomware. After using the payload du jour to get into a network, their malware spreads throughout, encrypting data for later ransom. The ransom further funds the adversary; as we noted in our report The State Of Ransomware Attacks And Defenses, over half a billion dollars of ransoms were paid in just the first six months of 2021. In this hazardous



Visibilität

Kommunikation innnerhalb



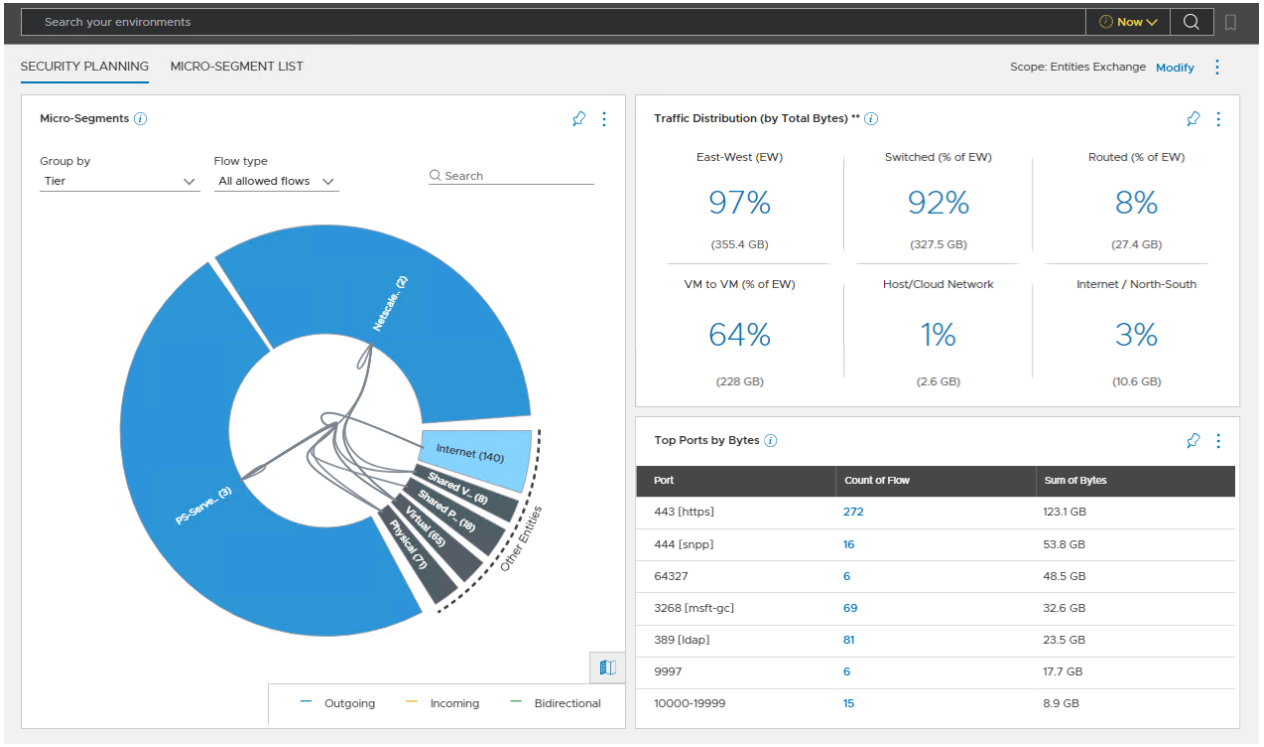
Microsegmentierung – Zusammenfassung

Vorgehen und Next Steps?

1. Identifizierung der „Kronjuwelen“
2. Visibilisierung der Verkehrsflüsse
3. Erarbeiten einer Policy (Template)
4. Test der Policy (Learning Mode)
5. Umsetzung der Microsegmentierung

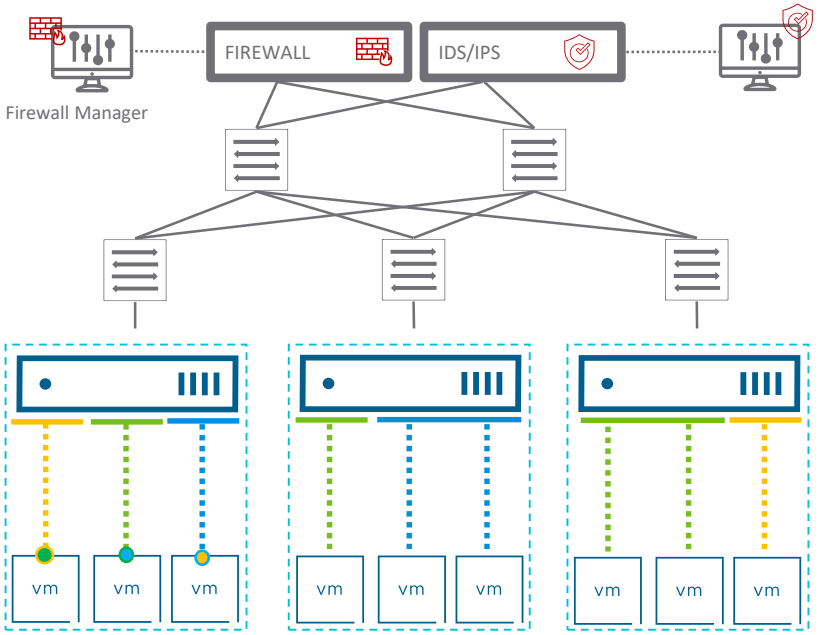
Systeme/Kommunikation

Was geht ab?



Visibilität

Hairpinning



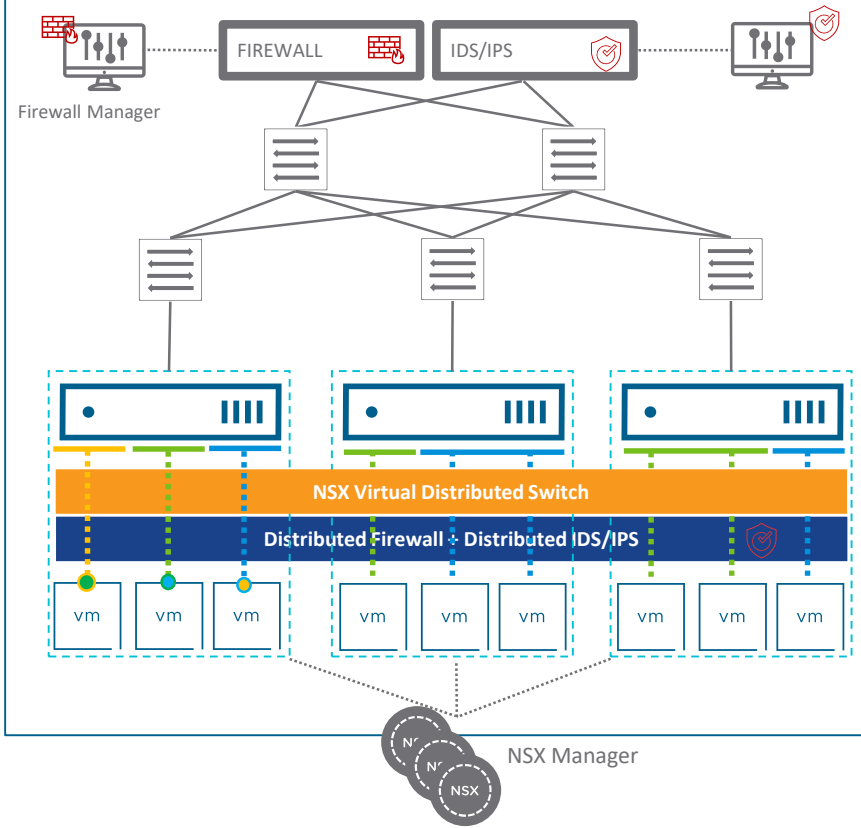
Performance

Skalierung

Management

Systeme/Kommunikation

Use Case – DC „interne“ Kommunikation

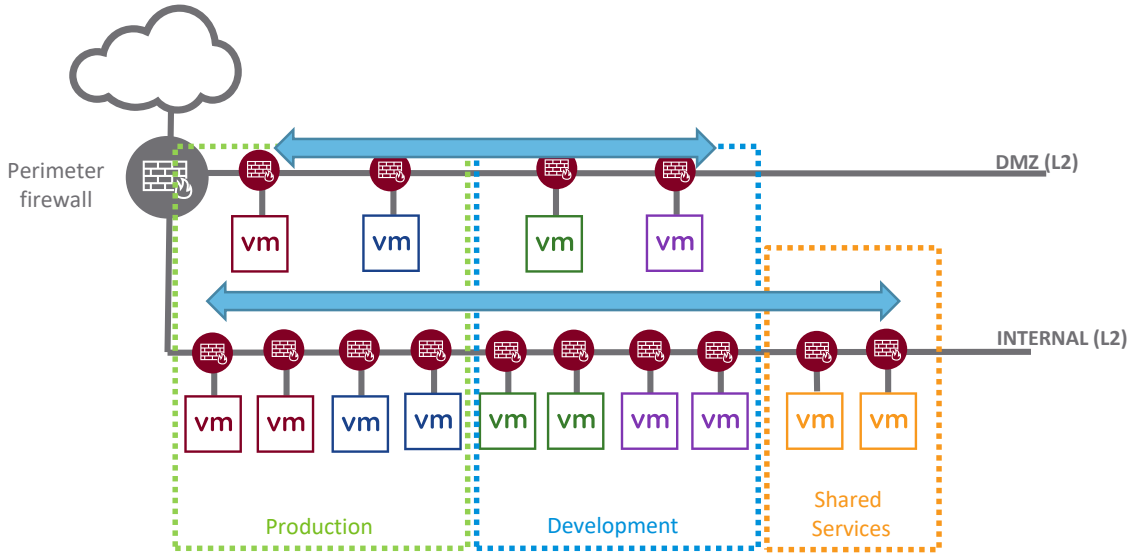


Performance

Skalierung

Management

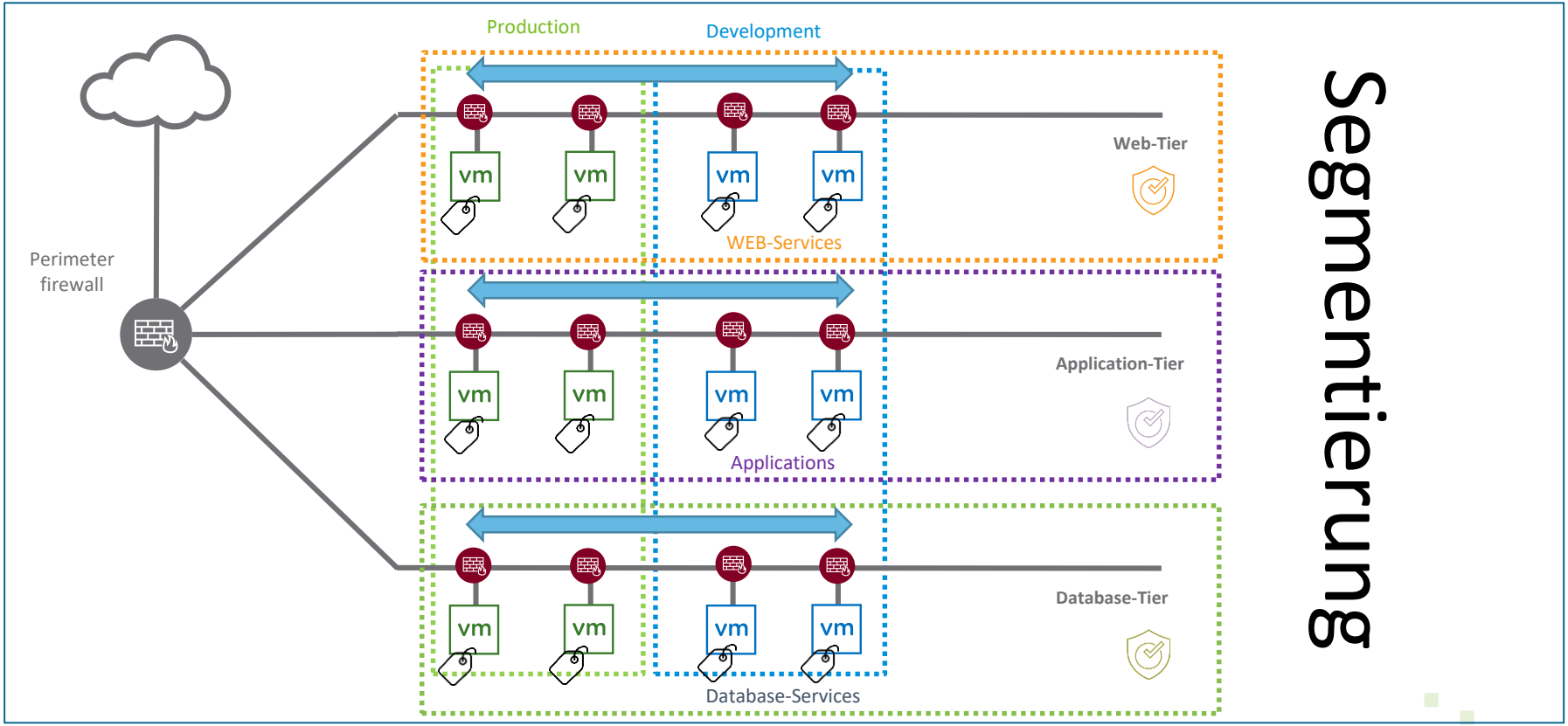
Use Case – Lateral Movement



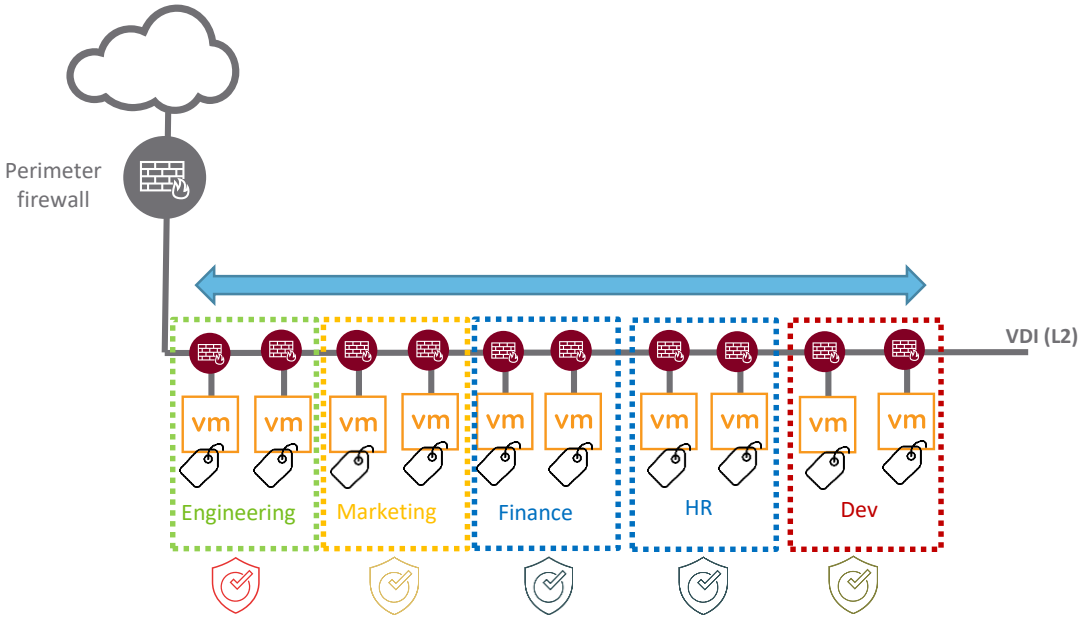
East-West
Lateral movement

Systeme/Kommunikation

Use Case – Zonenübergreifende Architektur



Use Case – „Clients“ im DC



Tags

Policies

Zusammenfassung

Microsegmentierung

Anforderung teilweise mandatory

Schut me

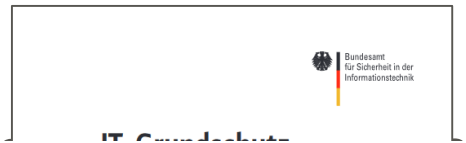
Da nts

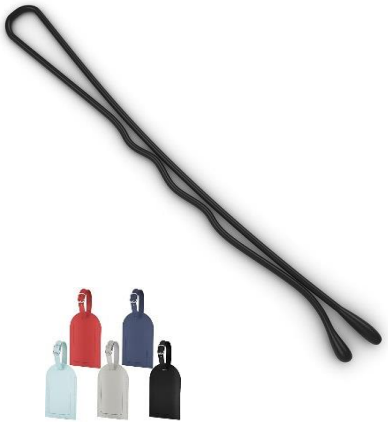
Pc

Vc en

Sich :en

Berei gie






Strategische Segmentierung – Mehr Sicherheit für Ihre Infrastruktur
Angepasste Konzepte sind gefragt
Vor allem an Standorten international tätiger Unternehmen nimmt der Erfüllungsgrad bei der Umsetzung von Sicherheits-
die Absicherung der Produktionsanlagen unter Umständen direkt an die Maschinen herangeführt werden muss.
controlware
Workshop
Und weiter?

Vielen Dank für Ihre Aufmerksamkeit!
Thank you very much for your attention!