TELEKOM SECURITY

Effiziente Sicherheit

mit softwaredefinierter Mikrosegmentierung

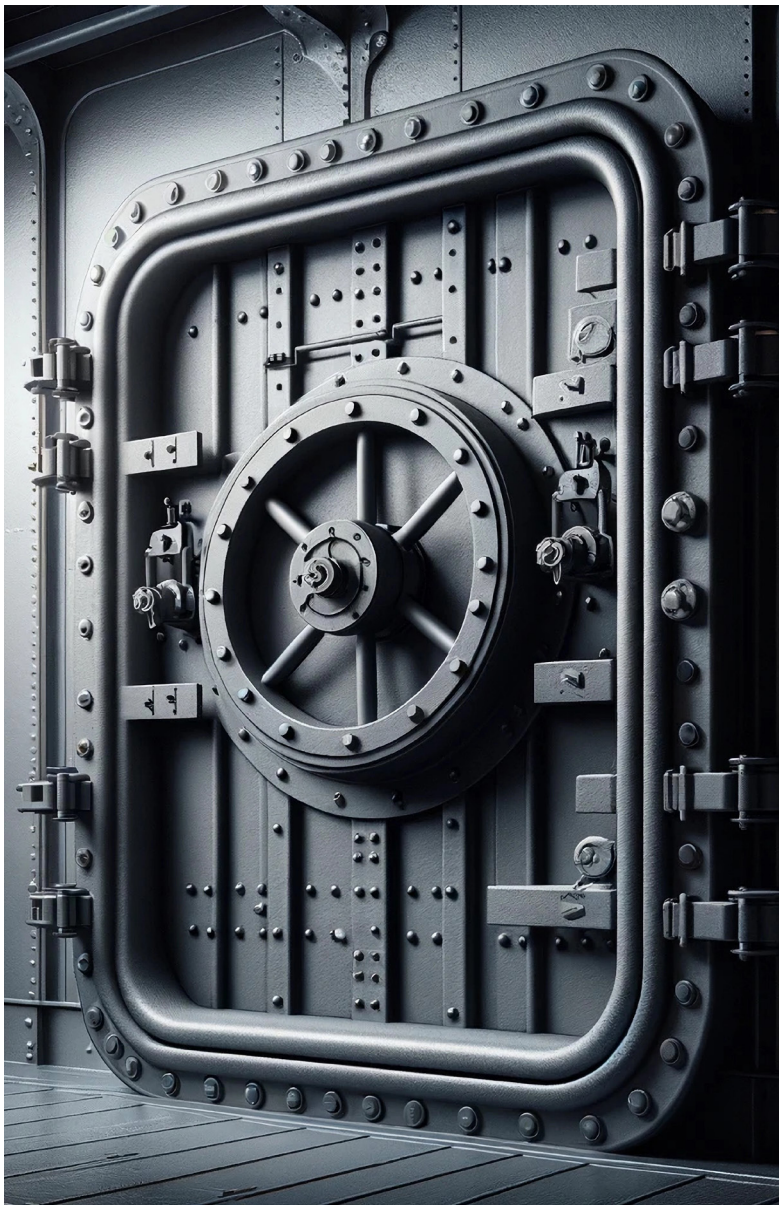
Connecting your world.

WILLKOMMEN IM ZEITALTER DER EINDÄMMUNG

Was passiert, wenn ein Angreifer erfolgreich in Ihr System eingedrungen ist? In den meisten Fällen passiert erst einmal gar nichts – denn Sie merken nicht, dass Sie infiltriert wurden. Laut einer im Dezember 2024 veröffentlichten Studie benötigten Unternehmen im Jahr 2024 durchschnittlich 258 Tage, um ein Datenleck zu identifizieren und einzudämmen[1]. In der Zwischenzeit haben die Angreifenden also jede Menge Zeit – und die nutzen sie, um sich in Ihrem System auszubreiten.

258 Tage

dauert es im Schnitt bis zur Identifizierung und Behebung eines Datenschutzverstoßes.



Softwaredefinierte Mikrosegmentierung (SDS) ist daher das Gebot der Stunde. Denn sie sorgt dafür, die Ausbreitungsmöglichkeiten von Viren und Schadsoftware im Angriffsfall so gering wie möglich zu halten. Damit bietet sie im Gegensatz zu anderen Schutzmaßnahmen vor allem auch die Möglichkeit, sich gegen unbekannte Gefahren zu wappnen.

Schotten dicht!

Das Prinzip der Segmentierung ist einfach – wir kennen es aus dem Schiffbau. Damit ein Schiff bei einem Leck nicht sinkt, wird der Rumpf durch Schotten in viele kleine wasserdichte Kammern unterteilt. Im Ernstfall dringt das Wasser daher nur in eines der Segmente ein und das Schiff bleibt schwimmfähig. Aber, und das lernen wir von der Titanic: Wichtig ist, dass die Schotten in allen Decks vorhanden sind. Anzahl, Kleinteiligkeit und Stärke der Schotten sowie ihre Verteilung über das ganze Schiff ergeben zusammen den Schutz vorm Untergang.

Auch in der IT-Sicherheit ist dieses Prinzip nicht vollkommen neu. Allerdings ist die klassische Netzwerksegmentierung den heutigen Architekturen, die eine Mischung aus historisch gewachsenen Umgebungen und modernen Cloud-Plattformen darstellen, nicht mehr gewachsen. Um trotz Plattformbrüchen eine durchgängige Sicherheit zu gewährleisten, ist eine neue Form der Segmentierung erforderlich.

In diesem Whitepaper werden traditionelle und neue Formen der Segmentierung mit ihren Vor- und Nachteilen vorgestellt. Dabei behandeln wir insbesondere auch die vielen ökonomischen Vorteile der SDS. Darüber hinaus wird auf die Rolle der softwaredefinierten Mikrosegmentierung im Kontext von rechtlichen Anforderungen und Zero Trust eingegangen. Anhand von Anwendungsbeispielen wird schließlich der Einsatz der SDS in der Praxis veranschaulicht.

[1] Statista 2024

WARUM NETZWERKSEGMENTIERUNG NICHT REICHT

Eine seit langem bekannte und häufig in klassischen Rechenzentrumsumgebungen eingesetzte Lösung ist die Segmentierung auf Netzwerkebene, auch als Makrosegmentierung bezeichnet. Darunter versteht man den Ansatz, die externen Zugänge eines Netzwerks durch Perimeter-Firewalls abzusichern und das interne Netzwerk in verschiedene (virtuelle) LAN-Segmente aufzuteilen, denen ein oder mehrere IP-Segmente zugewiesen werden. Der ein- und ausgehende Netzwerkverkehr zu und von diesen Segmenten wird so reguliert, dass die einzelnen Segmente gegeneinander abgeschirmt sind.

Schwächen und Risiken der Makrosegmentierung:

Zu große Segmente
Datenverkehr wird ausschließlich dann kontrolliert, wenn er eine Segmentsgrenze überschreitet, alle Ressourcen innerhalb eines Segmentes können vollkommen ungehindert miteinander kommunizieren. Der Einsatz moderner Firewalls kann dieses Phänomen nicht verhindern, weil innerhalb eines (V)LANs kein Routing stattfindet und somit die Firewalls nicht als Gateway verwendet werden können. Eine Verkleinerung der (V)LANs ist aus technischen Gründen nur sehr begrenzt möglich, wodurch große Bereiche entstehen, deren Kommunikation nicht kontrolliert werden kann.

Abbildung von Richtlinien nicht geregelt
Im Rahmen eines Segmentierungsprojektes müssen die bestehenden Kommunikationsbeziehungen im gesamten Netzwerk aufgenommen und mit eventuellen Anforderungen, die sich aus regulatorischen oder unternehmensinternen Richtlinien ergeben, abgeglichen werden. Dieser Prozess ist allein aufgrund der hohen Anzahl von Verbindungen in einem Unternehmensnetzwerk sehr aufwändig und zeitintensiv.

Aufwendige und fehleranfällige Implementierung
Nach erfolgreicher Konzepterstellung folgt die Implementierung. Dieser Schritt ist aufwendig zu planen, da viele Abteilungen involviert werden müssen und erfordert umfangreiches Knowhow. In der Regel müssen die IP-Adressen der Serversysteme im Rahmen des Umzugs in die neuen Segmenten geändert werden. Das bedeutet wiederum Anpassungen in den Applikationen, die zu weiteren Fehlerquellen führen können. Schatten-IT wird bei diesen Prozessen zudem oft nicht berücksichtigt, was weitere Probleme nach sich zieht.

Komplexe Rollback-Szenarien
Im Fehlerfall sind die Rollback-Szenarien höchst komplex, da Netzwerkkonfigurationen und alle sich daraus ergebenden Abhängigkeiten rückgängig gemacht werden müssen. Dies erfordert Zeit, die oft zu einem Produktionsausfall mit entsprechenden finanziellen Folgen und möglichen Reputationsverlusten für das Unternehmen führt.

Fazit: Hoher Aufwand, mittleres Schutzniveau
Der klassische Ansatz der Netzwerksegmentierung ist sehr aufwendig und risikobehaftet. Im Ergebnis wird durch Makrosegmentierung ein mittleres Schutzniveau erreicht, da es große Bereiche gibt, in denen Ressourcen weiterhin ungehindert miteinander kommunizieren können. Insbesondere in einer modernen Umgebung, die aus mehreren Plattformen besteht, z. B. aus klassischen Hardware-Servern im Rechenzentrum, virtualisierten Serverumgebungen, Anteilen in der Public Cloud sowie modernen Applikationen auf Basis von Containerumgebungen, ist dieser Ansatz nicht durchgängig umsetzbar und führt zu teilweise schwer erkennbaren Durchlässigkeiten. Aufgrund dieser Einschränkungen ist diese Methodik als Basis für eine Zero-Trust-Implementierung gänzlich ungeeignet.

KLEINKARIERT IST SICHERER: SOFTWARE-DEFINIERTE MIKROSEGMENTIERUNG

Die Lösung, um die geschilderten Schwächen der Makrosegmentierung zu adressieren, ist zunächst simpel: Der Perimeter muss sehr viel kleiner gefasst werden als das Netzwerksegment und die Kommunikation der einzelnen Ressourcen in einem Netzsegment untereinander muss geregelt werden. Dieser Ansatz wird als softwaredefinierter Segmentierung (SDS) bezeichnet. Es gibt keine eindeutige RFC-Definition für diesen Begriff, aber die Industrie hat sich auf die folgende Definition geeinigt:

Softwaredefinierter Segmentierung ist der Schutz eines Workloads im Netzwerk

Das Problem bei dieser Definition ist die Verwendung des Begriffs *Workload*, da jeder Hersteller diesen Begriff in dem Kontext interpretiert, in dem er sein Produkt am besten platzieren kann. Ein Anbieter, der technisch nicht in der Lage ist, auf einen Host zuzugreifen und z. B. Container-Anwendungen zu segmentieren, definiert den Begriff *Workload* einfach als eine logische Gruppe von Servern, die es zu schützen gilt. Ein anderer Anbieter, der technisch auf Host-Ebene ansetzt und somit Zugang zu den entsprechenden Informationen hat, versteht unter *Workload* hingegen einen Prozess, dessen Kommunikation als Bestandteil einer Applikation zu schützen ist. Weil eine gemeinsame Basis fehlt, ist die Vergleichbarkeit der einzelnen Anbieter mit ihren Lösungen daher leider schwierig.

Tipp: Erst die Ziele abstecken
Am Anfang sollte stets die Frage stehen, was genau das Ziel der Segmentierung ist und bis zu welchem Detaillierungsgrad die Ressourcen heute und mittelfristig geschützt werden sollen. Erst wenn hierüber Klarheit besteht, sollten die nächsten Schritte hinsichtlich der konkreten Ausgestaltung der Mikrosegmentierung geplant werden.

Hardware- oder softwarebasiert segmentieren?

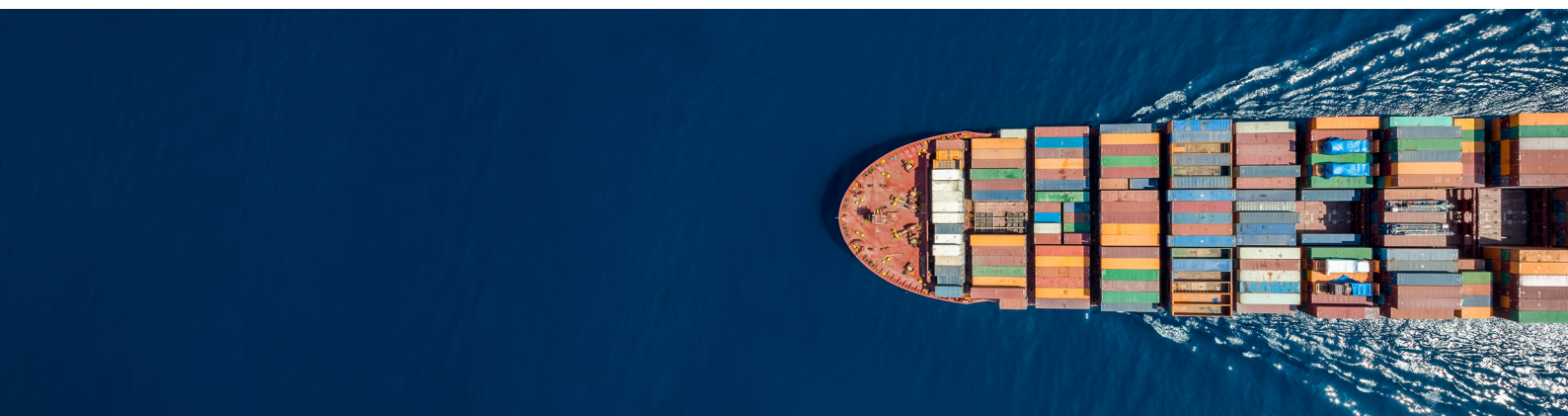
Während Makrosegmentierung immer eindeutig durch Netzwerkkomponenten realisiert wird, ist der Clou von Mikrosegmentierung der softwarebasierte Ansatz. ABER: Es ist möglich, Mikrosegmentierung hardwarebasiert umzusetzen und es gibt Fälle und Bereiche, in denen dieser Ansatz seine Berechtigung hat.

Hardwarebasierte Mikrosegmentierung
Um den Datenverkehr innerhalb eines LANs zu kontrollieren, muss auf einer sehr tiefen Netzwerkebene angesetzt werden. Dies hat zur Folge, dass die vorhandene Hardware für Netzwerk-Switches durch Systeme ersetzt werden muss, die es ermöglichen, Firewall-Policies pro LAN-Port zu definieren. Eine klassische Next Generation Firewall im L2-Modus ist nicht ausreichend, da sie nicht in der Lage ist, jedes einzelne Gerät anzusprechen.

Aus Projektsicht bedeutet dies eine aufwendige Implementierung, da die Netzwerkhardware im Rechenzentrum inklusive Neuverkabelung ausgetauscht werden muss. Der Aufwand für Fallback-Szenarien ist eher gering, da die Migration durch einfaches Umstecken der Systeme erfolgen kann.

Somit ist der kleinste Perimeter das an den LAN-Port angeschlossene Gerät. Eine Ausweitung auf den Schutz einzelner virtueller Systeme auf diesem oder von Containern ist ausgeschlossen.

Wegen der mit dieser Lösung verbundenen hohen Kosten in größeren Umgebungen erfolgt der Einsatz in der Regel in Teilbereichen des Netzwerkes, in denen andere Lösungen aufgrund technischer Restriktionen ausgeschlossen sind. Typische Beispiele für solche Teilbereiche sind etwa Fertigungsstraßen (OT) mit „embedded devices“, nicht stationäre autonome Systeme oder Bereiche, in denen der Einsatz anderer Lösungen aus regulatorischen Gründen ausgeschlossen wird, z. B. in Umgebungen mit hohem Geheimhaltungsgrad.



Softwaredefinierte Mikrosegmentierung (SDS)
Softwaredefinierte Mikrosegmentierung stützt sich auf verteilte Firewalls, die die Durchsetzung der Regeln für den Datenverkehr auf den einzelnen Systemen, also direkt an der Quelle und am Ziel durchführen.

Wesentlich ist, dass dieser Ansatz im Gegensatz zum hardwarebasierten Ansatz **topologieunabhängig** ist. Die Implementierung der einzelnen Firewalls erfolgt auf den Betriebssystemen der einzelnen (virtuellen) Serversysteme und Clients (optional) und ist somit völlig unabhängig von der bestehenden Netzwerkstruktur. Es müssen keine bestehenden VLANs und damit auch keine IP-Adressen und Routing-Mechanismen geändert werden.

Nicht mehr die Restriktionen, die das Netzwerk mit sich bringt, sind ausschlaggebend – **Sicherheit wird aus der Applikationslogik abgeleitet.** Voraussetzung dafür ist allerdings eine sehr detaillierte Erfassung bzw. Sichtbarkeit des vorhandenen Datenverkehrs. Im Gegensatz zur Makrosegmentierung sind moderne SDS-Lösungen in der Lage, die gesamte Kommunikation im Netzwerk automatisiert zu erfassen. Neben der klassischen Sicht können sie, da es sich um hostbasierte Firewalls handelt, auch die initiierenden und empfangenden Prozesse anhand von IP-Adresse, Port und Protokoll identifizieren.

Diese **umfassende Transparenz** erfüllt in der Regel alle regulatorischen Anforderungen aus Sicht des BSI-Grundschutzes und darauf aufbauender Regularien. Gleichzeitig wird die **Umsetzung von Schutzmechanismen bis auf die Prozessebene** einer Applikation ermöglicht. Damit wird verhindert, dass Angreifende oder Schadsoftware sich über Fremdapplikationen lateral bewegen und ausbreiten können.

Aus Projektsicht ergibt sich im Vergleich zur klassischen Makrosegmentierung eine deutlich **verkürzte Durchlaufzeit,** da in der Analyse-, Konzeptions- und Implementierungsphase durchgängig auf die gleiche Datenbasis zugegriffen werden kann und somit aufwändige (meist manuelle) Abgleichszenarien entfallen.

Einer der wichtigsten Punkte ist die **Risikoabschätzung für die Implementierung:** Security Policies werden den verteilten Firewalls zentral zugewiesen. Diese können ohne Netzwerk-Knowhow definiert werden, wodurch eine abteilungsübergreifende Koordination bei der Implementierung entfällt. Ein möglicher Rollback besteht lediglich durch den Rückruf der neu zugewiesenen Policies. Dies ist jedoch in wenigen Sekunden erledigt, wodurch die Planung aufwändiger Rollback-Szenarien unter Einbeziehung des Netzwerkes entfällt und das Ausfallrisiko für die Produktivumgebung gegen Null minimiert wird.

Vorteile der Mikrosegmentierung:

Zeitersparnis
Die Durchgängigkeit der Datenbasis und die einfache Implementierung verkürzen die Projektlaufzeit im Durchschnitt um ein Drittel[2], wodurch interne und externe Ressourcen eingespart werden.

Einheitliche Sicherheitsarchitektur
Über alle Plattformen hinweg, vom „alten“ Rechenzentrum, über Cloud-Umgebungen bis hin zu modernen Container-Umgebungen können einheitliche Schutzmechanismen durchgesetzt werden.

Zero-Trust-Fähigkeit
Mikrosegmentierung ist eine wesentliche Voraussetzung, um eine Zero-Trust-Philosophie umzusetzen. Mikrosegmentierung allein bedeutet nicht automatisch Zero Trust, aber ohne Mikrosegmentierung, egal ob hard- oder softwarebasiert, gibt es **KEIN** Zero Trust.

Tipp: Klassische Firewall weiterhin wichtig

SDS ersetzt die klassischen Firewalls nicht, sondern ist immer als Ergänzung zu verstehen. Die klassische Firewall wird weiterhin zwingend für Nord-Süd-Traffic, Deep Packet Inspektion, sowie die Implementierung weiterer Sicherheitsmaßnahmen etc. benötigt.

[2] Die Angabe basiert auf der Projekterfahrung der Telekom Security in verschiedenen Projekten zur Mikrosegmentierung, die konkrete Zeitersparnis hängt jedoch immer von unternehmens- und projektspezifischen Parametern ab.

ZEIT UND KOSTEN SPAREN

	Aufgabe	Dauer
1	**Klassisches Segmentierungsprojekt**	513
1.1	Anforderungen	125
1.1.1	Rechtliche Bedingungen	41
1.1.1.1	Externe Anforderungen (BSI, KRITIS, B3S)	40
1.1.1.2	Interne Anforderungen (Unternehmensrichtlinie)	40
1.1.2	Ist-Analyse der technischen Plattform	60
1.1.3	Struktur-/Schutzbedarfsanalyse	120
1.2	Analyse der Kommunikationsbeziehungen	120
1.3	Erstellung Segmentierungskonzept	60
1.4	Erstellung Migrationsplan/Rollback-Szenarien	30
1.5	Pilotimplementierung	60
1.6	Konzept-Review	20
1.7	Produktiver Rollout	180
1.8	"Aufräumen"	40

	Aufgabe	Dauer
1	**Software-definiertes Segmentierungsprojekt**	283
1.1	Anforderungen	125
1.1.1	Rechtliche Bedingungen	41
1.1.1.1	Externe Anforderungen (BSI, KRITIS, B3S)	40
1.1.1.2	Interne Anforderungen (Unternehmensrichtlinie)	40
1.1.2	Ist-Analyse der technischen Plattform	60
1.1.3	Struktur-/Schutzbedarfsanalyse	120
1.2	Rollout Agenten	40
1.3	Sichtbarkeit der Kommunikationsbeziehungen	60
1.4	Segmentierungs-/Label-Konzept	40
1.5	Pilot	20
1.6	Produktiver Rollout	100

45%
ZEIT-ERSPARNIS
513
283

Projektdauer im Vergleich[4]

Ökonomische Vorteile von SDS

Die Implementierung von SDS bietet nicht nur verbesserte Sicherheitsmechanismen, sondern auch messbare wirtschaftliche Vorteile. Unternehmen können durch softwaredefinierte Segmentierung signifikante Kosteneinsparungen und Effizienzgewinne bei gleichzeitig höherer Resilienz erreichen.

Zeitersparnis
Die Einführung softwaredefinierter Segmentierung geht deutlich schneller als die Einführung traditioneller, VLAN-gestützten Segmentierung. So ist die Implementierung in der Regel in weniger als sechs Monaten umgesetzt, während herkömmliche Firewall-Implementierungen oft 18 Monate oder länger dauern[3].

TOP 3 ZEITFAKTOREN

45% kürzere Projektlaufzeit

98% schnellere Implementierung von Netzwerkänderungen

Einsatzbereit in **<6** Monaten

Für die Gesamtprojektlaufzeit kann man unserer Erfahrung nach mit einer um 45% verkürzten Projektlaufzeit rechnen, wie die Tabelle unten erkennen lässt. Während die Definition von Anforderungen die gleiche Zeit in Anspruch nimmt, gibt es erhebliche Zeiteinsparungen bei der Pilotierung und dem produktiven Rollout

Noch deutlicher wird die überragende Effizienz von SDS, wenn man sich den laufenden Betrieb ansieht. Vorgänge wie das Einrichten neuer Geräte oder Zugänge, das Anpassen von Sicherheitsrichtlinien oder das Reagieren auf Vorfälle werden traditionell manuell vorgenommen – also durch Konfiguration einzelner Geräte wie Router, Firewalls oder Switches. Laut einer Studie von Forrester im Auftrag von Cisco ist die Implementierung solcher Änderungen im Netzwerk mit SDS beeindruckende 98% schneller[5].

Dies hat mehrere Gründe:

- **Zentrale Steuerung:**
  Änderungen werden einmal definiert und automatisch im ganzen Netzwerk umgesetzt.
- **Automatisierung:**
  Regelbasierte Abläufe sorgen für schnellere Reaktionen – ohne menschliches Zutun.
- **Transparenz:**
  Administratoren sehen sofort, wo welche Regeln gelten und können gezielt eingreifen.
- **Skalierbarkeit:**
  Neue Standorte, Nutzer oder Geräte lassen sich in Minuten integrieren – nicht in Tagen.

TIME-TO-VALUE

Softwaregesteuerte Netzwerke beschleunigen nicht nur die Technik im Hintergrund – sie machen Unternehmen insgesamt agiler. Die beeindruckende Zeitersparnis von bis zu 98% für die Implementierung von Änderungen im Netzwerk bedeutet auch eine 98% schnellere Time-to-Value.

+98%

[3] Akamai (2024) [4] Die Zahlen basieren auf der Umsetzungserfahrung zahlreicher Projekte der Deutschen Telekom. [5] Cisco (2016)

Kostensenkungen

Softwaredefinierte Segmentierung ist nicht nur effizient, sondern ein echter Wirtschaftsfaktor, denn sie führt zu bedeutenden Kostensenkungen – sowohl direkt als auch mittelbar.

Hardware- und Betriebskosten

Durch den Einsatz softwarebasierter Sicherheitsfunktionen kann auf teure Spezialhardware verzichtet werden. So lassen sich Infrastrukturkosten um bis zu 60 % im Vergleich zu klassischen, hardwarebasierten Firewalls senken[6]. Insgesamt können die IT-Betriebskosten durch Automatisierung und Vereinfachung der Architektur sogar um bis zu 80 % reduziert werden[7].

Personalkosten

Die optimierte Sicherheitsarchitektur ermöglicht es, Netzwerke gezielt zu segmentieren und Sicherheitsrichtlinien zentral zu steuern. Das reduziert den manuellen Aufwand erheblich: In der Praxis zeigt sich eine Reduktion des Personalbedarfs in der IT-Security um bis zu 33 % (gemessen in FTEs)[6]. Durch automatisiertes und zentrales Policy-Management sinkt der Arbeitsaufwand für Sicherheitsteams sogar um bis zu 90 %[8].

Compliance

Softwaredefinierte Segmentierung erleichtert auch die Einhaltung gesetzlicher Vorgaben und branchenspezifischer Standards. Vordefinierte und standardisierte Sicherheitsrichtlinien sorgen für eine einheitliche Umsetzung – und reduzieren den manuellen Aufwand bei Dokumentation und Kontrolle. Automatisierte Sicherheitskontrollen ermöglichen zudem schnellere Audits und vereinfachen Zertifizierungsprozesse erheblich. Durch die konsistente Umsetzung von Sicherheitsvorgaben lassen sich nicht zuletzt auch regulatorische Strafen vermeiden – ein wichtiger Faktor, gerade in stark regulierten Branchen.

Sicherheitsvorfälle

Auch die Kosten für Sicherheitsvorfälle sinken deutlich. Bedrohungen werden durch die präzise Segmentierung schneller erkannt und isoliert – das reduziert den Aufwand im Incident-Management um bis zu 70 %[6]. Die sogenannte laterale Ausbreitung – also das Weiterziehen eines Angriffs innerhalb des Netzwerks – kann durch gezielte Abgrenzung einzelner Bereiche um bis zu 66 % eingeschränkt werden[8]. Gleichzeitig verringert sich die Angriffsfläche des Netzwerks um bis zu 80 %, was das Risiko und die finanziellen Auswirkungen von Cyberangriffen nochmals erheblich minimiert[6]. All diese Faktoren tragen dazu bei, dass Unternehmen durch vermiedene Sicherheitsvorfälle jährlich Verluste von bis zu 2% des Umsatzes vermeiden können[6].

[6] VMware (2020)
[7] Cisco (2016)
[8] Illumio (2023)

RECHTLICHE ANFORDERUNGEN MIT SDS ERFÜLLEN

Gastbeitrag von Sandra Effertz, Senior Consultant Information Security, Auditorin der ISO27001, §8a kritische Infrastruktur und BSI-Praktikerin bei de-bit Computer-Service GmbH

Die gesetzlichen Anforderungen an die Sicherheit von Netzwerken und Daten werden immer strenger. SDS bietet eine effiziente Methode, um etwa die hohen Sicherheitsanforderungen des BSI-Kompendiums, der Kritis-Verordnung und der NIS-2-Richtlinie zu erfüllen.

Das IT-Grundschutz-Kompendium des BSI

Das IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnologie enthält zahlreiche Bausteine, die auf den Schutz von IT-Systemen abzielen. Folgende Anforderungsbausteine können auf Basis von softwaredefinierter Segmentierung umgesetzt werden:

INF.2: Netzwerksicherheit
Anforderungen an die Sicherheit der Netzwerkinfrastruktur und Kommunikationswege

Softwaredefinierte Segmentierung ist eine Methodik, um die ein- und ausgehende Kommunikation im Netzwerk jeder einzelnen Ressource zu kontrollieren. Jede Ressource hat spezifische Sicherheitsrichtlinien, die sich aus ihrer Klassifizierung ergeben. Diese Unterteilung minimiert die Angriffsfläche und erschwert es Angreifern, sich lateral im Netzwerk zu bewegen. Durch die granularen Sicherheitskontrollen wird der unautorisierte Zugriff auf kritische Ressourcen verhindert, was den Anforderungen des Bausteins INF.2 gerecht wird.

NET.1.1: Netzarchitektur und -design
Anforderungen an grundlegende Designprinzipien und die Architektur eines sicheren Netzwerks

Eine sichere Netzarchitektur und ein durchdachtes Design sind grundlegende Voraussetzungen für eine stabile und sichere Netzwerkumgebung. Softwaredefinierte Segmentierung spielt hierbei eine zentrale Rolle, indem sie eine strukturierte und organisierte Aufteilung der Ressourcen im Netzwerk ermöglicht. Durch die Einführung klar definierter Sicherheitsebenen können Netzwerke effizienter gestaltet werden, wodurch eine bessere Übersichtlichkeit und Verwaltung der Sicherheitsrichtlinien gewährleistet wird. Dies unterstützt die Umsetzung der Designprinzipien des Bausteins NET.1.1 und trägt zum Aufbau einer robusten Netzarchitektur bei.

NET.1.2: Netzwerksegmentierung und -trennung
Physische und logische Trennung von Netzwerken zur Erhöhung der Sicherheit

Der Baustein NET.1.2 hebt die Bedeutung der physischen und logischen Trennung der Netzwerkmanagementsysteme vom produktiven Netzwerk hervor. Das Produktionsnetz wird vom BSI als besonders schützenswert definiert, da die Infrastrukturkomponenten primäre Angriffsziele mit einem hohen Schadenspotential darstellen. SDS leistet eine hochgranulare Unterteilung der einzelnen Netzwerkmanagement-Ressourcen, wodurch Angriffsvektoren auf die kleinstmögliche Einheit begrenzt werden. Dies trägt besonders zum Schutz von hochsensiblen Informationen und privilegierten Zugriffen im Netzwerk bei und stellt somit eine effektive Methode zur Risikominimierung und Einhaltung der Sicherheitsanforderungen des NET.1.2 Bausteins dar.

NET.3.2
Durch den Einsatz von softwaredefinierter Mikrosegmentierung wird die Umsetzung der Anforderungen aus dem Baustein NET.3.2 maßgeblich erleichtert und professionalisiert. Unternehmen profitieren insbesondere durch die deutliche Reduzierung interner Angriffsflächen, eine flexible Anpassung von Trennungen zwischen Netzbereichen und eine beschleunigte Umsetzung von Sicherheitsrichtlinien. Die granulare Steuerung von Kommunikationsbeziehungen ermöglicht eine dynamische Netzseparierung ohne aufwändige physische Umstrukturierungen. Dadurch werden Betriebsaufwände gesenkt und gleichzeitig höhere Sicherheitsniveaus erreicht. Im Ernstfall kann schneller auf Vorfälle reagiert und betroffene Systeme effektiv isoliert werden, was Ausfallzeiten und Folgeschäden reduziert. Unternehmen erreichen damit nahezu eine vollständige Erfüllung der Netztrennungsanforderungen des BSI IT-Grundschutzes, ohne in kostspielige und starre physische Infrastrukturen investieren zu müssen.

OPS.1: IT-Betrieb
Anforderungen an den sicheren Betrieb von IT-Systemen

Ein sicherer IT-Betrieb erfordert eine kontinuierliche Überwachung und Anpassung der Sicherheitsmaßnahmen. SDS ermöglicht eine dynamische Anpassung der Sicherheitsrichtlinien an die aktuelle Bedrohungslage. Dadurch wird eine hohe Flexibilität im IT-Betrieb gewährleistet. Zudem wird die Anzahl der Sicherheitsvorfälle reduziert, da die Schadensauswirkung im Falle eines Angriffs auf eine einzelne Ressource beschränkt bleibt. Dies vereinfacht das Management und die Behebung von Vorfällen, was den Anforderungen von OPS.1 entspricht.

DER.1: Detektion von Sicherheitsvorfällen
Anforderungen an die Erkennung und Reaktion auf Sicherheitsvorfälle

SDS unterstützt die Erkennung von Sicherheitsvorfällen durch detaillierte Überwachungsmöglichkeiten innerhalb der einzelnen Ressourcen. Anomalien im Netzwerkverkehr können so schneller erkannt und isoliert werden. Dank der kleinteiligen Segmentierung können Sicherheitsvorfälle auf die betroffene Ressource eingegrenzt und sofortige Gegenmaßnahmen eingeleitet werden. Diese proaktive Erkennung und Isolierung von Vorfällen erfüllt die Anforderungen des Bausteins DER.1.

CON.1: Netzsteuerung und -überwachung
Anforderungen an die Kontrolle und Überwachung des Netzwerkverkehrs

Die Steuerung und Überwachung des Netzwerkverkehrs wird durch SDS wesentlich präziser. Jede Verbindung zwischen einzelnen Ressourcen kann überwacht und kontrolliert werden. Der zusätzliche Einsatz von Technologien wie Firewalls und Intrusion Detection Systems (IDS) an zentralen Stellen im Netzwerk ermöglicht eine feingranulare Kontrolle des Datenverkehrs auf verschiedenen Ebenen. Damit wird den Anforderungen des Bausteins CON.1 entsprochen und eine lückenlose Überwachung und Kontrolle des Netzwerkes gewährleistet.

APP.1: Applikationssicherheit
Anforderungen an den Schutz von Anwendungen

Die Sicherheit von Anwendungen kann durch die Isolierung in Mikrosegmente erheblich gesteigert werden. Anwendungen, deren Ressourcen in separaten Netzwerkbereichen laufen, sind besser vor Angriffen aus anderen Teilen des Netzwerks geschützt. Spezifische Sicherheitsrichtlinien für jede Ressource stellen sicher, dass nur autorisierte Benutzer und Anwendungen darauf zugreifen können. Dies minimiert das Risiko von Sicherheitslücken und erfüllt die Anforderungen des Bausteins APP.1.

Die BSI-Kritisverordnung

Die Verordnung über die Anforderungen an die IT-Sicherheit von kritischen Infrastrukturen (Kritisverordnung) verlangt von Betreibern kritischer Infrastrukturen spezifische Sicherheitsmaßnahmen, um die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Systeme zu gewährleisten.

SDS trägt zur Erfüllung der Anforderungen der Kritis-Verordnung bei, indem sie eine detaillierte und strikte Trennung kritischer Systeme und Dienste ermöglicht. So verhindert Mikrosegmentierung, dass Sicherheitsvorfälle in einem Bereich die gesamte Infrastruktur beeinträchtigen und unterstützt damit die Verfügbarkeit, Integrität und Vertraulichkeit der IT-Systeme. Durch die spezifische Kontrolle und Überwachung jeder einzelnen Ressource können Betreiber kritischer Infrastrukturen gezielte Schutzmaßnahmen ergreifen, die den hohen Sicherheitsstandards der Verordnung entsprechen.

Die NIS-2-Richtlinie

Die NIS-2-Richtlinie zielt darauf ab, die Cybersicherheit in der EU zu stärken, indem sie höhere Sicherheitsanforderungen an Anbieter digitaler Dienste und Betreiber wichtiger Dienste stellt. Zu den Anforderungen zählen Maßnahmen zum Risikomanagement, Meldepflichten bei Sicherheitsvorfällen und die Zusammenarbeit zwischen den Mitgliedstaaten.

SDS bietet einen entscheidenden Vorteil bei der Erfüllung der NIS-2-Richtlinie: Sie ermöglicht eine strukturierte und detaillierte Überwachung sowie eine schnelle Reaktion auf Sicherheitsvorfälle. Durch die Isolierung einzelner Ressourcen können Vorfälle effizient eingedämmt und Schäden minimiert werden. Darüber hinaus unterstützt SDS die Erfüllung der Meldepflichten, da Vorfälle schneller erkannt und gemäß den Anforderungen der NIS-2-Richtlinie gemeldet werden können.

Richtlinienkonform und zertifizierungsreif

SDS bietet eine umfassende Lösung zur Erfüllung der Sicherheitsanforderungen des IT-Grundschutz-Kompendiums, der Kritisverordnung und der NIS-2-Richtlinie. Die Kontrolle der einzelnen Ressourcen im Netzwerk erhöht die Kontrolle über den Netzwerkverkehr und reduziert mögliche Angriffsflächen. Dies führt zu einem robusteren, widerstandsfähigeren Netzwerk, das besser vor Bedrohungen geschützt ist und hohen Anforderungen an Informationssicherheit gerecht wird.

Neben den Sicherheitsanforderungen selbst steigen auch die externen Anforderungen an Unternehmen, die Umsetzung der Sicherheitsanforderungen nachzuweisen. Softwaredefinierte Segmentierung bietet eine richtlinienkonforme Umsetzung der gesetzlichen Anforderungen und damit eine aus technischer Sicht zertifizierungsreife Lösung.

ANWENDUNGSBEISPIELE

In Kooperation mit unserem Partner:

Akamai

Softwaredefinierte Segmentierung komplexer Serverlandschaft

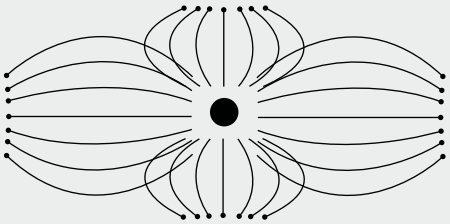
Unser Kunde aus dem Finanzsektor stand vor der Herausforderung, die BaFIN-Vorgaben zur IT-Sicherheit kurzfristig umsetzen zu müssen. Bisher hatte das Unternehmen mit 3.000 virtualisierten und physischen Servern nur auf Makrosegmentierung mit klassischer Firewall-/ VLAN Technologie gesetzt.

Herausforderung
Voraussetzung zur Umsetzung des Segmentierungsprojektes ist die detaillierte Sichtbarkeit aller Kommunikationsbeziehungen. Die Komplexität der gewachsenen Strukturen erschwerte die Herstellung dieser Transparenz, was zu einem Projektstopp geführt hatte.

Lösung
In einem ersten Schritt erfolgte ein Rollout der Akamai Guardicore Agenten zur Aufzeichnung der Kommunikation. Über Netzwerkmechanismen wurden dann die Bestandssysteme eingebunden, so dass alle Kommunikationsbeziehungen im Unternehmen an einer zentralen Stelle einsehbar waren. Auf Basis der dynamischen Akamai Guardicore Labels war in einem zweiten Schritt die agile Erzeugung von Security Policies möglich. Die Richtlinienumsetzung zur Reduzierung erlaubter Kommunikation erfolgte anschließend ohne den Rollout weiterer Software und ohne Umbauten im Netzwerk – die Anpassung von IP-Adressen oder Routing war nicht nötig.

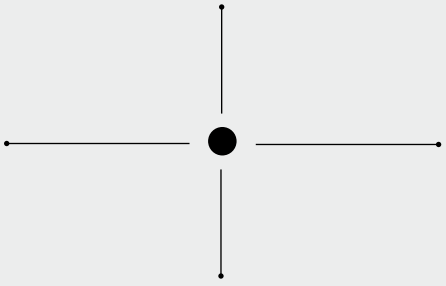
Kundennutzen
Der schlanke Projektablauf mit kurzfristig greifbaren Ergebnissen ermöglichte die Konzentration der Projektressourcen auf die komplexen Bereiche, so dass die Vorgaben der BaFIN schnell umgesetzt werden konnten. Das Unternehmen profitiert zudem von der plattform- und betriebssystemunabhängigen Transparenz über sämtliche Kommunikationsbeziehungen.

Angriffsfläche **ohne Segmentierung**



229.500 Kommunikationspfade

Angriffsfläche **nach der Segmentierung**
*Erlaubte eingehende Verbindungen zur Zielapplikation



2.465 Kommunikationspfade

Allen Entitäten wird per Default-Einstellung nicht getraut, Least-Privilege-Prinzip wird umgesetzt

Mehr Sicherheit für die Produktion

Unser Kunde, ein produzierendes Unternehmen mit zahlreichen internationalen Standorten auf vier Kontinenten, wollte die Sicherheit seiner Operativen Technologie (OT) erhöhen. An allen Standorten zusammen sind derzeit über 10.000 Endgeräte installiert, die der OT zugeordnet sind.

Herausforderung

Eine dezidierte Trennung zwischen der IT- und der OT-Welt fehlt bislang. Schwachstellen in der OT können so zum Beispiel direkt aus dem Internet oder über kompromittierte IT-Systeme ausgenutzt werden. Das Sicherheitsniveau des Netzwerkes soll deshalb in einem ersten Schritt dadurch erhöht werden, dass eine physische Netzwerktrennung implementiert wird. Angestrebt wird eine Gestaltung des OT-Netzwerks nach der IEC 62443 Norm.

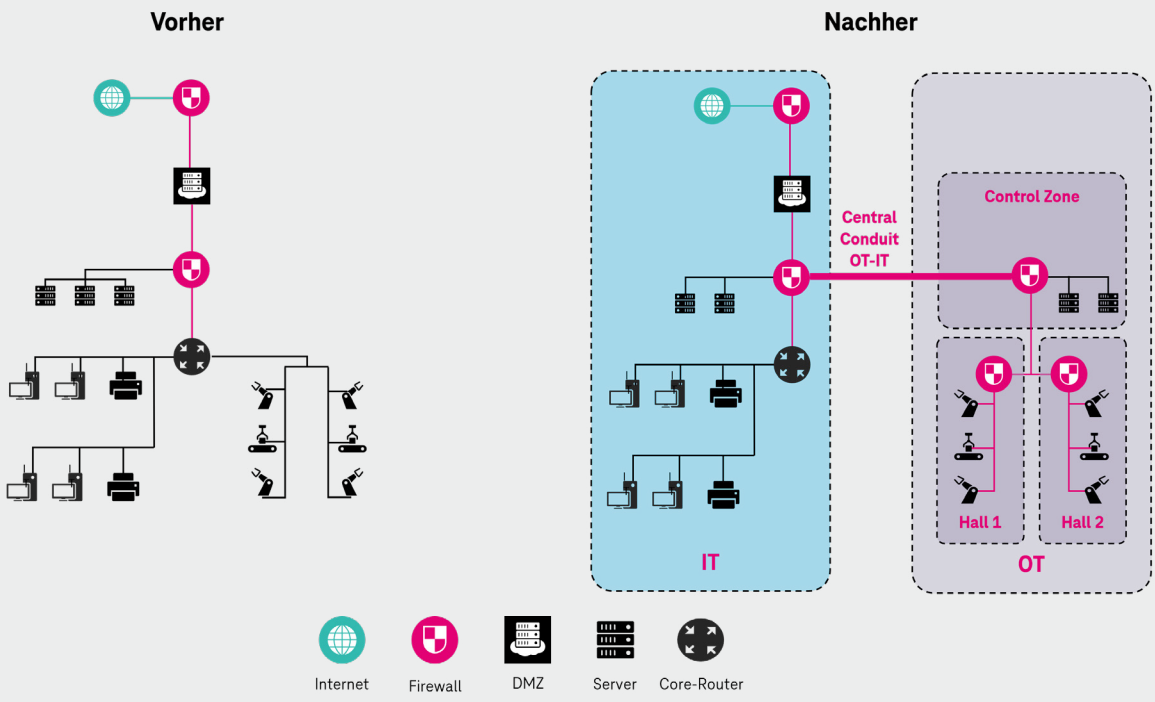
Lösung

Das Produktionsnetzwerk wird durch einen zentralen Übergang vom IT-Bestandsnetz getrennt. Dazu wird ein zentrales OT-Firewall-Cluster eingesetzt, das durch eine industrielle DMZ unterstützt wird. Neben der Schaffung einer eigenen OT-Hosting-Zone, in der künftig sowohl Netzwerkbasisdienste als auch OT-Applikationen zur Verfügung gestellt werden, werden die einzelnen Hallenbereiche durch dedizierte Firewall-Cluster abgesichert. Durch diese Architektur entsteht eine Zonierung des Netzwerkes, das die verschiedenen Produktionsbereiche von anderen Bereichen wie z.B. der Logistik grundlegend trennt.

Das gesamte Netzwerk wird auf der physischen Ebene durch den Neuaufbau von Security-Switchen realisiert. Diese werden zentral über die jeweiligen Hallen-Firewalls mit verwaltet. Dadurch ist es möglich, spezielle Security-Bereiche auf einer sehr granularen Ebene über das Firewall-Regelwerk zu definieren.

Kundennutzen

Das Produktionsnetz ist durch die Mikrosegmentierung bestmöglich vor Datenklau und Sabotage geschützt. Gleichzeitig leistet die Mikrosegmentierung neben der grundsätzlichen Trennung von OT- und IT-Welt auch die dedizierte Isolierung kritischer Endgeräte. Dies können etwa Produktionsgeräte sein, die auf Grund langer Einsatzzyklen mit veralteten Betriebssystemen arbeiten. Dank des punktgenauen Einsatzes der Sicherheitsmechanismen wird die Leistungsfähigkeit des Netzwerkes nicht eingeschränkt. Die zentrale Verwaltung aller eingesetzten Netzwerkkomponenten ermöglicht eine durchgängige Umsetzung der Sicherheitsrichtlinien. Durch den Einsatz spezieller Security-Switche ist auch eine unabhängige von der Routing-Grenze durchführbare Umsetzung möglich. Dies ermöglicht eine feingranualare Anpassung des Sicherheitsniveaus und schnelle Reaktionszeiten bei Änderungen und/oder Angriffen.



In Kooperation mit:

COLORTOKENS

Einheitlichen Sicherheitsarchitektur für IT und OT

Unser Kunde, ein vertriebsorientiertes Unternehmen, hat seine Applikationen fast vollständig in die Public Cloud verlagert, nur einige Applikationen werden als SaaS-Dienst genutzt. Darüber hinaus betreibt er jedoch ca. 350 OT-Assets einer kleinen Fertigung in Eigenregie. Ziel des Projektes war die Herstellung einer einheitlichen Sicherheitsarchitektur für IT und OT.

Herausforderung

Grundsätzlich wird ein effizienter Betrieb der zu implementierenden Lösung angestrebt, der das kleine unternehmenseigene IT-Team nicht überlastet. Auch die Umstellung muss dem Budget des Mittelständlers entsprechend kosteneffizient gestaltet werden. Eine weitere Herausforderung: Im OT-Bereich handelt es sich teilweise um sehr alte Systeme (Windows XP Steuerrechner) und/oder ein Eingriff auf diese Systeme ist auf Grund von Herstellerrestriktionen nicht möglich.

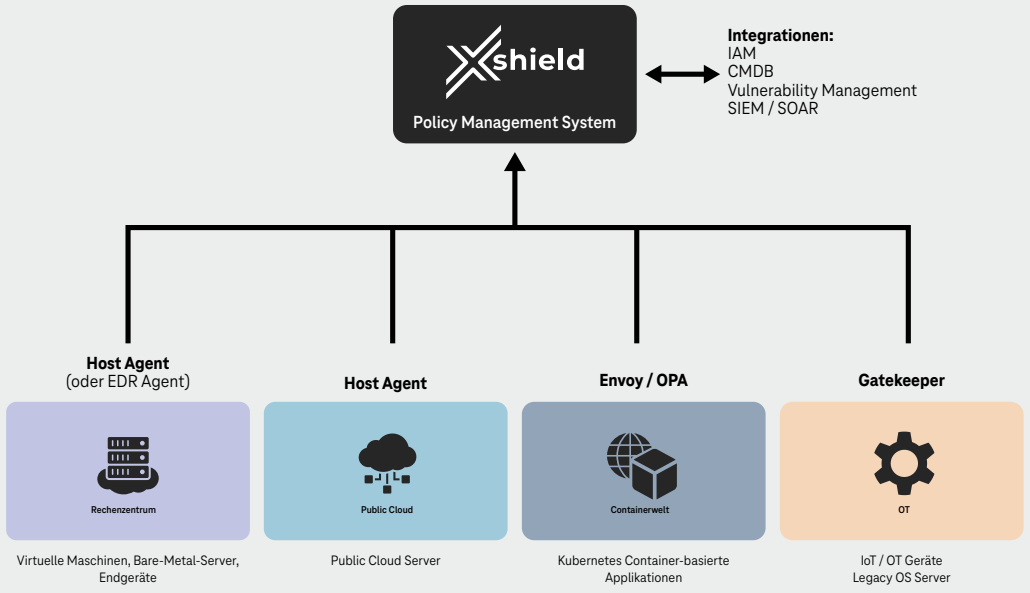
Lösung

Die Netzwerksicherheit ist bereits durch den Einsatz von Firewalls grundlegend gegeben, ebenso die Trennung zwischen den Cloud-Tenants und der OT-Umgebung. Um den Anforderungen des Kunden nach digitaler Resilienz zu entsprechen, wird eine softwarebasierte Mikrosegmentierungslösung implementiert, die nichtautorisierte laterale Bewegungen verhindert. Auf den Serversystemen in der Cloud werden hierfür Agenten installiert. So kann die Sicherheit der einzelnen Systeme unabhängig von den Einstellungen des Cloudanbieters granular gesteuert werden. Über einen bestimmten Zeitraum erfasst die Lösung automatisch alle bestehenden Verbindungen, um daraus Zero-Trust-Policies abzuleiten, die die Kommunikation begrenzen.

Eine besondere Herausforderung ist die Integration der OT-Umgebung, da der Einsatz von Agenten auf der Mehrheit der OT-Assets nicht möglich und eine manuelle Integration in die Verwaltungsebene zu aufwendig ist. Die Lösung von Colortokens ermöglicht es, sowohl die IT- als auch die OT-Umgebung einheitlich zu verwalten. Sie bietet Sichtbarkeit und Durchsetzung von Security Policies in einer vereinheitlichten Umgebung sowohl für die Serversysteme in der Cloud als auch für das OT-Umfeld. Hierfür wird an einem zentralen Punkt im OT- Netzwerk eine Gatekeeper Appliance installiert und mit minimalen Eingriffen in das Netzwerk der Datenverkehr umgeleitet.

Kundennutzen

Der Kunde erhält eine einheitliche Verwaltung und Kontrolle für alle Endgeräte mit nahezu Echtzeitsichtbarkeit von Netzwerkverbindungen. Die Installation in beiden Welten, IT und OT, erfolgt risikoarm, da sowohl der Rollout der Agenten in der IT als auch die Installation der Gatekeeper Appliance in der OT zunächst keinerlei Einfluss auf die Produktionsdaten nimmt. Weil im OT-Umfeld die bestehende Netzwerkinfrastruktur (Verkabelung, Switche und Router) sowie die logische Netzwerkkonfiguration (VLAN, Routing) vollständig beibehalten werden, ist die Lösung mit weniger Kosten verbunden als Alternativlösungen. Im IT-Bereich besteht der Budgetvorteil darin, dass keine wesentlichen Vorabinvestitionen getätigt werden müssen, sondern die Lizensierung nach und nach erfolgen kann.



FAZIT: JETZT GEFAHREN EINDÄMMEN

Softwaredefinierte Segmentierung ist eine effektive Strategie, um Sicherheit im gesamten Netzwerk zu etablieren. Das gilt sowohl für moderne Multicloud-Architekturen als auch für flache MPLS-Netzwerke, vom Kleinunternehmen bis zum Großkonzern.

Komplexe Multiplattform-Netzwerke
Moderne IT-Umgebungen auf verteilten Plattformen benötigen eine durchgängige Security-Architektur. Die klassischen Ansätze der rein netzwerkbasierten (Makro-)Segmentierung sind jedoch nur in Teilen dieser Umgebungen implementierbar. Sie funktionieren nur dort, wo ich Kontrolle über das Netzwerk habe, was bei Cloudplattformen nicht der Fall ist. Zudem sind sie viel zu grob in ihren Perimetern und sehr aufwändig zu implementieren. Softwaredefinierte Mikrosegmentierung ist hier die erste Wahl.

Flache (MPLS-)Netzwerke
Aber auch wer bisher ein eher flaches Netz, im LAN oder WAN auf MPLS Basis, hat, sollte sich überlegen, ob der direkte Einstieg in die Mikrosegmentierung nicht effizienter, schneller und kostengünstiger ist und deutlich bessere Ergebnisse bringt.

OT oder Umgebungen mit besonderen Anforderungen
Es gibt auch Umgebungen mit besonderen Anforderungen, etwa in der industriellen Produktion. Auch Bereiche mit hohen Auflagen an die Geheimhaltung (VS-NfD) zählen dazu. In solchen Umgebungen kann eine Kombination aus software- und hardwarebasierter Mikrosegmentierung erforderlich sein. Wichtig ist dann, die Segmentierung trotzdem aufeinander abgestimmt umzusetzen. Sind zu viele Brüche und Security-Anbieter involviert, ist eine Konsolidierung empfehlenswert.

Klare ökonomische Vorteile
Softwaredefinierte Segmentierung bietet jedoch nicht nur mehr Sicherheit, sondern punktet auch mit messbaren ökonomischen Vorteilen. Zunächst bringt sie eine deutliche Zeitersparnis in der Projektumsetzung mit sich, was die Time-to-Value um 98% beschleunigt.
Darüber hinaus führt die Einführung von SDS zu bedeutenden Kostensenkungen. IT-Betriebskosten fallen durch die Automatisierung um 80% geringer aus, die Kosten für Infrastruktur und Hardware sinken um 60% und die Incident-Kosten sinken um 70%.

AUF DEN ERNSTFALL VORBEREITET?

Es ist leider nicht mehr die Frage, OB ein Unternehmen angegriffen wird, sondern vielmehr, WANN es passieren wird. Sind Sie für einen potenziellen Angriff gewappnet und ist Ihr System in der Lage, auch mit unbekannten Gefahren zurechtkommen?

Gern unterstützen wir Sie auf dem Weg zu effektiver Prävention mit softwaredefinierter Segmentierung.

Interesse oder weitere Fragen?

Wir freuen uns auf Ihre Mail oder Ihren Anruf!

Unser Angebot: Orientierungsworkshop

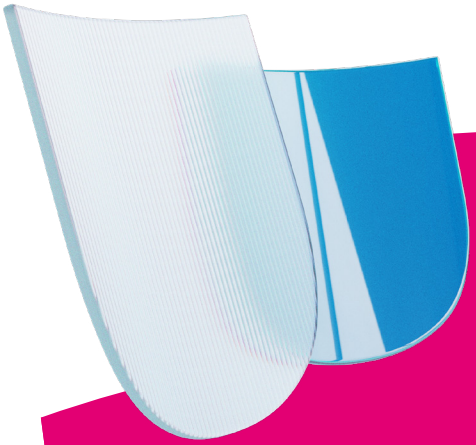
Sie möchten SDS einführen, stehen aber noch am Anfang? Unser Workshop bietet einen schnellen Überblick und fachkundige Unterstützung bei der Einführung von softwaredefinierter Segmentierung. Gemeinsam klären wir bei Ihnen vor Ort im Rahmen eines eintägigen Workshops, was es zu beachten gilt.

Wo stehen Sie?
Dabei geht es um Ihre individuelle Situation inklusive interner und externer Anforderungen. Welches Knowhow ist bereits heute im Unternehmen vorhanden, welche Security-Produkte sind im Einsatz?

Wo geht die Reise hin?
Was sind die *low hanging fruits* – wo können mit SDS schnelle Ergebnisse erzielt werden? Gibt es Bereiche, in denen sich SDS verbietet? Und wo ist bereits Netzwerksegmentierung vorhanden, die weiterentwickelt werden kann oder integriert werden muss?

Unsere Experten nehmen sich Zeit, damit Sie schneller und sicherer ans Ziel kommen. Ohne Schiffbruch.

Deutsche Telekom Security GmbH | 05/2025



Kontakt
security.dialog@telekom.de
security.telekom.de

Herausgeber
Deutsche Telekom Security GmbH
Office Port 1
Friedrich-Ebert-Allee 71–77
53113 Bonn

Connecting your world.