NetDescribe

NetDescribe Use Case

Netzwerk-Segmentierung | verteilte Standorte

mit Akamai Guardicore

www.**netdescribe**.com

1. Die Ausgangssituation

Die Zahl der erfolgreichen Cyber-Angriffe auf deutsche Unternehmen wächst. Angreifer*Innen beschränken sich längst nicht mehr nur auf lokale Ressourcen, sondern weiten ihre Angriffe auf die gesamte IT-Landschaft aus. Die zunehmende Vernetzung zwischen Geräten, Tools und Nutzer*Innen spielt ihnen dabei in die Hände. Vielen Unternehmen mangelt es an den nötigen Sicherheitspraktiken, um ihre Systemumgebungen und Daten über mehrere Rechenzentren und Clouds hinweg konsistent zu schützen.

Diese Situation wirft bei vielen Unternehmen die Frage auf, ob eine Cyber Versicherung, wie sie von vielen großen Versicherungskonzernen angeboten wird, ausreicht, um das Risiko eines Angriffs zu minimieren.

Kann man sich gegen Cyber-Angriffe versichern?

Eine Cyber Security Versicherung gegen Angriffe, Erpressungen und Datendiebstahl scheint zunächst ein verlockender Gedanke zu sein. Viele Unternehmen halten dies für einen wichtigen Schritt zur Prävention.
Leider ist es ein Trugschluss, dass diese Versicherungen bereits eine Risikominderung darstellen. Denn ausschlaggebend für den Abschluss und die Konditionen einer solchen Police sind die vom Unternehmen selbst ergriffene Maßnahmen zum Schutz gegen mögliche Cyber-Attacken. Dabei gilt: je mehr technische Maßnahmen das Unternehmen bereits umgesetzt hat, desto vorteilhafter, bzw. kostengünstiger wird eine Police. Zu den Sicherheitsempfehlungen der Versicherer gehört unter anderem die Netzwerksegmentierung.

2. Der Use-Case

Im konkreten Fall geht es um ein Unternehmen aus der Automobil Handelsbranche mit 17 verteilten Standorten in Deutschland, das sich um eine Cyber Security Versicherung bemüht.
Um der Vorgabe einer Netzwerksegmentierung zu entsprechen, sollte ursprünglich eine Lösung mit Hardware Firewalls realisiert werden. In der weiteren Planung stellte sich jedoch heraus, dass der enorm hohe zeitliche und praktische Aufwand gegen eine solche Lösung spricht.

Die Lösung von NetDescribe

Nach nur wenigen, aber intensiven Beratungs-gesprächen mit NetDescribe und einem technischen Deep Dive konnten wir den Kunden von einer Netzwerksegmentierung mit der Technologie von Akamai Guardicore Segmentation überzeugen.

Zwei Hauptfaktoren waren für die Entscheidung ausschlaggebend: Kosten und Zeit.

Erstens war die softwarebasierte Lösung von Akamai Guardicore wesentlich günstiger als die Investition in 52 hardwarebasierte Firewalls (pro Standort 3 Firewalls + ein Backup).

Zweitens konnte der Projektplan für die Umsetzung der Netzwerksegmentierung von 12 Monaten auf fünf Monate reduziert werden.

Was ist Akamai Guardicore Segmentation?

Die Akamai Guardicore Centra Plattform ist eine softwarebasierte Lösung zur Netzwerk-segmentierung. Sie ermöglicht umfassende Transparenz auf Prozessebene, verhaltens-basierte Richtlinien und Echtzeiterkennung von Sicherheitsverstößen, um die wichtigsten Ressourcen Ihres Unternehmens zu schützen.
Im Ergebnis erhalten Sie eine kosteneffiziente, schnelle Lösung für konsistente Sicherheit – egal für welche Anwendung, egal in welcher IT-Umgebung.

Was bedeutet Netzwerksegmentierung

Bei der Netzwerksegmentierung wird das eigene Netzwerk in kleine separate Segmente (Subnetzwerke) unterteilt.
Oftmals wird das Netzwerk in drei logische Zonen aufgeteilt: “Trusted Zone, DMZ & Management Zone“, um diese mit Sicherheitskontrollen voneinander abschotten zu können.
Wichtig ist, dass alle Systeme innerhalb einer Zone ähnliche Anforderungen an den Schutzbedarf stellen. Gradmesser und Taktgeber ist dabei das System, welches die höchsten Anforderungen stellt.

Was ist Mikrosegmentierung?

Die effektivste Methode, die Verbindung zwischen Servern einzuschränken, ist die Segmentierung des Netzwerks. Es gibt drei grundlegende Arten der Netzwerksegmentierung, wobei die Mikrosegmentierung die Herangehensweise ist, die Unternehmen verwenden können, um zunehmend granulare Richtlinien und Einschränkungen durchzusetzen.

Abb. 1: Beispiel flaches Netzwerk verteilte Standorte

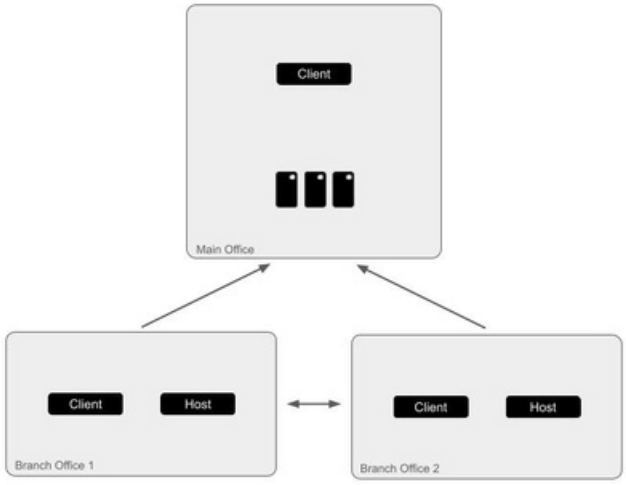


Abb. 2: Beispiel (flaches) Netzwerk Segmentierung

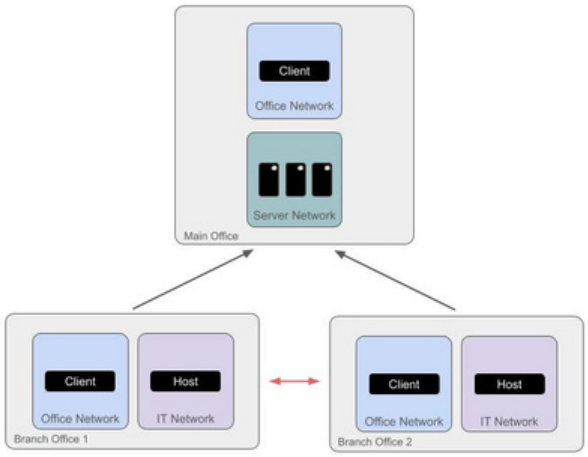
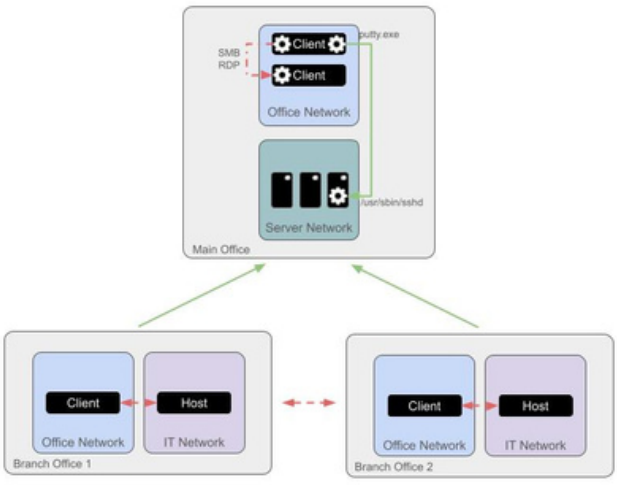


Abb. 3: Beispiel Mikrosegmentierung (flaches Netzwerk)



Umgebungs-Segmentierung

Dieser Ansatz trennt verschiedene Umgebungen voneinander. So kann in Ihrem Unternehmen beispielsweise der Entwicklungsbereich von der Produktionsumgebung getrennt werden.
Das ist die erste, entscheidende Phase jeder Segmentierungsstrategie, auf die weitere Segmentierungen folgen.

Anwendungs-Segmentierung

Dieses sogenannte "Ring-Fencing" trennt jede spezifische, kritische Anwendung vom Rest des Netzwerks. Die besten Mikrosegmentierungs-Lösungen ermöglichen sogar eine Steuerung auf Prozessebene.

Prozess-Segmentierung

Die engste Form der Segmentierung findet innerhalb einer Anwendung statt. Hier können Sie Policies für die Verwaltung der Kommunikation zwischen Ebenen innerhalb desselben Anwendungs-Clusters erstellen und beispielsweise den Datenverkehr zwischen Web-, Anwendungs- und Datenbankservern steuern.

Ohne Absicherung Ihrer IT-Systeme, keine Cyberversicherung!

Das Interesse an Cyberversicherungen ist groß, denn täglich sorgen neue Ransomware-Fälle für Schlagzeilen. Der Wunsch, den finanziellen Schaden durch eine Versicherung abzufangen, ist verständlich.
Die Angriffe sind aber nicht das einzige Problem. Viele Unternehmen ergreifen immer noch wenige oder unzureichende IT-Sicherheitsmaßnahmen und vergessen elementare Basics wie Backup/Restore, Systemhärtung und **Netzwerksegmentierung**.

Die Versicherungsbranche reagiert auf die hohe Zahl an Schadensmeldungen mit schlechteren Konditionen und hohen Prämien. Wollen Sie als Unternehmen eine solche Police abschließen, müssen Sie anhand einer detaillierten Checklist nachweisen, wie gut Ihre IT-Systeme abgesichert sind. Werden grundlegende Maßnahmen nicht erfüllt, steigt das Risiko. Schlimmstenfalls erhält Ihre Firma gar kein Versicherungsangebot.

Vorteile der softwarebasierten Netzwerksegmentierung mit Akamai Guardicore Segmentation

- Umsetzungsdauer 5 Monate
- Setup der SaaS Plattform
- Verteilung des Software-Agenten mit den vorhanden IT-Systemen (ohne Ausfallzeiten)
- logische Gruppierung der Assets in der Plattform
- Segmentierung durch Erstellung von Sicherheitsregeln auf Basis der logischen Gruppierung der Assets und den gesammelten Kommunikationsbeziehungen

Netzwerksegmentierung ist daher die Best-Practice-Lösung für Ihre IT-Sicherheit!

Nachteile der Netzwerksegmentierung mit Firewalls

- Umsetzungsdauer 12 Monate
- Definition neuer Netze/Segmente für alle Standorte
- PreSetup von Perimeter Firewall und Switches
- Integration der Hardware Firewall in das vorhandene Netzwerk an den jeweiligen Standorten (vor Ort bzw. Remote mit Ausfallzeiten)
- Neue IP-Adressen der jeweiligen neuen Netzsegmente auf den Systemen konfigurieren (vor Ort bzw. Remote mit Ausfallzeiten)
- Segmentierung durch Erstellung von Sicherheitsregeln, nachdem alle vorherigen Schritte erfolgreich durchgeführt wurden (Idealerweise werden die Firewall-Regeln schon im PreSetup definiert. Oft sind aber nicht alle Kommunikationsbeziehungen bekannt.)

Vergleich Hardware- und Software-basierte Segmentierung

Eine nachträgliche Netzwerksegmentierung, mit einer hardwarebasierten Firewall, setzt eine Umstrukturierung der vorhandenen IT-Infrastruktur voraus.
Diese muss entsprechend geplant und über alle erforderlichen Systeme umgesetzt werden.
In den meisten Fällen ergibt sich ein hoher Zeit- und Arbeitsaufwand, der eine Downtime der bereitgestellten Dienste und ggf. eine nachträgliche Anpassung an die Software mit sich bringt.

Eine nachträgliche Netzwerksegmentierung, die mit einer softwarebasierten Lösung umgesetzt wird, kann unterbrechungsfrei im laufenden Betrieb erfolgen, da die existierende IT-Infrastruktur nicht geändert werden muss.
Durch den softwarebasierten Ansatz werden die entsprechenden Kommunikationsbeziehungen (bis auf Prozess- und Benutzerebene) protokolliert und können im Anschluss zur Erstellung der Segmentierung genutzt werden. Unabhängig davon, in welchem Netz (RZ, On Premises, Cloud) sich die Systeme befinden.