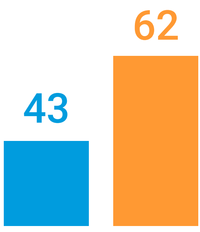
INFOGRAFIK

Segmentierung: Der Schlüssel für Finanzdienstleister auf ihrem Weg zu Zero Trust

Bereitstellungshindernisse zum Schutz kritischer Banksysteme überwinden

Angesichts einer erheblichen Zunahme an Ransomware-Angriffen haben nur die Finanzinstitute mit fortgeschrittener Segmentierung ihre Abwehr weiterentwickelt und den finanziellen und betrieblichen Aufwand verringert.

Die Anzahl der (erfolgreichen und erfolglosen) Ransomware-Angriffe ist in den letzten zwei Jahren um 50 % gestiegen …



… von durchschnittlich 43 im Jahr 2021 auf 62 im Jahr 2023.

92 %

der Entscheidungsträger im Bereich IT-Sicherheit stimmen zu, dass Segmentierung entscheidend ist, um schädliche Angriffe abzuwehren.

88 % der Finanzinstitute geben an, dass die Mikrosegmentierung für ihr Unternehmen mindestens eine hohe Priorität hat, wobei sie bei 39 % der Befragten oberste Priorität hat.

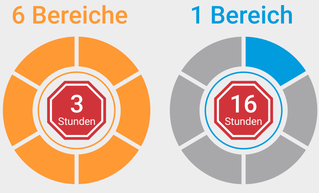
Obwohl an die Technologie geglaubt wird, verläuft die Implementierung der Segmentierung schleppend. Nur 39 % der Finanzdienstleister haben 2023 mehr als zwei kritische Geschäftsbereiche segmentiert (gegenüber 26 % im Jahr 2021), und 45 % haben vor zwei oder mehr Jahren ein Netzwerksegmentierungsprojekt gestartet, was darauf hindeutet, dass die Bemühungen zum Stillstand gekommen sind.

Die Einführung eines Zero-Trust-Frameworks gehört zu den wichtigsten Gründen, warum Finanzinstitute ein Segmentierungsprojekt gestartet haben. Weniger als die Hälfte (47 %) gibt jedoch an, dass die Implementierung des Zero-Trust-Frameworks vollständig definiert und abgeschlossen ist.

Durchhaltevermögen zahlt sich aus. Unternehmen, die sechs wichtige Geschäftsbereiche segmentiert haben, konnten ihre Verteidigung weiterentwickeln.

Der Umfang der Segmentierung ist wichtig

Nach einem Angriff wird Ransomware mehr als 5-mal schneller gestoppt, wenn sechs Bereiche segmentiert werden.



Wie können Finanzinstitute von Segmentierung profitieren?

01
Die Einhaltung gesetzlicher Vorschriften mit detaillierten Einblicken vereinfachen und beschleunigen

02
Wichtige Systeme wie Geldtransfers, Zahlungen und Kundenanwendungen schützen

03
Unbefugte laterale Netzwerkbewegungen verhindern, indem der Zugriff von Dritten ordnungsgemäß isoliert und Zugangswege verwaltet werden

04
Cloud-, PaaS- und andere neue Technologien auf kosteneffiziente und sichere Weise anpassen

Laden Sie den vollständigen Bericht herunter, um Ihre Zero-Trust-Initiative zu starten

 | Support | Veröffentlicht: Mai 2024