Ist Ihre Legacy-Firewall Zero-Trust-tauglich?

Heutzutage wird überall digital gearbeitet — nicht nur im Büro, sondern auch im Flugzeug, im Homeoffice und in der Fabrik. Mit der Verlagerung von Anwendungen in die Cloud bzw. der Nutzung von SaaS-Applikationen fungiert das Internet zunehmend als neues Unternehmensnetzwerk. **Ist Ihre Legacy-Firewall den Anforderungen eines zukunftsfähigen Zero-Trust-Ansatzes zum Schutz von Usern, Daten und Anwendungen gewachsen?** Wir verraten Ihnen, welche Warnsignale darauf hindeuten, dass es Zeit für einen Wechsel zu einer neuen Lösung ist.

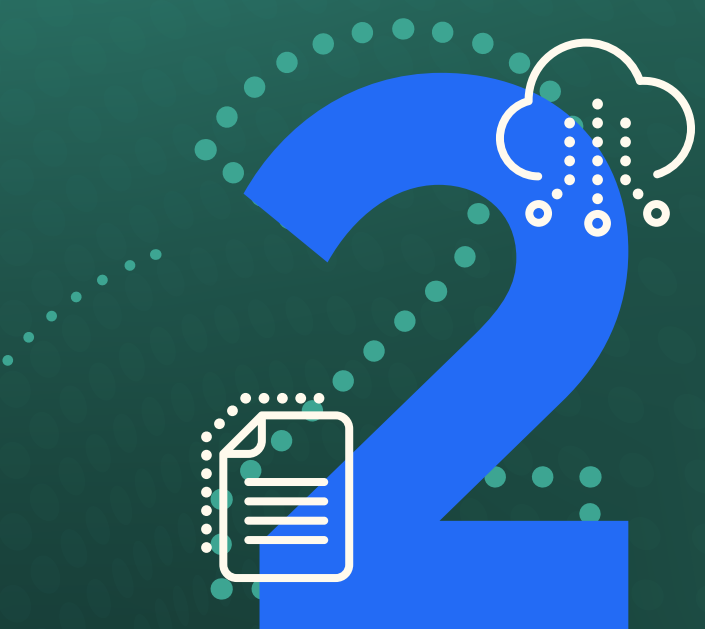
WARNSIGNAL NR. 1

Keine Erkennung lateraler Bewegungen

Als die User noch im Büro saßen und alle Unternehmensanwendungen sich in Rechenzentren befanden, wo sie von herkömmlichen Firewalls geschützt wurden, wurden Ressourcen und Entitäten innerhalb des Netzwerks automatisch als vertrauenswürdig eingestuft. Gelingt es in einer solchen Konstellation einem Bedrohungsakteur jedoch, sich unbefugten Zugang zum Netzwerk zu verschaffen — sei es durch Kompromittieren legitimer User, Ausnutzen einer Fehlkonfiguration oder wegen anderer Schwachstelle —, wird es fast unmöglich, laterale Bewegungen in Echtzeit zu blockieren.

WARNSIGNAL NR. 2

Gefährdete Cloud-Ressourcen



Virtuelle Firewalls werden als VM-Instanzen in der öffentlichen Cloud ausgeführt. Dabei muss an jedem Ausgangs- und Eingangspunkt eine Instanz bereitgestellt werden. Herkömmliche Firewalls wurden zur Sicherung des Netzwerkperimeters entwickelt. Sie gewährleisten keinen Schutz vor Bedrohungsakteuren, die Schwachstellen in Cloud-Umgebungen ausnutzen, um die Integrität und den Sicherheitsstatus Ihrer Workloads und vertraulichen Daten zu kompromittieren.

WARNSIGNAL NR. 3

Hang zu freizügigen Richtlinien

Im Bestreben, innovative Produkte schneller zur Marktreife zu bringen, bitten agile Entwickler ihre IT- und Sicherheitsadministratoren gerne um die Einrichtung sehr freizügiger Richtlinien, die dann allzu oft nach Abschluss des Projekts nicht wieder aufgehoben werden. Herkömmliche Firewalls sind nicht flexibel genug, um dynamische Richtlinienänderungen auf Basis von beobachteten Verhaltens- und Umgebungsattributen durchzusetzen.

85 % der Netzwerkadministratoren stimmen der Aussage zu, dass Firewall-Funktionen am besten über die Cloud bereitgestellt werden sollten.[1]

Wir informieren Sie über 7 Warnsignale, an denen Sie erkennen, dass Ihre Legacy- bzw. Next-Gen-Firewalls nicht Zero-Trust-tauglich sind.

E-Book herunterladen

1. Quelle: Zscaler, Umfrage zu Netzwerk-Firewalls

Experience your world, secured.™

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
USA
+1 408 533 0288
www.zscaler.de