Gigamon®

STUDIE

Die IT- und Sicherheitsland-schaft 2020 und darüber hinaus und die Rolle von Zero Trust

Executive Summary

Die Gigamon Studie zum Thema Zero Trust entstand aus der These, dass sich die Wahrnehmung rund um Zero Trust verändert und der Ansatz auf immer größeres Interesse stößt. Zero Trust hatte aufgrund seiner Botschaft „nie vertrauen, immer verifizieren" bislang eine eher negative Konnotation. Die Vorstellung war, dass dadurch insbesondere die Mitarbeiterproduktivität sinken würde. Die vorliegende Studie widerlegt das, denn **87 %** der befragten IT- und Sicherheitsexperten berichteten von einer verbesserten Produktivität nach Einführung von Zero Trust.

Darüber hinaus hat die aktuelle wirtschaftliche Lage Arbeitsprozesse erheblich verändert und neue Herausforderungen und zusätzliche Sicherheitsbedrohungen mit sich gebracht – wie **84 %** der Entscheider bestätigten. Zero Trust wird heute als strategischer Ansatz angesehen, um diese zusätzlichen Belastungen aufzufangen.

97 % der Teilnehmer gaben an, dass Zero Trust dem Unternehmen geholfen habe oder helfen könnte, die aktuelle globale Situation besser zu meistern.

Im Rahmen der Studie wurden die Antworten von **500** Entscheidern aus IT- und Sicherheitsabteilungen aus Deutschland, Großbritannien und Frankreich ausgewertet. Die Ergebnisse untermauerten die Hypothese, dass Zero Trust positive Wirkung auf Unternehmen entfaltet. Immer mehr Unternehmen beschäftigen sich mit dem Konzept und beginnen, diese Architektur einzuführen. Damit steigt auch die generelle Bekanntheit des Zero-Trust-Ansatzes.

89 % der Befragten gaben an, sich schon intensiv damit auseinandergesetzt zu haben.

Insgesamt bestätigten **76 %** der Teilnehmer, die bereits mit dem Modell vertraut waren, dass sie Zero Trust bereits einsetzen oder dies unmittelbar planen. Mit der zunehmenden Umsetzung werden auch die Vorteile deutlich. Die Anwender von Zero Trust sind Beleg dafür, dass Zero Trust ein Wettbewerbsvorteil für Unternehmen ist und kein notwendiges Übel.

Hauptgründe für die Einführung einer Zero-Trust-Architektur

54% Netzwerksicherheit erhöhen und Risiken minimieren

51% Datenschutz erhöhen und das Management der Daten vereinfachen

49% Risiken einer Systemkompromittierung durch eigene Mitarbeiter minimieren

Der Hauptgrund für die Einführung einer Zero-Trust-Architektur ist höhere Sicherheit – **54 %** der Befragten, die Zero Trust eingeführt haben oder dies planen, wollen damit die Netzwerksicherheit erhöhen und Risiken minimieren. Vor dem Hintergrund eines sich stetig weiterentwickelnden Netzwerks geht Zero Trust davon aus, dass kein Nutzer oder Endgerät sicher ist, nur weil vorliegende Anmeldedaten genutzt werden. Stattdessen wird das Verhalten der Assets genau untersucht und nur auf Basis dieser Informationen Zugriff auf das Netzwerk und die Ressourcen gewährt. Datenschutz und eine einfachere Datenverwaltung waren mit **51 %** der zweite wichtige Grund, um Zero Trust einzuführen. Man kann nichts überwachen was man nicht sieht. Unternehmen brauchen daher volle Transparenz über alles, was in ihrem Netzwerk passiert, um Zero Trust einzuführen. **59 %** der Befragten gaben an, Zero Trust einzuführen, um das Risiko zu minimieren, dass das System durch eigene Mitarbeiter kompromittiert wird.

In dieser „neuen Normalität" kann Zero Trust seinen Wert unter Beweis stellen, während Unternehmen ihre Arbeitsweisen und -prozesse an die veränderte Landschaft anpassen. Cyberkriminelle versuchen, flexibles Arbeiten auszunutzen, bei dem Mitarbeiter das Unternehmensnetzwerk auch von zu Hause aus schützen müssen.

Interessanterweise waren die Unternehmenskultur sowie das Verhalten der Mitarbeiter sowohl Grund als auch Hindernis für die Einführung von Zero Trust. Schatten-IT und Mitarbeiterschulungen wurden als wichtigste Herausforderungen von den Befragten genannt und zeigen, dass Unternehmen Zero Trust einführen, um die Bedrohung durch Insider zu minimieren.

Auf der anderen Seite gaben **65 %** der Befragten, die Zero Trust nicht eingeführt haben, eine nicht passende Unternehmenskultur als Hauptgrund für diese Entscheidung an – und die Unterstützung durch die Mitarbeiter wurde als wichtigste Voraussetzung für die Einführung genannt.

In dieser herausfordernden Zeit müssen sich Unternehmen weiter verändern, um Sicherheit und Wettbewerbsfähigkeit aufrechtzuerhalten. Mit Zero Trust können IT- und Sicherheitsteams gewährleisten, dass ihre Organisation sicher bleibt – und zwar ohne die Produktivität oder die Benutzererfahrung zu beeinträchtigen.

Weitergehende Informationen erhalten Sie im vollständigen Studienbericht.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 www.gigamon.com

EMEA Headquarters
100 Brook Drive, Green Park, Reading, RG2 6UJ United Kingdom
+44 (0)118 304 0300 emea-info@gigamon.com

09.20_04