ESG Kurzfassung

Zero Trust Impact Report: Wichtige Erkenntnisse für Deutschland

Datum: Juni 2022 **Autor:** John Grady, Senior Analyst; Adam DeMattia, Custom Research Director

Eine wachsende Angriffsfläche fördert das Interesse an Zero Trust

Die durch die digitale Transformation entstandene Hyperkonnektivität zwischen Benutzern, Anwendungen, Daten und Dingen vergrößert die Angriffsfläche enorm und erhöht das Risiko. Angreifer versuchen, diese Trends auszunutzen, und verwenden eine Vielzahl von Methoden, um Ziele zu kompromittieren, was oft zu erheblichen Störungen des Geschäftsbetriebs führt. Daher haben zahlreiche Unternehmen begonnen, Zero-Trust-Architekturen zu implementieren, um ihre Cybersicherheitsprogramme zu modernisieren und die Auswirkungen dieser Angriffe zu begrenzen. Um einen tieferen Einblick in den Stand der Dinge in Bezug auf Zero Trust zu erhalten und zu erfahren, wie sich die Segmentierung konkret in ihre Strategie einfügt, beauftragte Illumio die Enterprise Strategy Group (ESG) mit der Durchführung einer weltweiten Umfrage unter 1.000 Unternehmen in Nordamerika, Europa, Asien-Pazifik und Japan. Zu den wichtigsten Erkenntnissen unter den deutschen Umfrageteilnehmern gehören:

- Lediglich 21 % der deutschen Befragten sind der Meinung, dass ihr Unternehmen auf einen Sicherheitsverletzung vorbereitet ist. Dies könnte auf frühere Erfahrungen zurückzuführen sein. 88 % der Befragten berichteten über negative Auswirkungen wie etwa die Beeinträchtigung des Ansehens der Marke oder des Aktienwerts (34 %), Probleme mit der Einhaltung von Vorschriften (32 %) oder den Verlust sensibler Daten (27 %) infolge eines Angriffs.

- Mehr als drei Viertel (79 %) der deutschen Unternehmen, deren Daten und Systeme durch einen Ransomware-Angriff in Geiselhaft genommen wurden, waren gezwungen, das Lösegeld entweder direkt oder über einen Cyber-Versicherungsanbieter zu bezahlen. Das durchschnittliche Lösegeld, das in Deutschland bezahlt wurde, betrug mehr als 676.000 €.

- Unternehmen in Deutschland räumen Zero Trust eine hohe Priorität ein. 86 % der Befragten gaben an, dass Zero Trust zu den Top-3-Prioritäten im Bereich der Cybersicherheit gehört, und stellen durchschnittlich 45 % ihres gesamten Sicherheitsbudgets für Zero Trust-Initiativen bereit.

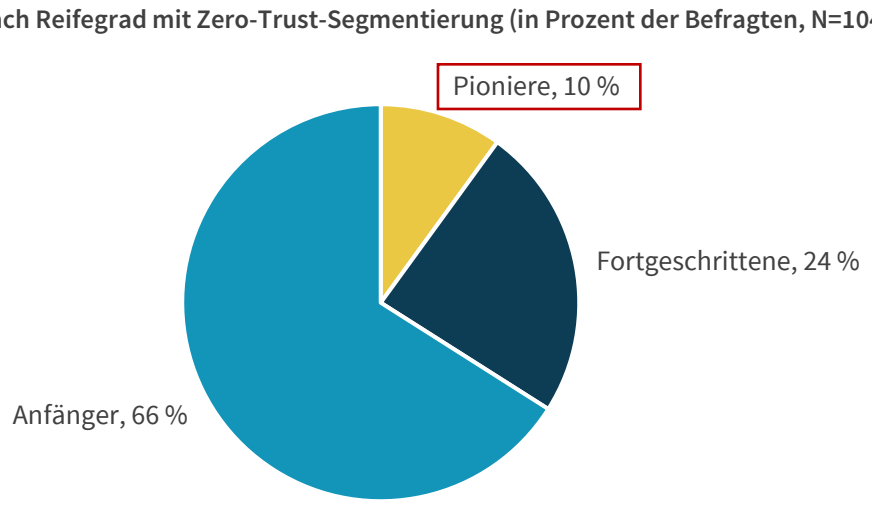
- Trotz der weiten Verbreitung von Zero Trust und der damit einhergehenden Wahrscheinlichkeit, angegriffen zu werden, gehen 61 % der deutschen Unternehmen nicht davon aus, dass sie Opfer einer Sicherheitsverletzung werden. Damit liegen sie deutlich hinter ihren Kollegen aus Großbritannien (46 %) und den USA (39 %) und weisen auf eine eklatante Diskrepanz zwischen dem hin, was deutsche Unternehmen vorgeben zu tun und wie sie tatsächlich vorgehen.

Reifegrad der Zero-Trust-Segmentierung

Im Rahmen der Studie bewertete die ESG, an welchem Punkt sich die Befragten in Bezug auf ihre Fortschritte bei der Zero-Trust-Segmentierung befinden. Zero-Trust-Segmentierung ist ein moderner Ansatz, um die Ausbreitung von Sicherheitsverletzungen in der hybriden IT-Umgebung, von der Cloud bis zum Rechenzentrum, zu verhindern. Dazu gehört ein umfassender Einblick in alle Anwendungstypen, Standorte und Endpunkte, die schnelle und effektive Eindämmung von Angriffen, die richtige Segmentierung verschiedener Teile der Umgebung (z. B. IT von OT und Entwicklung von Produktion). Außerdem müssen diese Fähigkeiten auf die gesamte Umgebung ausgeweitet werden, um Ressourcen mit hoher Priorität zu isolieren und Mikrosegmentierung auf alle Anwendungen anzuwenden, um jegliche Seitwärtsbewegungen in der Umgebung zu verhindern.

Die Teilnehmer der Studie wurden anhand ihrer Antworten auf fünf Kernfragen in drei Kategorien eingeteilt. Diese Fragen betrafen ihre Segmentierungstechnologie und -praktiken in Bezug auf die Integration mit SIEM- und SOAR-Lösungen, die Trennung von Umgebungen, die Fähigkeit, Infizierungen einzudämmen, sowie die konsistente Transparenz und Durchsetzung in der gesamten Umgebung. Die Teilnehmer der Gruppe Anfänger berichteten über sehr gute Fähigkeiten in 0–2 Bereichen, Fortgeschrittene in 3–4 Bereichen und Pioniere in allen 5 Bereichen. Gerade einmal 10 % der deutschen Unternehmen wurden in die Kategorie der Pioniere aufgenommen. Das bedeutet, dass viele zwar die Bedeutung von Zero Trust erkennen, aber noch einen weiten Weg vor sich haben, wenn es um die Umsetzung der Segmentierung geht, um eine Mentalität der „Vermutung einer Sicherheitsverletzung" zu unterstützen.

Abbildung 1. Reifegrad der Zero-Trust-Segmentierung in Deutschland



Quelle: ESG, eine Abteilung von TechTarget, Inc.

Warum sind solche Gruppierungen wichtig? Unternehmen, die als Pioniere eingestuft wurden, konnten im Vergleich zu ihren Mitbewerbern erhebliche Sicherheits- und Geschäftsvorteile verzeichnen. Unter den Befragten aus aller Welt berichteten die Pioniere der Zero-Trust-Segmentierung:

- Bessere Transparenz. Bei den Pionieren war die Wahrscheinlichkeit, dass sie einen umfassenden Einblick in den Datenverkehr in ihrer gesamten Umgebung hatten, 4,3-mal höher und die Wahrscheinlichkeit, dass sie einen umfassenden Einblick in alle Arten von Anwendungsarchitekturen hatten, fünfmal höher.

- **Geringere jährliche Ausfallkosten.** Bei den Pionieren war die Wahrscheinlichkeit, dass sie einen kritischen Ausfall aufgrund eines Angriffs vermeiden konnten, doppelt so hoch und die mittlere Wiederherstellungszeit (mean time to recover, MTTR) war 68 % kürzer. Durch die Vermeidung von Ausfällen und die schnellere Wiederherstellung, wenn es doch zu Angriffen kommt, konnten diese Unternehmen einen Kostenvorteil in Höhe von 20,1 Millionen Dollar pro Jahr für Ausfallzeiten erzielen.

- **Schnellere digitale Transformation.** Die Pioniere werden im Laufe des nächsten Jahres 14 Produktionsanwendungen in die Cloud verlagern, die sie sonst aufgrund mangelnden Sicherheitsvertrauens nicht nutzen würden, und so durchschnittlich 39 Arbeitsstunden pro Woche einsparen.

- **Vertrauen in die Verhinderung von Cyberkatastrophen.** Pioniere fühlten sich mehr als doppelt so häufig auf den Umgang mit Cyberangriffen vorbereitet und gaben an, jährlich fünf Cyberkatastrophen zu verhindern.

Wenn Sie mehr über den Erfolg der Pioniere der Zero-Trust-Segmentierung erfahren möchten und darüber, was sie tun, um diese Ergebnisse zu erreichen, lesen Sie den vollständigen Bericht.

Die **Enterprise Strategy Group** ist ein integriertes Technologieanalyse-, Forschungs- und Strategieunternehmen, das der globalen IT-Gemeinschaft Marktinformationen, umsetzbare Erkenntnisse und Go-to-Market-Inhaltsdienste bietet.

www.esg-global.com contact@esg-global.com +1 508 482 0188