Whitepaper zum CISA Zero Trust Maturity Model

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

WHITEPAPER

Kurzfassung

In der sich rasant entwickelnden Cybersicherheitslandschaft von heute sehen sich Unternehmen mit einer wachsenden Zahl komplexer Bedrohungen konfrontiert. Herkömmliche perimeterbasierte Sicherheitsmodelle sind bei der Absicherung von Netzwerken zunehmend wirkungslos, da die digitale Transformation voranschreitet und standortunabhängiges Arbeiten zur Norm wird. Die Cybersicherheit muss sich weiterentwickeln, um Daten und Systeme unabhängig vom Standort der User oder Geräte zu schützen.
Als Reaktion auf diese Herausforderungen hat die Cybersecurity and Infrastructure Security Agency (CISA) ein Zero Trust Maturity Model entwickelt, um Unternehmen bei der effektiven Einführung und Umsetzung von Zero-Trust-Prinzipien zu unterstützen.

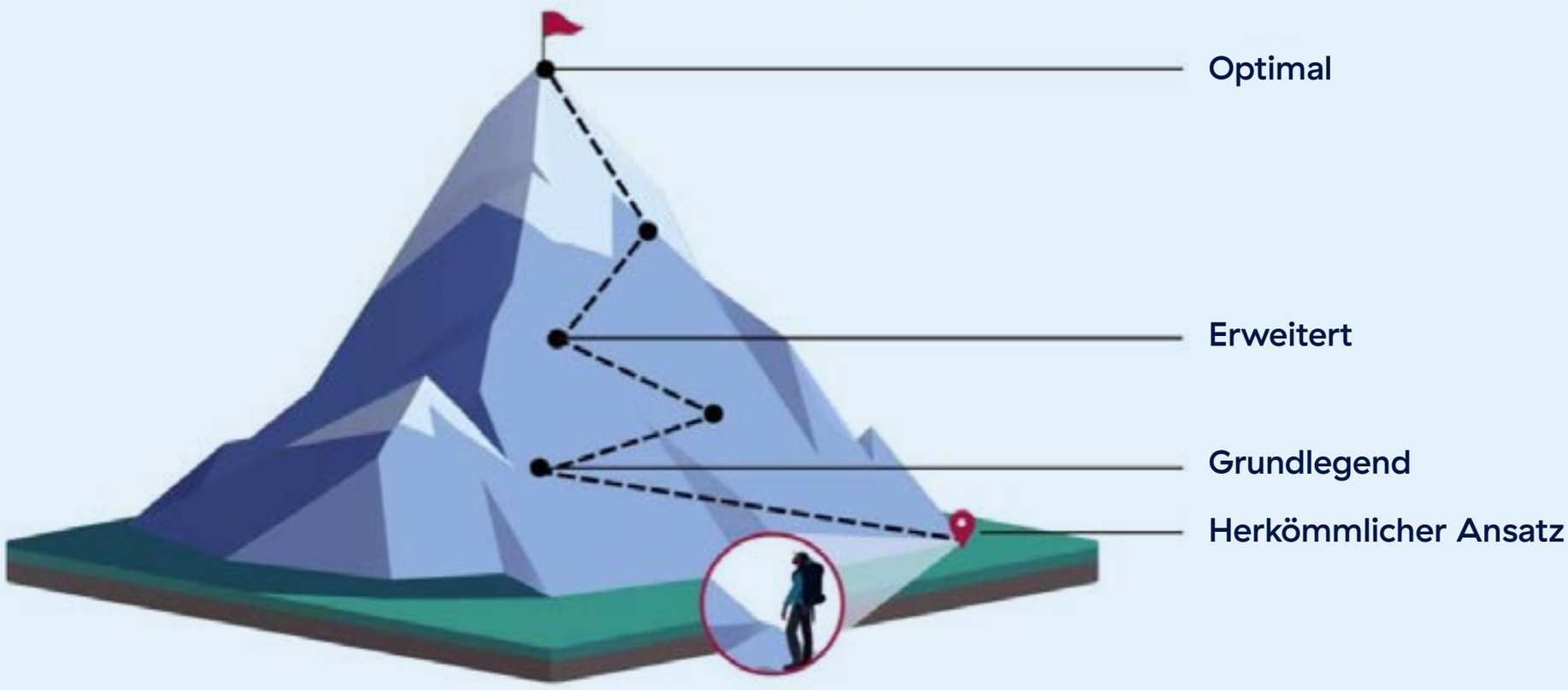
Was ist Zero Trust?

Das Zero-Trust-Sicherheitsmodell geht davon aus, dass Bedrohungen sowohl intern als auch extern auftreten können und daher keinem User oder Gerät standardmäßig vertraut werden sollte. Jede Zugriffsanfrage — egal ob von innerhalb oder außerhalb des Netzwerks — wird streng authentifiziert, autorisiert und kontinuierlich überwacht. Das Zero-Trust-Framework konzentriert sich darauf, die Sicherheit in der gesamten Infrastruktur eines Unternehmens zu gewährleisten, wobei der Schwerpunkt auf Identitäts- und Zugriffsmanagement sowie Echtzeit-Monitoring liegt.

Was ist das CISA Zero Trust Maturity Model?

Das CISA Zero Trust Maturity Model bietet Unternehmen ein Framework für die schrittweise Einführung und Weiterentwicklung von Zero-Trust-Prinzipien. Dieses Modell bietet einen stufenweisen Ansatz für die Implementierung von Zero Trust in einem Unternehmen, von der ersten Sensibilisierung und Planung bis hin zu ausgereiften, integrierten Sicherheitsabläufen.
Es stellt eine strukturierte Methode bereit, um zu ermitteln, wo ein Unternehmen auf seinem Weg zu Zero Trust steht und welche Schritte es als Nächstes unternehmen sollte, um die Sicherheit zu verbessern.

Der Weg zu ausgereiftem Zero Trust



Quelle: CISA

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

Das CISA-Modell unterteilt Zero Trust in mehrere Schlüsselbereiche, darunter Identitäts- und Zugriffsmanagement, Gerätesicherheit, Netzwerksicherheit, Datensicherheit, Anwendungssicherheit sowie Transparenz und Analyse. Das Reifegradmodell unterstützt Unternehmen dabei, ihre aktuellen Aktivitäten in jedem dieser Bereiche zu bewerten und einen klaren Weg zur Stärkung ihres Sicherheitsstatus zu definieren. Unternehmen werden anhand von vier Reifegraden (herkömmlich, grundlegend, fortgeschritten und optimal) bewertet. Mit jeder Stufe steigen die Anforderungen an den Schutz — ebenso wie der Aufwand und der daraus resultierende Nutzen.

Das Zero Trust Maturity Model von CISA wird zunehmend als globaler Maßstab für die Zero-Trust-Implementierung genutzt. Mehrere Regierungen weltweit, unter anderem in Großbritannien und Australien, orientieren ihre Cybersicherheitsstrategien am Reifegradmodell und setzen dabei auf dessen klar strukturierten Weg zur Stärkung von Zero Trust. Darüber hinaus hat die Cloud Security Alliance ihr Zero Trust Advancement Center ebenfalls an das Reifegradmodell angepasst und damit dessen Funktion als gemeinsames Framework für Unternehmen weltweit weiter gefestigt. Mit der zunehmenden Verbreitung von Zero Trust bietet das Reifegradmodell eine gemeinsame Sprache und Roadmap für die Reifegradentwicklung, die sowohl öffentlichen als auch privaten Einrichtungen dabei hilft, ihre Fortschritte zu bewerten und ihre Sicherheitsstrategien zu verfeinern.

DIE ZENTRALEN KOMPONENTEN DES MODELLS

1. **Identitäts- und Zugriffsmanagement:** Beinhaltet starke Authentifizierungsmechanismen wie die Multifaktorauthentifizierung (MFA), um die Identität von Usern zu überprüfen, bevor ihnen Zugriff gewährt wird.

2. **Gerätesicherheit:** Stellt sicher, dass Geräte sicher sind, verwaltet werden und den Sicherheitsrichtlinien entsprechen, bevor auf Unternehmensressourcen zugegriffen wird.

3. **Netzwerksicherheit:** Implementiert Segmentierung und Monitoring, um laterale Bewegungen einzuschränken und verdächtige Aktivitäten innerhalb des Netzwerks zu erkennen.

4. **Datensicherheit:** Schützt vertrauliche Daten durch Verschlüsselung, strenge Zugriffskontrollen und Überwachung der Datennutzung.

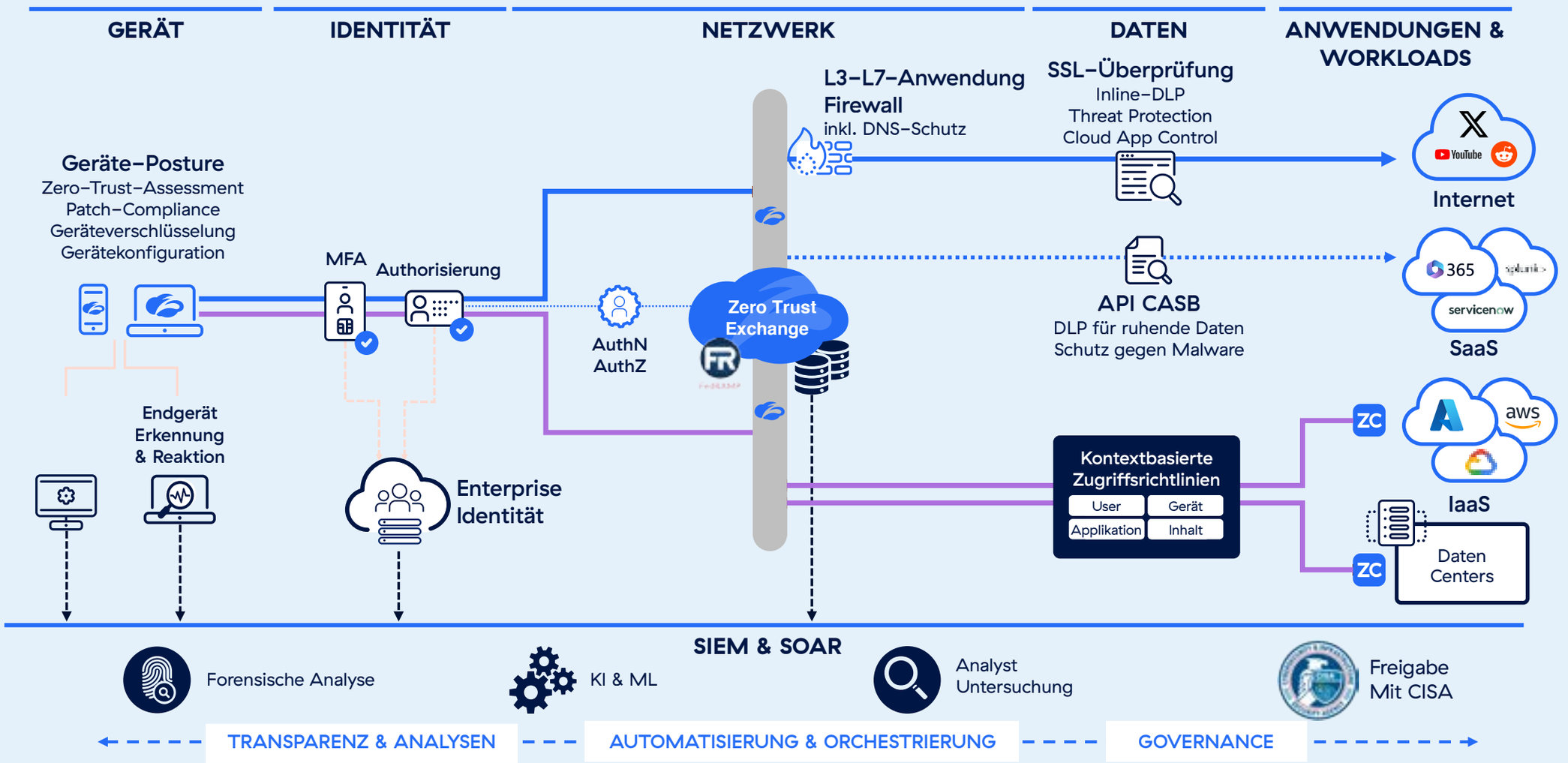
5. **Anwendungssicherheit:** Gewährleistet die Sicherheit von Anwendungen durch die Implementierung sicherer Entwicklungsmethoden, kontinuierlicher Überwachung und Schwachstellenmanagement.

6. **Transparenz und Analysen:** Verbessert den Überblick über die aktuelle Situation durch kontinuierliche Überwachung des gesamten Traffics und aller Ereignisse, Identifizierung anomaler Verhaltensweisen und Bereitstellung von Warnmeldungen in Echtzeit.

7. **Automatisierung und Orchestrierung:** Integriert und automatisiert Systeme, um die Effektivität und Effizienz von Cybersystemen zu verbessern.

8. **Governance:** Legt Richtlinien, Verfahren und Kontrollmechanismen fest, um eine wirksame Umsetzung sicherzustellen.

©2025 Zscaler, Inc. Alle Rechte vorbehalten.



Implementierung des Zero Trust Maturity Model von CISA mit Zscaler

Durch die Implementierung der Zscaler ZTE verbessern Sie Ihren Sicherheitsstatus umgehend, indem Sie von herkömmlicher perimeterbasierter Sicherheit zu einer umfassenden, mehrschichtigen Verteidigungsstrategie wechseln. Durch die kontinuierliche Überprüfung von Usern, Geräten und Daten können Unternehmen das Risiko von Datenpannen, Insider–Bedrohungen und externen Angriffen reduzieren. Dieser Ansatz minimiert die Angriffsfläche und verhindert die laterale Ausbreitung von Bedrohungen. Mit Zscaler können Unternehmen außerdem ihre Strategie bezüglich des Zero Trust Maturity Model vorantreiben, denn Zscaler bietet robuste Produkte und Funktionen, die wichtige Bereiche wie Identitäts– und Zugriffsmanagement, Gerätesicherheit, Netzwerksicherheit, Datensicherheit, Anwendungssicherheit sowie Transparenz und Analyse unterstützen.

IDENTITÄT

- **Zugriff mit minimaler Rechtevergabe:** Zscaler minimiert Konten mit weitreichenden Berechtigungen, indem granulare, rollenbasierte Zugriffskontrollen und kontextbezogene Richtlinien (z. B. User–Standort, Gerätezustand) durchgesetzt werden.

- **Single Sign–On (SSO) und Multifaktorauthentifizierung (MFA):** Zero–Trust–Richtlinien werden durch die Integration von SSO/MFA unterstützt, wodurch eine starke Authentifizierung gewährleistet und das Risiko einer Kompromittierung von Anmeldedaten verringert wird.

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

- **Kontinuierliches User-Monitoring:** ZTE stellt sicher, dass User kontinuierlich authentifiziert werden und ihr Verhalten überwacht wird, um Risiken zu minimieren.

- **Integration mit Identitätsanbietern (IdPs):** Zscaler lässt sich nahtlos mit führenden Identitätsanbietern wie Okta, Microsoft Azure AD und Ping Identity integrieren, um strenge Richtlinien für die User-Authentifizierung und -autorisierung durchzusetzen.

GERÄTE

- **Prüfungen des Gerätestatus:** Zscaler nutzt Integrationen mit EDR-Tools (Endpoint Detection and Response), um Sicherheitsüberprüfungen durchzuführen und sicherzustellen, dass nur sichere, verwaltete Geräte auf sensible Ressourcen zugreifen können.

- **Agentbasierte Durchsetzung:** Der schlanke Software-Agent Zscaler Client Connector (ZCC) sorgt dafür, dass der gesamte User-Traffic über die Zscaler-Security-Cloud geleitet wird, wodurch Transparenz und eine konsistente Durchsetzung von Sicherheitsrichtlinien gewährleistet werden.

- **Zero Trust für IoT- und nicht verwaltete Geräte:** Die Lösungen von Zscaler umfassen Funktionen zur Kontrolle des Zugriffs durch nicht verwaltete Geräte — einschließlich IoT — mithilfe von Verhaltensrichtlinien und granularen Zugriffskontrollen.

NETZWERK

- **Zero Trust Network Access (ZTNA):** Zscaler Private Access (ZPA) ersetzt herkömmliche VPNs durch ZTNA. User erhalten Zugriff mit minimaler Rechtevergabe auf bestimmte Anwendungen, nicht auf das gesamte Netzwerk.

- **Secure Access Service Edge (SASE):** Zscaler erfüllt die Anforderungen der SASE-Architektur, indem skalierbare Sicherheitsservices wie Secure Web Gateways (SWG) und Cloud-Firewall in verteilten Umgebungen bereitgestellt werden.

- **Mikrosegmentierung:** Zscaler stellt sicher, dass User und Workloads auf Anwendungsebene segmentiert werden, wodurch laterale Bewegungen im Falle einer Sicherheitsverstöße minimiert werden.

- **Lückenlose Verschlüsselungsüberwachung:** Zscaler überprüft verschlüsselten Internet-Traffic mittels SSL/TLS-Interception, ohne die Performance oder den Datenschutz zu beeinträchtigen.

ANWENDUNGEN UND WORKLOADS

- **Anwendungssegmentierung:** Zscaler ZPA bietet eine anwendungsbasierte Segmentierung anstelle der herkömmlichen Netzwerksegmentierung und stellt so direkte, sichere Verbindungen zwischen Usern und Anwendungen bereit.

- **Workload-Sicherheit:** Zscaler Workload Segmentation (ZWS) sichert die Kommunikation zwischen Workloads in öffentlichen und privaten Cloud-Umgebungen durch „identitätsbasierte Mikrosegmentierung” ab.

- **Kontinuierliches Monitoring:** Monitoring auf Anwendungsebene überprüft User-Aktivitäten und Zugriffsmuster auf Anomalien und stellt sicher, dass kompromittierte Konten keine weiteren Berechtigungen erhalten können.

- **SaaS-Sicherheit:** Der Cloud Access Security Broker (CASB) von Zscaler kontrolliert den Zugriff auf genehmigte und nicht genehmigte SaaS-Anwendungen und verhindert so den unbefugten Zugriff auf Daten und deren Nutzung.

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

DATEN

- **Data Loss Prevention (DLP):** Die cloudbasierte DLP-Lösung von Zscaler schützt sensible Daten in E-Mails, im Internet, in SaaS- und privaten Anwendungen. Sie erkennt und verhindert die Weitergabe von geistigem Eigentum und personenbezogenen Daten.

- **Cloud Security Posture Management (CSPM):** Zscaler bietet Einblicke und Abhilfemaßnahmen bei Fehlkonfigurationen in Cloud-Datenspeicher-systemen und reduziert so Risiken.

- **Verschlüsselungskontrolle:** Zscaler setzt strenge Verschlüsselungsprotokolle sowohl für Daten während der Übertragung als auch für ruhende Daten durch und stellt so sicher, dass sensible Informationen durchgehend geschützt sind.

- **Erkennung von Schatten-IT:** Zscaler CASB erkennt und beschränkt die Nutzung nicht genehmigter oder riskanter Anwendungen/Services und schützt Daten so vor versehentlichem Verlust oder böswilligem Missbrauch.

GOVERNANCE, TRANSPARENZ UND ANALYSEN, AUTOMATISIERUNG UND ORCHESTRIERUNG

- **Zentralisiertes Sicherheitsmanagement:** Die Zscaler Zero Trust Exchange bietet eine zentrale Übersicht über Traffic, Richtlinien und Sicherheitsvorfälle.

- **Integrierte Sicherheitsanalysen:** Zscaler liefert durch erweiterte Dashboards und Protokolle Echtzeit-Transparenz über User- und Anwendungsaktivitäten und lässt sich für eine optimierte Reaktion auf Vorfälle in SIEM/SOAR-Plattformen integrieren.

- **Bedrohungsinformationen:** Zscaler nutzt globale Bedrohungsinformationen und Verhaltensanalysen, um Bedrohungen im gesamten Zero-Trust-System proaktiv zu erkennen und darauf zu reagieren.

- **Durchsetzung von Richtlinien:** Zscaler automatisiert Richtlinienänderungen und Compliance-Prüfungen und gewährleistet so eine konsistente Governance für User, Anwendungen und Daten.

Der Ansatz von Zscaler zur Implementierung von Zero Trust und das Zero Trust Maturity Model (ZTMM) von CISA sind sehr ähnlich und stimmen in mehreren wichtigen Bereichen überein, nicht nur in Bezug auf die Grundpfeiler von Zero Trust. Die Architektur von Zscaler unterstützt wichtige ZTMM-Funktionen wie die dynamische Durchsetzung von Richtlinien, zentralisierte Transparenz und adaptive risikobasierte Zugriffskontrollen — entscheidende Elemente für die Weiterentwicklung einer Zero-Trust-Strategie. Durch die Nutzung eines Cloud-nativen Inline-Ansatzes unterstützt Zscaler Unternehmen dabei, ihren im CISA-Modell beschriebenen Reifegrad zu verbessern, Angriffsflächen zu reduzieren und gleichzeitig den sicheren Zugriff zu optimieren.

Strategische Roadmap für die Einführung von Zero Trust

Sowohl die Zscaler-Implementierung als auch das Zero Trust Maturity Model von CISA bieten Unternehmen eine strategische Roadmap für die Einführung von Zero-Trust-Prinzipien. Wir unterteilen den Implementierungsprozess in überschaubare Phasen, sodass Unternehmen realistische Ziele und Zeitpläne für jede Phase festlegen können. Diese Roadmap stellt sicher, dass Unternehmen einen strukturierten Ansatz für die Zero-Trust-Implementierung verfolgen und so das Risiko von Lücken oder Fehlentscheidungen verringern.

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

Schrittweise Implementierung

Durch die schrittweise Implementierung können Unternehmen ihren Zero-Trust-Reifegrad im Laufe der Zeit kontinuierlich verbessern. Dieser schrittweise Ansatz erleichtert die Implementierung von Zero Trust, ohne vorhandene Systeme oder Ressourcen zu überlasten. Darüber hinaus können Unternehmen damit den Fortschritt überwachen und ihre Strategien bei Bedarf anpassen. Dadurch kann Zscaler kontinuierlich neue Produkte herausbringen, um den Sicherheitsstatus unserer Kunden zu verbessern, und gleichzeitig kann die CISA in Zukunft die Anforderungen anpassen. Was heute als „optimal“ gilt, kann in Zukunft „fortgeschritten“ sein.

Kein Unternehmen ist dem anderen gleich

Die Cybersicherheitsanforderungen und die Infrastruktur jedes Unternehmens sind einzigartig. Die ZTE-Implementierung von Zscaler und das Zero Trust Maturity Model von CISA sind flexibel genug, um an die spezifischen Ziele, Herausforderungen und Ressourcen eines Unternehmens angepasst zu werden. Unabhängig davon, ob ein Unternehmen Zero Trust bereits vollständig eingeführt hat oder gerade erst damit begonnen hat, bietet das Modell die notwendigen Leitlinien, um das Zero-Trust-Framework an die jeweiligen Anforderungen anzupassen.

Messung von Fortschritt und Erfolg

Das Reifegradmodell umfasst eindeutige Metriken und Bewertungskriterien, anhand derer Unternehmen ihre Fortschritte im Laufe der Zeit verfolgen können. Durch die Messung des Erfolgs anhand vordefinierter Stufen können Unternehmen Verbesserungsmöglichkeiten identifizieren und sicherstellen, dass sie sich in die richtige Richtung bewegen, um eine ausgereifte Zero-Trust-Umgebung zu erreichen.

Fazit

Das Zero Trust Maturity Model 2.0 von CISA bietet Unternehmen ein klares, strukturiertes Framework für die Einführung und Weiterentwicklung von Zero-Trust-Prinzipien. Durch die Implementierung dieses Modells können Unternehmen ihre Cybersicherheit erheblich verbessern, Risiken mindern und die Einhaltung gesetzlicher Vorschriften sicherstellen.

Angesichts der sich ständig weiterentwickelnden Bedrohungslandschaft wird Zero Trust an Bedeutung gewinnen, sodass das CISA-Modell zu einem unverzichtbaren Hilfsmittel für Unternehmen wird, die ihre digitalen Umgebungen vor den heutigen hochentwickelten Bedrohungen schützen möchten. Durch eine strategische, schrittweise Implementierung können Unternehmen Zero Trust in einer Weise einführen, die ihren spezifischen Anforderungen und Möglichkeiten entspricht, und so den langfristigen Erfolg ihrer Cybersicherheitsmaßnahmen sicherstellen.

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Die Zscaler Zero Trust Exchange™ schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlusten. Als weltweit größte Inline-Cloud-Sicherheitsplattform wird die SASE-basierte Zero Trust Exchange™ in über 150 Rechenzentren auf der ganzen Welt bereitgestellt. Weitere Informationen erhalten Sie auf **zscaler.com/de**. Gerne können Sie uns auch auf X folgen **@zscaler**.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™ sowie weitere unter **zscaler.com/de/legal/trademarks** aufgeführte Marken sind entweder (i) eingetragene Handelsmarken bzw. Dienstleistungsmarken oder (ii) Handelsmarken bzw. Dienstleistungsmarken von Zscaler, Inc. in den USA und/oder anderen Ländern. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.

+1 408 533 0288 Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA zscaler.com/de

zscaler™

Zero Trust Everywhere