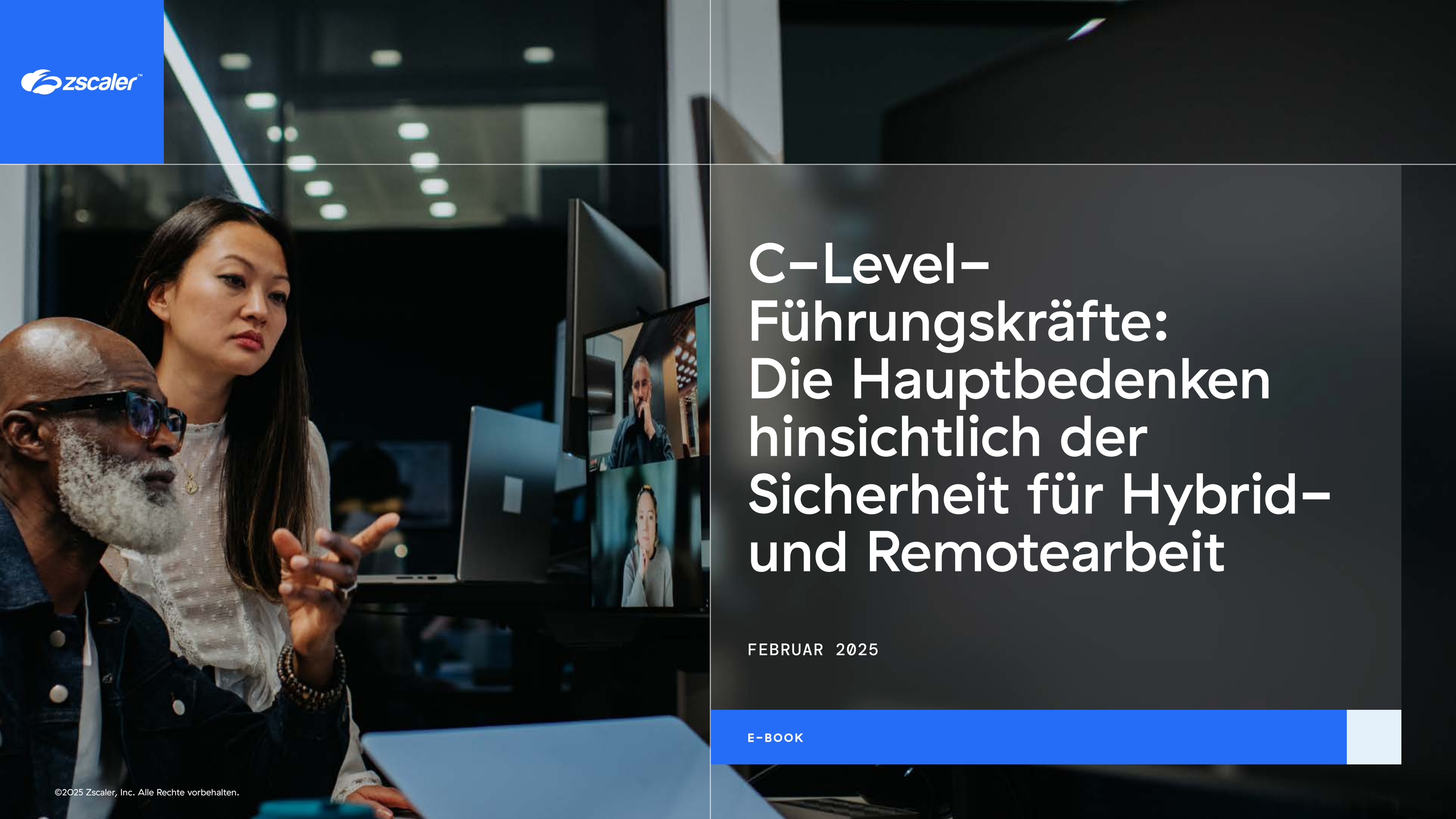


C-Level-Führungskräfte: Die Hauptbedenken hinsichtlich der Sicherheit für Hybrid- und Remotearbeit

FEBRUAR 2025

E-BOOK

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

Inhalt



Einführung 3

Übersicht über kritische Netzwerk- und Remote-Sicherheitsprobleme 3

Die Entwicklung der digitalen Sicherheitslandschaft 4

Neueste Trends in den Bereichen digitale Sicherheit und Remotearbeit 4

Die größten Sicherheitsbedenken von Führungskräften 5

Schutz sensibler Daten 5

Umgang mit Insider-Bedrohungen 5

Sicherstellung der Einhaltung von Vorschriften 5

Strategien für Führungskräfte zur Beseitigung von Sicherheitsbedenken 6

Implementierung eines robusten Identitäts- und Zugriffsmanagements 6

Verbesserung der Bedrohungserkennungs- und Abwehrfunktionen 6

Regelmäßige Sicherheitsschulungen und Sensibilisierungsprogramme 6

Nutzung von Zscaler-Lösungen für Sicherheit im Büro, im Rahmen hybrider Arbeitsmodelle und an Remote-Standorten 7

Zscaler Internet Access (ZIA) 7

Zscaler Private Access (ZPA) 8

Erweiterte Sicherheitsfunktionen 8

So schützen Sie Ihr Team mit Zscaler 9

Umstieg von Firewalls auf Zero Trust 9

Ein umfassender Zero-Trust-Ansatz 9

Quellen 9

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

Einführung

Cyberangriffe nahmen im zweiten Quartal 2024 weltweit um stolze 30 % im Vergleich zum Vorjahr zu[1]. Die zunehmende Verbreitung von Remotearbeit hat die Angriffsfläche vergrößert und Unternehmen für eine Vielzahl von Bedrohungen anfällig gemacht. Laut dem ThreatLabz-Report zu verschlüsselten Angriffen von Zscaler blockierte die Zscaler Cloud 32,1 Milliarden Angriffe, die in TLS/SSL-Traffic eingebettet waren. Dabei machten verschlüsselte Bedrohungen 87,2 % aller blockierten Angriffe aus — ein Anstieg von 10,3 % im Vergleich zum Vorjahr.[2] Diese Daten verdeutlichen, dass Bedrohungsakteure zunehmend auf Verschlüsselung setzen, um ihre bösartigen Aktivitäten zu verbergen.

Veraltete Technologien wie Firewalls und virtuelle private Netzwerke (VPNs) reichen nicht mehr aus, um Unternehmensdaten, -anwendungen und -netzwerke zu schützen, was Entscheidungsträgern und Führungskräften im Hinblick auf die Absicherung von Remotearbeitsumgebungen zahlreiche Herausforderungen beschert. Führungskräfte stehen unter ständigem Druck, das Risiko von Verstößen zu minimieren, die Einhaltung von Vorschriften und Branchenstandards sicherzustellen und den Diebstahl wertvoller Daten wie geistigen Eigentums oder Geschäftsgeheimnisse zu verhindern.

Die gute Nachricht: Cloudbasierte Zero-Trust-Lösungen wurden eigens zum Schutz der Netzwerke von Unternehmen mit Remote- und Hybrid-Belegschaften konzipiert. Mit der richtigen Technologie können Führungskräfte diese Hauptbedenken ausräumen.

Übersicht über kritische Netzwerk- und Remote-Sicherheitsprobleme

Remotearbeit kann die Kontrolle von Unternehmen über Daten und die Integrität ihrer Sicherheitsarchitektur schwächen. Mitarbeiter können nicht verwaltete Geräte verwenden, auf denen möglicherweise keine Sicherheitssoftware installiert ist oder die nicht aktiv überwacht werden, um auf Unternehmensressourcen, einschließlich kritischer Anwendungen, zuzugreifen.

Darüber hinaus haben Sicherheitsexperten keinen vollständigen Überblick darüber, wie Remote-Mitarbeiter mit vertraulichen Daten umgehen und ob sie diese nach der Verwendung löschen. Mitarbeiter speichern möglicherweise Daten auf ihren privaten Geräten und sind dadurch anfällig für Ransomware-Angriffe, Datenpannen und andere Bedrohungen.

Durch die Umstellung auf cloudbasierte Anwendungen wird die Angriffsfläche noch weiter vergrößert und die Sicherheit Ihrer digitalen Infrastruktur beeinträchtigt.



©2025 Zscaler, Inc. Alle Rechte vorbehalten.



Die Entwicklung der digitalen Sicherheitslandschaft

Vor der Pandemie reichten Firewalls und VPNs möglicherweise aus, um die Netzwerke und vertraulichen Daten eines Unternehmens zu schützen. Durch Remote- und Hybridarbeit ist es jedoch notwendig geworden, die Methoden, mit denen Unternehmen ihre digitalen Umgebungen schützen, vollständig zu überarbeiten.

Neueste Trends in den Bereichen digitale Sicherheit und Remotearbeit

Remote-Mitarbeiter benötigen unabhängig von ihrem Standort zwangsläufig Unternehmensressourcen, um ihre Arbeit zu erledigen. Viele Unternehmen haben daher cloudbasierte Software-as-a-Service-Anwendungen (SaaS) eingeführt, um die Remotearbeit zu unterstützen und die Produktivität zu steigern. Die Bereitstellung von SaaS in einem verteilten Netzwerk von Mitarbeitern führt zu einer größeren Angriffsfläche und erhöht das Risiko von unbefugtem Zugriff und Sicherheitsverletzungen.

Cyberkriminelle haben auch raffiniertere Taktiken entwickelt — darunter Credential Stuffing und Zero-Day-Angriffe — und machen es der Führungsetage damit noch schwerer, die Cybersicherheit zu gewährleisten. Tatsächlich sind die Vereinigten Staaten mit 49,95 % aller Angriffe nach wie vor das Hauptziel von Ransomware, gefolgt vom Vereinigten Königreich, Deutschland, Kanada und Frankreich.[3] Diese Angriffe schaden nicht nur dem Ruf Ihres Unternehmens und dem Vertrauen Ihrer Kunden, sondern setzen Ihr Unternehmen auch dem Risiko aus, gegen Datenschutz- und Sicherheitsvorschriften zu verstoßen — ganz zu schweigen von finanziellen Risiken.

Angesichts dieser Trends ergreifen Führungskräfte und Sicherheitsverantwortliche neue Sicherheitsmaßnahmen, beispielsweise:

- **Zero-Trust-Architektur**, die nach dem Prinzip „Niemals vertrauen, immer überprüfen“ funktioniert. Alle User und Geräte, einschließlich BYOD (Bring Your Own Device), müssen überprüft werden.
- **Bedrohungserkennung auf Basis von künstlicher Intelligenz (KI) und maschinellem Lernen (ML)**, die dabei hilft, komplexe Cyberangriffe proaktiv zu identifizieren und abzuwehren.
- **Anwendungssegmentierung**, die eine laterale Ausbreitung von Bedrohungen verhindert.
- **Endgerätesicherheit**, die sich auf den Schutz der von Remote-Mitarbeitern verwendeten Geräte konzentriert. KI-gestützte Lösungen können Bedrohungen erkennen und blockieren, bevor sie sich auf Endgeräte auswirken, und so einen besseren Schutz für verteilte Belegschaften gewährleisten.

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

Die größten Sicherheitsbedenken von Führungskräften

Angesichts der zunehmenden Verbreitung von Remote- und Hybridarbeit und der wachsenden Abhängigkeit von cloudbasierten Lösungen müssen Führungskräfte und CISOs Sicherheitskonzepte entwickeln, die über perimeterbasierte Sicherheit hinausgehen.

Schutz sensibler Daten

Wenn Mitarbeiter über ungeschützte Netzwerke auf Geschäftsdaten zugreifen und diese auf privaten Geräten speichern, erhöht sich das Risiko eines unbefugten Zugriffs und einer unsachgemäßen Handhabung der Daten. Der Schutz vertraulicher Daten in Remotearbeitsumgebungen umfasst:

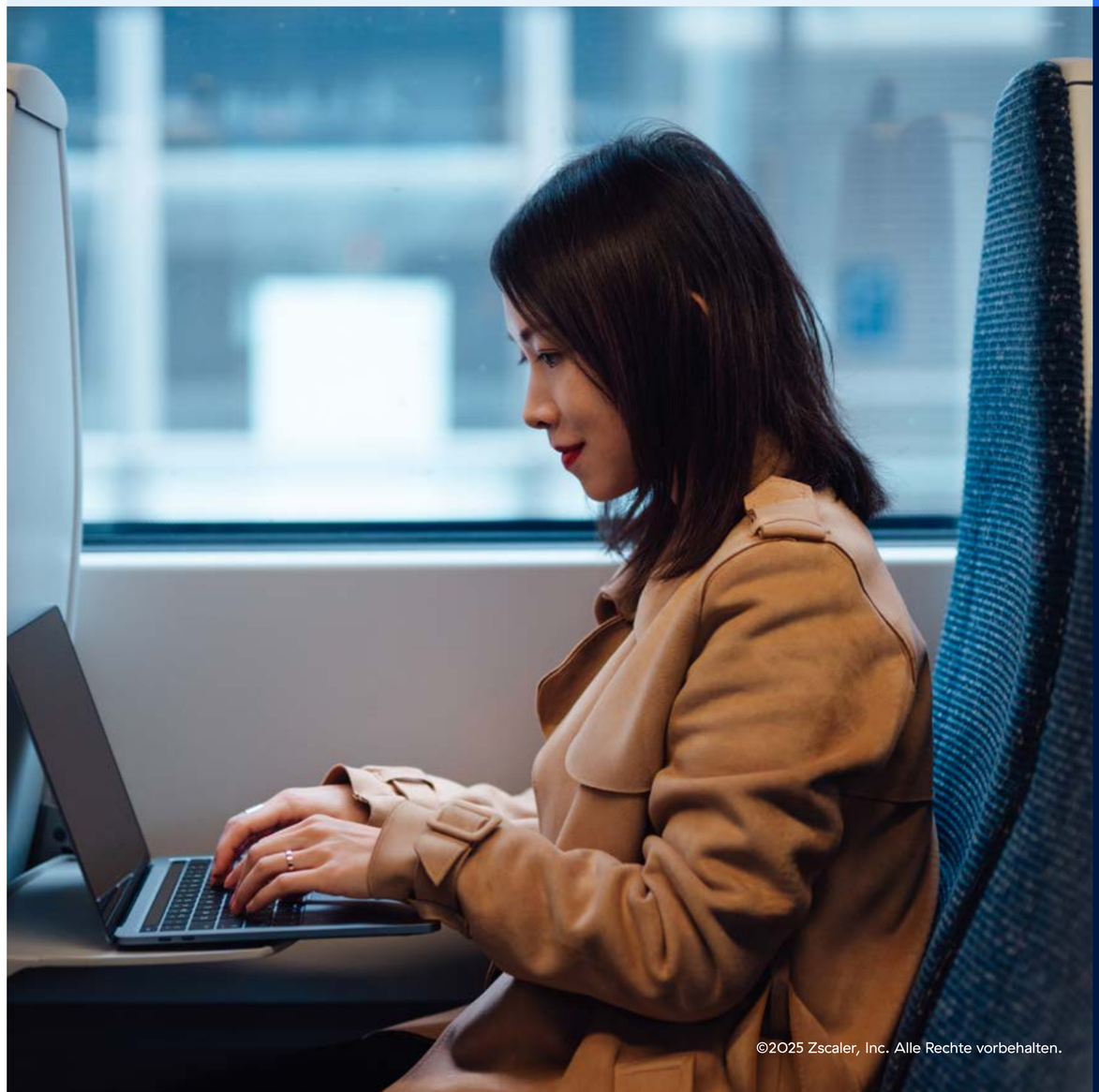
- **End-to-End-Verschlüsselung** zum Schutz ruhender Daten und solcher während der Übertragung, insbesondere bei Verwendung von nicht geschützten Kanälen.
- **Identitäts- und Zugriffsmanagement,** um sicherzustellen, dass nur autorisierte Mitarbeiter auf die erforderlichen Daten zugreifen und diese verwenden können.
- **Methoden zur Verhinderung von Datenverlusten,** um die Gefahr einer versehentlichen Offenlegung oder Datenpanne zu verringern.

Umgang mit Insider-Bedrohungen

Versehentliche und vorsätzliche Handlungen von Mitarbeitern im Büro oder der Remote-Belegschaft können die Systemsicherheit gefährden. Beispielsweise könnte ein neuer Mitarbeiter Opfer von Phishing werden oder ein verärgerter Mitarbeiter könnte vertrauliche Unternehmensdaten missbrauchen. Rollenbasierte Zugriffskontrolle, Richtlinien für den Zugriff mit minimaler Rechtevergabe und Verhaltensanalysen können dazu beitragen, das Risiko von Insider-Bedrohungen zu minimieren.

Sicherstellung der Einhaltung von Vorschriften

Dutzende Regierungsbehörden haben Data Protection-Gesetze zum Schutz der personenbezogenen Daten von Verbrauchern eingeführt, wie z. B. die Datenschutz-Grundverordnung (DSGVO) und den California Consumer Privacy Act (CCPA). Darüber hinaus gibt es branchenspezifische Vorschriften wie den Health Insurance Portability and Accountability Act (HIPAA). Um die Einhaltung dieser gesetzlichen Anforderungen in Remotearbeitsumgebungen sicherzustellen, sind umfassende Governance-Strategien erforderlich.



©2025 Zscaler, Inc. Alle Rechte vorbehalten.

Strategien für Führungskräfte zur Ausräumung von Sicherheitsbedenken

Führungskräfte aus der Unternehmensleitung können verschiedene Strategien anwenden, um die komplexen Sicherheitsherausforderungen der modernen Arbeitswelt zu bewältigen.

Implementierung eines robusten Identitäts- und Zugriffsmanagements

Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) ist eine effektive Methode, um unbefugten Zugriff auf das Netzwerk und die Systeme Ihres Unternehmens zu verhindern. So wird sichergestellt, dass nur die entsprechenden Personen Zugriff auf die Anwendungen und Daten haben, die sie für ihre Arbeit benötigen.

IAM minimiert die Angriffsfläche und reduziert die unnötige Offenlegung sensibler Daten. Im Gegensatz zu perimeterbasierten Sicherheitsmethoden beinhaltet IAM strengere Zugriffskontrollen unabhängig vom Gerät und Standort eines Users. Führungskräfte sollten die Implementierung einer Plattform in Betracht ziehen, die flexible IAM-Lösungen und -Integration unterstützt.

Verbesserung der Bedrohungserkennungs- und Abwehrfunktionen

Da Cyberkriminelle ihre Strategien weiterentwickeln, müssen auch Sicherheitsverantwortliche ihre Methoden anpassen, um Angriffe mit fortschrittlicher Bedrohungserkennung und -abwehr zu verhindern. Implementieren Sie Lösungen, die KI- und ML-Modelle verwenden, um den Traffic im Netzwerk und das Verhalten der User zu überwachen und Abweichungen automatisch zu erkennen.

KI und ML ergänzen auch Zero-Trust-Lösungen, die kompromittierte Geräte und Dateien in Echtzeit isolieren, eine schnelle Reaktion auf Bedrohungen ermöglichen und einen proaktiveren Ansatz für die Cybersicherheit unterstützen. ML-Algorithmen können auch potenzielle Schwachstellen aufzeigen und gleichzeitig neuartige Bedrohungen erkennen und blockieren.

Regelmäßige Sicherheitsschulungen und Sensibilisierungsprogramme

Sicherheitsrichtlinien und -tools sind nur so gut wie die Personen, die sie anwenden. Ein typisches Beispiel: 80 % der CISOs sind der Meinung, dass Fahrlässigkeit von Mitarbeitern und menschliche Risiken bis 2026 zu den größten Problemen im Bereich Cybersicherheit gehören werden.[4] Mitarbeiter in Remotearbeitsumgebungen sind besonders gefährdet, da sie sich nicht immer persönlich an Sicherheitsexperten wenden können, um Hilfe zu erhalten, was zu Verzögerungen und irreversiblen Schäden führen kann.

Um diese Szenarien zu entschärfen, können Unternehmen fortlaufende Schulungen zur Cybersicherheit durchführen, die Mitarbeiter mit bestehenden, neu auftretenden und sich weiterentwickelnden Bedrohungen und Best Practices vertraut machen und sie darauf vorbereiten, sich in einer sich ständig verändernden Bedrohungslandschaft zurechtzufinden. Schulen Sie Ihr Team in Best Practices für Remotearbeit, Passwort-Hygiene und sicherem Umgang mit Daten. Führen Sie außerdem regelmäßig Schulungen durch, um die Mitarbeiter über die unternehmensweiten Cybersicherheitsprotokolle und die leicht zugänglichen Ressourcen zu informieren, die ihnen im Falle einer Kompromittierung ihrer Geräte, Daten und des Zugriffs auf Anwendungen zur Verfügung stehen.

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

Nutzung von Zscaler-Lösungen für Sicherheit im Büro, im Rahmen hybrider Arbeitsmodelle und an Remote-Standorten

Die cloudbasierten Zero-Trust-Lösungen von Zscaler sind darauf ausgelegt, Führungskräfte dabei zu unterstützen, Arbeitsumgebungen heute und in Zukunft abzusichern, wenn sich Bedrohungen weiterentwickeln. Die Zscaler Zero Trust Exchange™ umfasst die folgenden zentralen Lösungen, um sicherzustellen, dass Teams über umfassende Sicherheit verfügen:

Zscaler Internet Access (ZIA)

Zscaler Internet Access ist eine Cloud-native, KI-gestützte Zero-Trust-Lösung, die die digitale Sicherheit für Remote-Mitarbeiter erhöht. Durch den Einsatz einer Zero-Trust-Proxy-Architektur, die den gesamten TLS/SSL-Traffic in großem Maßstab überprüft, und direkten User-to-App-Verbindungen auf der Grundlage von Identität, Kontext und Unternehmensrichtlinien, gewährleistet ZIA einen nahtlosen und sicheren Zugriff auf SaaS- und webbasierte Anwendungen mit den folgenden Schlüsselfunktionen:

- **Cloud-native Secure Web Gateway (SWG):** Bieten Sie ein sicheres, schnelles Web-Erlebnis und erkennen und verhindern Sie gleichzeitig erweiterte Angriffe mit KI-gestützter Analyse und URL-Filterung in Echtzeit.
- **KI/ML-basierte Advanced Threat Prevention:** Stoppen Sie fortschrittliche Bedrohungen wie Botnets, Ransomware, Command-and-Control, riskante Freigabe, bösartige aktive Inhalte, Cross-Site-Scripting, betrügerische Websites und mehr.
- **KI-gestützte URL-Filterung:** Gewährleisten Sie sichere Webanwendungssitzungen für Ihre User, indem Sie raffinierte Bedrohungen wie Phishing und Ransomware abwehren und Richtlinien zur akzeptablen Nutzung anwenden.
- **Cloud Access Security Broker (CASB):** Sichern Sie cloudbasierte Anwendungen ab, schützen Sie Daten, stoppen Sie Bedrohungen und gewährleisten Sie die Einhaltung von Vorschriften in Ihren SaaS- und IaaS-Umgebungen mit integriertem Schutz.
- **Data Loss Prevention (DLP):** Die Übertragung von Daten erfolgt dank vollständiger Inline-Überprüfung, einschließlich Exact Data Match (EDM), Indexed Document Matching (IDM) und maschinellem Lernen, geschützt.
- **Dynamische risikobasierte Richtlinien:** Stoppen Sie laufende Angriffe und machen Sie Ihre Abwehrmechanismen zukunftssicher, indem Sie User-, Geräte-, Anwendungs- und Inhaltsrisiken kontinuierlich analysieren und dynamische Sicherheits- und Zugriffsrichtlinien erstellen.
- **Zero Trust Firewall:** Profitieren Sie von schnellen, sicheren Verbindungen innerhalb und außerhalb des Netzwerks sowie lokalen Internet-Breakouts für den gesamten User-Traffic auf allen Ports und Protokollen, ohne Hard- oder Software-Updates verwalten zu müssen.
- **KI-gestützte Browserisolierung:** Web-Sitzungen werden im Browser des Users nur als Pixel dargestellt, wodurch eine nahezu native Web-Erfahrung ohne das Risiko von Datenverlusten oder Geräteinfektionen ermöglicht wird.
- **DNS-Sicherheit:** Filtern Sie riskante und schädliche Domains und unterbinden Sie mithilfe von Zscaler Firewall die Verwendung von DNS-Tunneling zur Übertragung von schädlichen Payloads und sensiblen Daten.



©2025 Zscaler, Inc. Alle Rechte vorbehalten.

Zscaler Private Access (ZPA)

Zscaler Private Access ist die branchenweit erste KI-gestützte ZTNA-Lösung (Zero Trust Network Access) und ein Cloud-natives Angebot, das allen Usern Zero-Trust-Zugriff bereitstellt. Durch die direkte Verbindung zu privaten Anwendungen bei gleichzeitiger Minimierung der Angriffsfläche unterbindet ZPA laterale Bedrohungsbewegungen mithilfe einer KI-gestützten User-to-App-Segmentierung und schützt vor raffinierten Angriffen durch integrierte Überprüfung des Traffics sowie Anwendungsschutz und Data Protection. Zu den wichtigsten Funktionen von ZPA, die die hybride Belegschaft schützen können, gehören:

- **KI-gestützte Anwendungssegmentierung:** Anwendungen werden automatisch erkannt und KI-erstellte Empfehlungen zu Anwendungssegmenten und Richtlinien werden bereitgestellt, um die Angriffsfläche zu reduzieren und laterale Bewegungen zu verhindern.
- **Workload-to-Workload-Segmentierung:** Sichere Workload-Kommunikation in Hybrid- und Multicloud-Umgebungen wie AWS und Azure.
- **Remotezugriff mit entsprechender Rechtevergabe:** Stellen Sie Remote-Mitarbeitern und externen Usern clientlosen Remotezugriff auf sensible RDP-, SSH- und VNC-Produktionssysteme bereit.
- **Private Service Edge:** Bieten Sie Ihren On-Premise-Usern ZTNA mit direktem Zugriff mit minimaler Rechtevergabe auf private Anwendungen.
- **Business Continuity:** Gewährleisten Sie auch bei Verbindungsausfällen und unvorhergesehenen Zwischenfällen unterbrechungsfreien, richtlinienkonformen Zugriff auf geschäftskritische Anwendungen.
- **Unterstützung von Extranet-Anwendungen:** Ermöglichen Sie Zero-Trust-Zugriff auf Anwendungen von Geschäftspartnern und Anbietern, die in ihren Netzwerken gehostet werden.
- **Digital Experience Monitoring:** Optimieren Sie Ihre digitale Erfahrung, damit User produktiv bleiben, indem Sie Anwendungs-, Netzwerk- und Geräteprobleme schnell erkennen und beheben.

Erweiterte Sicherheitsfunktionen

Zscaler bietet mehrere erweiterte Funktionen, darunter:

- **SSL/TLS-Überprüfung** im großen Maßstab für vollständige Data Protection und Überprüfung von User zu Anwendung.
- **KI-gestützte Inline-Bedrohungserkennung**, um Angriffsvektoren abzuschalten, bevor sie ihr Ziel erreichen.
- **Risk360™** für intuitive Risikovisualisierungen, Faktoren, Details und Berichte, damit Sie sofort Maßnahmen zur Risikominderung ergreifen können.

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

So schützen Sie Ihr Team mit Zscaler

Wenn Sie die Sicherheit Ihrer Remotearbeitsumgebung optimieren möchten, sollten Sie sich von veralteten Cybersicherheitslösungen verabschieden. Die Zero-Trust-Plattform von Zscaler bietet mehrere Möglichkeiten, den Umstieg zu erleichtern.

Umstieg von Firewalls auf Zero Trust

Firewalls und VPNs sind in der modernen Geschäftswelt nicht mehr zeitgemäß, da sie Ihr Unternehmensnetzwerk erweitern und Angreifern mehr Einstiegsmöglichkeiten bieten. Im Gegensatz dazu fungiert die Zscaler Zero Trust Exchange™ als intelligente Schaltstelle, die sowohl eingehenden als auch ausgehenden Traffic zu und von den Geräten der User überprüft, um Bedrohungen zu erkennen und zu blockieren, während sie gleichzeitig Verbindungen zu Anwendungen und Cloud-Ressourcen sicher vermittelt.

Ein umfassender Zero-Trust-Ansatz

Für einen echten Zero-Trust-Sicherheitsansatz sind identitätszentrierte, kontextorientierte Zugriffsrichtlinien erforderlich, die auf jeden User, jedes Gerät und jede Anwendung zugeschnitten sind. Das Ziel besteht darin, sicherzustellen, dass nur vertrauenswürdige User auf bestimmte Ressourcen zugreifen können und dass diese User und Ressourcen durch die etablierten Kontrollen Ihres Unternehmens festgelegt werden. Sie können in Ihrem Zero Trust-Sicherheitsframework Regeln festlegen, um Usern basierend auf Standort, Identität, Zeit/Datum und mehr Zugriff zu gewähren. Zscaler führt Sie durch diesen Prozess, damit Ihr Unternehmen mit diesen Kontrollen gut aufgestellt ist.

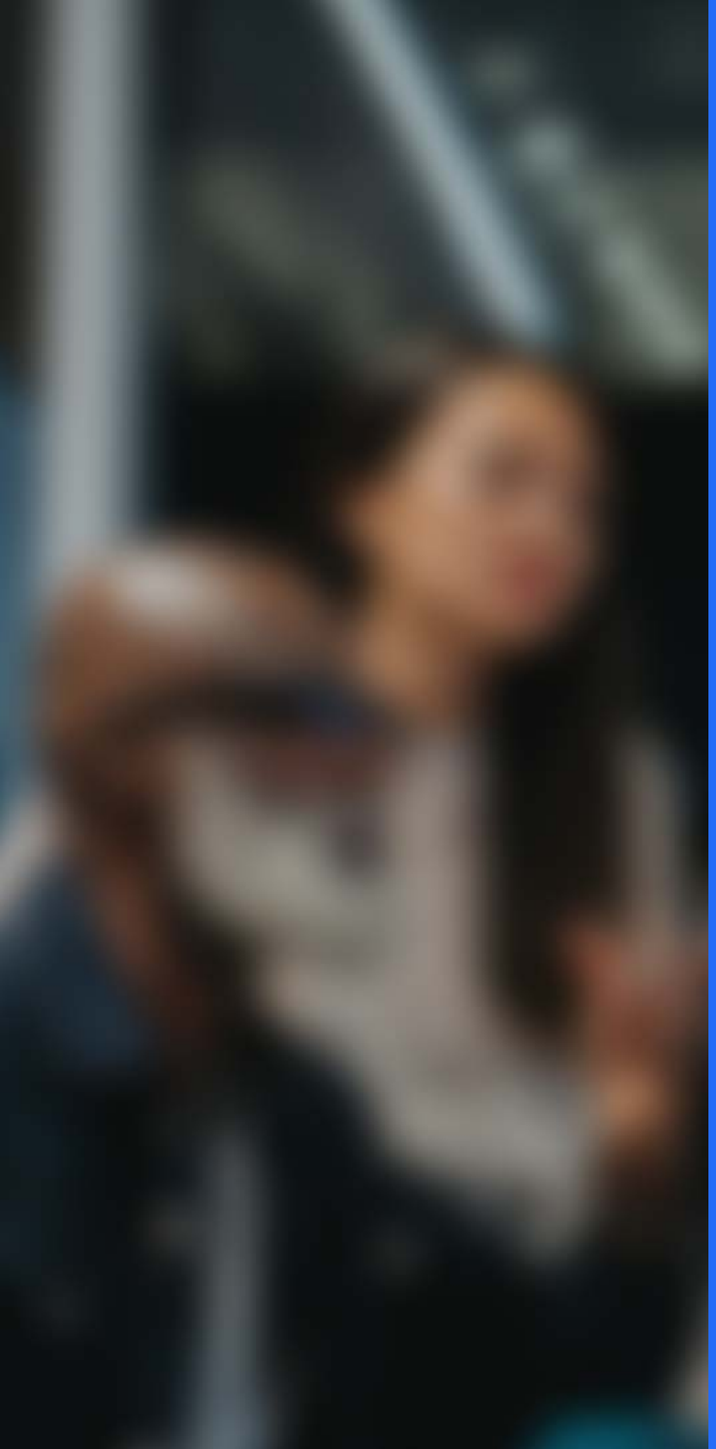
Fordern Sie eine Demo an, um mehr darüber zu erfahren, wie Zscaler Ihnen bei der Transformation Ihres Sicherheitsstatus zum Schutz Ihrer verteilten Belegschaft helfen kann.

QUELLEN:

1. Intelligent CISO, Check Point Research unveils Q2 2024 cyberattack trends, highlighting global and UAE increases, 29. Juli 2024.
2. Zscaler, ThreatLabz-Report zu verschlüsselten Angriffen 2024, 2024.
3. Zscaler, Ransomware-Report von ThreatLabz 2024, 2024.
4. Infosecurity Magazine, 70% of CISOs Expect Cyber-Attacks in Next Year, Report Finds, 21. Mai 2024.



©2025 Zscaler, Inc. Alle Rechte vorbehalten.



zscaler™ | Experience your world, secured.™

©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.

