CLOUDFLARE

WHITEPAPER

Zero Trust-Architektur – ein Wegweiser

Maßnahmen, Tools und Teams zur Verwandlung und Modernisierung der IT-Sicherheit

Inhaltsverzeichnis

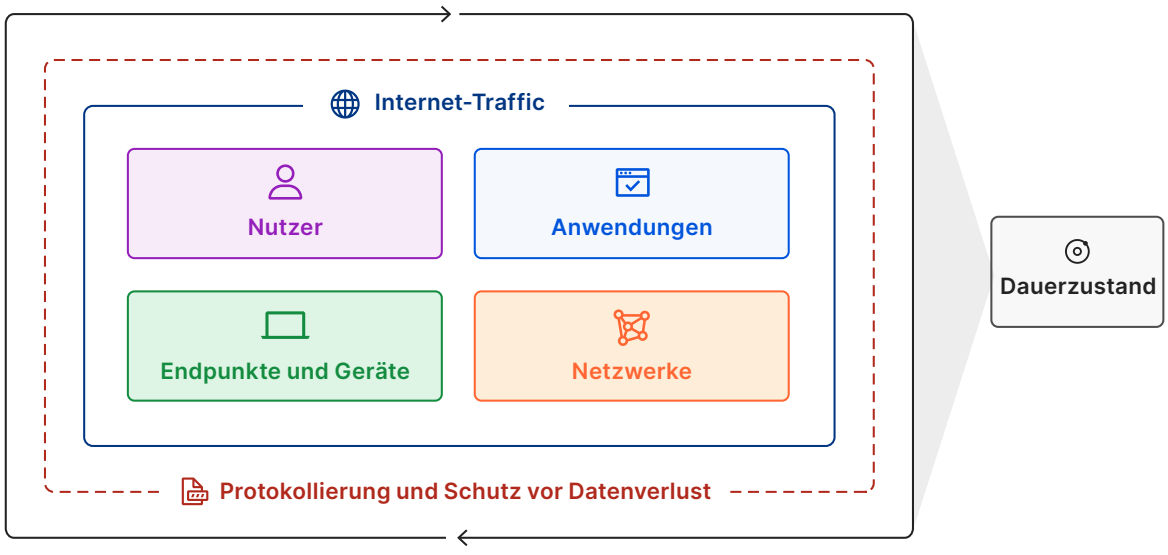
Einleitung

Die Entwicklung herkömmlicher Netzwerkarchitektur stützt sich auf das Perimetermodell, bei dem jedem ein gewisses Vertrauen entgegengebracht wird, sobald er sich im Netzwerk befindet. Doch moderne Trends wie das Hosting in der Cloud und hybrides Arbeiten stellen die klassische perimeterbasierte Netzwerkarchitektur in mancher Hinsicht vor Probleme.

Beheben lassen sich diese durch die Implementierung einer Zero Trust-Architektur, mit der sich der gesamte ein- und ausgehende Traffics eines Unternehmens verifizieren und autorisieren lässt. Eine solche Architektur kann auch schrittweise eingeführt werden, sodass die Beschäftigten nicht durch Verbindungsprobleme oder andere Schwierigkeiten bei ihrer Arbeit behindert werden.

Dieser von Sicherheitsexperten und -expertinnen entwickelte Leitfaden soll Möglichkeiten für eine anbieterunabhängige Zero Trust-Architektur aufzeigen und präsentiert einen Modellzeitplan für deren Implementierung. Bei der vorgestellten Zeitplanung wurde ein Unternehmen zugrunde gelegt, die bei der Einführung eines Zero Trust-Modells noch ganz am Anfang steht. Sie kann aber auch Firmen als Orientierung dienen, bei denen die Entwicklung schon weiter fortgeschritten ist.

Bei der Implementierung einer allumfassenden Zero Trust-Architektur müssen sieben Aspekte der IT-Sicherheit eines Unternehmens berücksichtigt werden. Sie muss nicht zwingend in der in der Reihenfolge eingeführt werden, die in den Abschnitten zu Bestandteilen und Referenzarchitektur dargestellt ist.



Bestandteile einer Zero Trust-Architektur

	Bestandteil	Ziel	Aufwand	Seite
1. Phase	Internet-Traffic	Globale DNS-Filterung einsetzen	▮	9
	Anwendungen	Eingehende E-Mails überwachen und Phishing-Versuche herausfiltern	▮	13
	DLP und Protokolle	Fehlkonfigurationen und öffentlich übermittelte Daten in SaaS-Tools erkennen	▮	20
2. Phase	Nutzer	Eine Unternehmensidentität schaffen	▮▮	5
	Nutzer	Einfache MFA für alle Anwendungen durchsetzen	▮	6
	Anwendungen	HTTPS und DNSSEC durchsetzen	▮	17
	Internet-Traffic	Durch SSL verborgene Bedrohungen blockieren oder isolieren	▮▮	9–10
	Anwendungen	Zero Trust-Richtlinien für öffentlich adressierbare Anwendungen durchsetzen	▮	14–16
	Anwendungen	Anwendungen vor Angriffen auf Schicht 7 schützen	▮	16
	Netzwerke	Alle für das Internet offenen Eingangsports zur Anwendungsbereitstellung schließen	▮	12
3. Phase	Anwendungen	Alle Firmenanwendungen inventarisieren	▮▮	13–14
	Anwendungen	Zero Trust-Richtlinien für SaaS-Anwendungen durchsetzen	▮▮	14–16
	Netzwerke	Netzwerkzugang von Nutzern segmentieren	▮▮▮	11
	Anwendungen	ZTNA für wichtige nicht öffentlich adressierbare Anwendungen	▮	14–16
	Geräte	MDM/UEM zur Kontrolle von Firmengeräten implementieren	▮▮	7
	DLP und Protokolle	Sensible Daten definieren und ermitteln, wo sie sich befinden	▮▮	18–19
	Nutzer	Security-Token versenden	▮▮	6
	DLP und Protokolle	Bezüglich bekannter Gefahrenquellen auf dem neuesten Stand bleiben	▮	21
4. Phase	Nutzer	MFA mit Security-Token durchsetzen	▮▮	6
	Anwendungen	Zero Trust-Richtlinien durchsetzen und ZTNA für alle Anwendungen anwenden	▮▮▮	14–16
	DLP und Protokolle	SOC zur Protokollauswertung, Richtlinienaktualisierung und Migration schaffen	▮▮	20
	Geräte	Endpunktschutz implementieren	▮▮	7
	Geräte	Alle Geräte, APIs und Services des Unternehmens inventarisieren	▮	8
	Netzwerke	Breitbandinternet für Verbindungen zwischen Firmenzweigstellen nutzen	▮▮▮	11–12
	DLP und Protokolle	Aktivitäten von Mitarbeitenden für sensible Anwendungen protokollieren und überprüfen	▮▮	18
	DLP und Protokolle	Das Abfließen sensibler Daten aus Anwendungen unterbinden	▮▮▮	19
	Dauerzustand	DevOps-Ansatz zur Richtliniendurchsetzung bei neuen Ressourcen	▮▮	22
	Dauerzustand	Automatische Skalierung für On-Ramping-Ressourcen implementieren	▮▮▮	22–23

So stufen wir den für jeden Schritt erforderlichen Aufwand ein:

- ▮ – **Gering;** von einem einzelnen Mitarbeitenden oder einem kleinen Team umsetzbar
- ▮▮ – **Mittel;** erfordert ein ganzes Team und gründliche Vorbereitung
- ▮▮▮ – **Hoch;** erfordert mehrere Teams und einen Projektplan

Zero Trust – ein Wegweiser

Nutzer

Dazu zählen Angestellte, Auftragnehmer und Kunden. Zur Implementierung des Zero Trust-Prinzips muss sich ein Unternehmen zunächst ein genaues Bild davon machen, wem Vertrauen geschenkt werden kann und in Bezug worauf. Man spricht in diesem Zusammenhang auch von „Identität“. Danach muss festlegt werden, auf welchem Weg sich die Nutzeridentität auf sichere Weise authentifizieren lässt.

Eine Unternehmensidentität schaffen

Aufwand	– **Mittel**
Beteiligte(s) Team(s)	• Das für den Identitätsanbieter zuständige Team (normalerweise Sicherheit oder IT) • Die Administratoren, die interne, von Beschäftigten und Partnern verwendete Anwendungen verwalten
Produkt(e)	Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin
Zusammenfassung	Zur Authentifizierung und Autorisierung von Nutzern, die auf Firmenanwendungen zugreifen, ist eine einheitliche Unternehmensidentität erforderlich. Das ermöglicht eine reibungslosere Durchsetzung hochpräziser Anwendungsrichtlinien. **Folgende Fragen sollten Sie sich in diesem Zusammenhang außerdem stellen:** • Ist Ihr Unternehmen im Bereich Fusionen und Übernahmen aktiv? Wie werden Sie verschiedene Identitätsanbieter zusammenführen? • Nutzen Sie Authentifizierungsprotokolle, die nicht webbasiert sind (z. B. Active Directory, NTLM, Kerberos)?
Maßnahmen	1. Alle Firmennutzer beim Identitätsanbieter eintragen lassen a. Diese Werte können oft von einem Personalverwaltungssystem wie Workday oder ADP aus synchronisiert werden 2. Die Korrektheit der Nutzerdaten überprüfen 3. Registrierungsdaten neuer Nutzer zur Einrichtung eines Anmeldeprofils übermitteln

Multi-Faktor-Authentifizierung für alle Anwendungen durchsetzen

Aufwand	– **Gering** (bei Anwendung einfacher MFA) – **Mittel** (bei Verwendung von Security-Token)
Beteiligte(s) Team(s)	• Das für den Identitätsanbieter zuständige Team (normalerweise Sicherheit oder IT) • Die Administratoren, die interne, von Beschäftigten und Partnern verwendete Anwendungen verwalten
Produkt(e)	**Identitätsanbieter:** Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin **Reverse-Proxys für Anwendungen:** Microsoft Azure AD App Proxy, Akamai EAA, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA) **Security-Token:** Yubico
Zusammenfassung	Der beste Schutz vor dem Diebstahl von Anmeldedaten durch Phishing oder Datenlecks ist die Multi-Faktor-Authentifizierung (MFA). Meistens kann diese direkt bei einem Identitätsanbieter aktiviert werden. Bei Applikationen, für die Ihr Identitätsanbieter nicht über eine direkte Integration verfügt, empfiehlt sich zur Durchsetzung der MFA das Vorschalten eines Reverse-Proxy für Anwendungen.
Maßnahmen	1. Interne Nutzer über die bevorstehende MFA-Durchsetzung informieren; Registrierungsmöglichkeiten für verschiedene SMS- oder App-basierte Authentifizierungsdienste anbieten 2. MFA bei Ihrem Identitätsanbieter aktivieren 3. Für Anwendungen, die bei Ihrem Identitätsanbieter nicht integriert sind, einen vorgeschalteten Reverse-Proxy aktivieren 4. (Zusatz) Security-Token per Post oder persönlich an Mitarbeitende ausgeben 5. (Zusatz) MFA per Security-Token für die sensibelsten Anwendungen durchsetzen

Endpunkte und Geräte

Dies beinhaltet alle Geräte, APIs oder Softwaredienste eines Unternehmens ebenso wie solche, die auf Firmendaten Zugriff haben. Unternehmen müssen sich zunächst einen lückenlosen Überblick über ihre Geräte, APIs und Dienste verschaffen. Danach können Zero Trust-Richtlinien auf Grundlage des jeweiligen Kontexts eingeführt werden.

Mobilgeräteverwaltung implementieren

Aufwand	– **Mittel**
Beteiligte(s) Team(s)	• IT
Produkt(e)	**Mac:** Jamf, Kandji **Windows:** Microsoft Intune
Zusammenfassung	In der Regel muss bei Zero Trust-Architekturen Software mindestens auf einem Teil der Nutzerrechner installiert werden. Ein Großteil der Unternehmen verwaltet Software und Konfigurationen für ihren gesamten Nutzergerätebestand mittels MDM (Mobile Device Management; Mobilgeräteverwaltung).
Maßnahmen	Weitere Einzelheiten finden Sie auf der Website des jeweiligen MDM-Anbieters

Endpunktschutz implementieren

Aufwand	– **Mittel**
Beteiligte(s) Team(s)	• IT-Sicherheit • IT
Produkt(e)	VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender
Zusammenfassung	Software für den Endpunktschutz ist auf dem Rechner eines Nutzers installiert und sucht nach bekannten Bedrohungen, die den Gerätebetrieb beeinträchtigen. Sie kann auch eingesetzt werden, um die Installation von Betriebssystem-Patches und -Aktualisierungen zu erzwingen. Die Rückmeldungen der Software können und sollten in die Richtlinien zur Kontrolle des Anwendungszugriffs einfließen.
Maßnahmen	1. Software für Endpunktschutz auf Nutzerrechnern installieren, die MDM nutzen 2. Bedrohungsschutz und Compliance-Kontrolle auf der Plattform für Endpunktschutz aktivieren

Geräte, APIs und Services inventarisieren

Aufwand	– Gering
Beteiligte(s) Team(s)	• IT-Sicherheit • IT
Produkt(e)	**Geräteinventarisierung:** VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender, Oomnitza **API/Service-Inventarisierung:** Anwendungskonnektor von Cloudflare, Zscaler Private Access (ZPA)
Zusammenfassung	Software für Endpunktschutz und Asset-Management kann genutzt werden, um alle Geräte zu verfolgen, die an Nutzer ausgegeben wurden. Es sollte eine genaue Geräteliste geführt werden, um nachverfolgen zu können, welche Geräte zulässig sind und auf bestimmte Anwendungen zugreifen dürfen. APIs und Dienste sollten auch in einer beständig aktualisierten Inventarliste erfasst werden. Durch Scannen des Netzwerks lassen sich neue APIs und Softwaredienste aufspüren, die über ein internes oder externen Netzwerk kommunizieren können.
Maßnahmen	1. Software für Endpunktschutz auf Nutzerrechnern installieren, die MDM nutzen 2. API-/Service-Scanner für das Netzwerk installieren

Internet-Traffic

Dies beinhaltet sämtlichen Nutzer-Traffic, der für Webseiten außerhalb des Kontrollbereichs eines Unternehmens bestimmt ist: Er kann mit geschäftsbezogenen Aufgaben in Verbindung stehen, aber auch auf die persönliche Nutzung von Websites zurückgehen. Der gesamte ausgehende Datenverkehr kann Malware und schädlichen Websites ausgesetzt sein. Ein Unternehmen muss sich daher einen Überblick und die Kontrolle über den für das Internet bestimmten Traffic verschaffen.

DNS-Anfragen an bekannte Gefahrenquellen oder riskante Ziele blockieren

Aufwand	**– Gering**
Beteiligte(s) Team(s)	• IT-Team mit Zugriff auf Router oder Rechnerkonfiguration • IT-Sicherheit
Produkt(e)	**DNS-Filterung:** Cisco Umbrella DNS, Cloudflare Gateway, DNSFilter, Zscaler Shift
Zusammenfassung	DNS-Filterung kann per Routerkonfiguration oder direkt auf einem Nutzerrechner angewandt werden. Sie zählt zu den schnellsten Wegen, Nutzer vor bekannten Schad-Websites zu schützen.
Maßnahmen	**DNS-Filterung:** Die Konfiguration der DNS-Auflösung für das Firmen-WLAN sollte so aktualisiert werden, dass sie auf den passenden DNS-Auflösungsdienst verweist; auf diese Weise können bekannte Schad-Webistes blockiert werden

Durch SSL/TLS verborgene Bedrohungen blockieren oder isolieren

Aufwand	**– Mittel**
Beteiligte(s) Team(s)	• IT-Team mit Zugriff auf Router oder Rechnerkonfiguration • IT-Sicherheit
Produkt(e)	**TLS-Entschlüsselung:** Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) **Browserisolierung:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation

Durch SSL/TLS verborgene Bedrohungen blockieren oder isolieren (Fortsetzung)

Zusammenfassung	Einige Bedrohungen verbergen sich hinter SSL und können nicht per HTTPS-Überprüfung blockiert werden. Zum besseren Schutz von Nutzern von solchen Gefahren sollte TLS-Entschlüsselung eingesetzt werden.
Maßnahmen	**TLS-Entschlüsselung:** 1. Sicherstellen, dass die richtige Client-Software auf einem Nutzerrechner installiert ist a. Nach VPN-Verbindungen oder Software suchen, die den ausgehenden Web-Traffic des Geräts beeinträchtigen könnten 2. Das Root-Zertifikat auf dem Gerät für TLS-Entschlüsselung konfigurieren 3. Richtlinien dazu aktivieren, wann eine Entschlüsselung von Nutzerdatenverkehr zu vermeiden ist a. Empfehlenswert für Websites, die Certificate Pinning nutzen b. Manche Unternehmen verzichten auch für den privaten Traffic der Nutzer (z. B. Bank, Social Media usw.) auf Verschlüsselung **Browserisolierung:** 1. Browserisolierung kann mit Client-Software auf einem Gerät oder über einen Isolierungslink angewandt werden; beide Herangehensweisen sollten in Betracht gezogen werden

Netzwerke

Dazu zählen alle öffentlichen, nicht öffentlichen und virtuellen Netzwerke einer Firma. Unternehmen müssen sich zunächst eine klare Vorstellung von ihren bestehenden Netzwerken machen und diese so in Segmente aufteilen, dass laterale Bewegungen verhindert werden. Anschließend können Zero Trust-Richtlinien erstellt werden, die bis ins Detail bestimmen, auf welche Abschnitte eines Netzwerks Nutzer, Endpunkte und Geräte zugreifen können.

Netzwerkzugang von Nutzern segmentieren

Aufwand	– Hoch
Beteiligte(s) Team(s)	• IT-Sicherheit • IT
Produkt(e)	**Zero Trust Network Access (ZTNA):** Cloudflare Zero Trust (Kombination von Access und Gateway), Netskope Private Access, Zscaler Private Access (ZPA)
Zusammenfassung	Nutzer haben normalerweise Zugriff auf das gesamte nicht öffentliche Netzwerk, wenn sie ein VPN verwenden oder sich im Netzwerk ihrer Zweigstelle befinden. Bei einem Zero Trust-System erhalten sie jedoch nur Zugang zu den Abschnitten des Netzwerks, auf die sie zur Erfüllung einer konkreten Aufgabe zugreifen müssen. Zero Trust-Netzwerklösungen erlauben Anwendern zwar den Fernzugriff auf ein lokales Netzwerk, jedoch nur unter Einhaltung hochpräziser Richtlinien auf Grundlage von Faktoren, die unter anderem nutzer- oder gerätebezogen sind.
Maßnahmen	1. ZTNA für ein nicht öffentliches Netzwerk bereitstellen a. Normalerweise mittels eines Anwendungskonnektors, GRE- oder IPSec-Tunnels 2. ZTNA-Client auf Nutzergeräten installieren, für die MDM genutzt wird 3. Richtlinien zum Segmentieren der Nutzerzugriffsrechte im nicht öffentlichen Netzwerk festlegen

Breitbandinternet für Verbindungen zwischen Firmenzweigstellen nutzen

Aufwand	– Hoch
Beteiligte(s) Team(s)	• Network Engineering • IT
Produkt(e)	Cloudflare Magic WAN, Cato Networks, Aryaka FlexCore

Nutzung von Breitbandinternet für Verbindungen zwischen Firmenzweigstellen (Fortsetzung)

Zusammenfassung	Verbindungen zwischen Standorten nicht öffentlicher Netzwerke (z. B. Rechenzentren und Zweigstellen) wurden bisher üblicherweise mit Multi-Protocol Label Switching (MPLS) oder anderen von Telekomfirmen angebotenen nicht öffentlichen Vernetzungsmethoden hergestellt. Diese MPLS-Verbindungen sind normalerweise mit hohen Kosten verbunden und da sich die Qualität des Standardinternets gesteigert hat, können Unternehmen inzwischen für einen Bruchteil der Kosten durch das Routing von Datenverkehr über das Internet mittels sicherer Tunnel einen ebenso gut geschützten Zugang bieten.
Maßnahmen	1. Für den Anfang sollten zwei Standorte mit MPLS-Verbindung ausgewählt werden;diese benötigen eine Art von Internetverbindung. 2. Es sollte ein Paar redundanter Anycast GRE- oder IPsec-Tunnel über die Internetleitungen aufgebaut werden, die zu dem Edge-Netzwerk des cloudbasierten WAN-Anbieters führen 3. Anschließend müssen Zustand und Verbindungsfähigkeit dieser Tunnel überprüft werden; die Performance (Durchsatz, Latenz, Paketverlust, Jitter) von Traffic-Workloads, die dem Betriebsdatenverkehr so nahekommen sollten wie möglich, muss getestet werden 4. Routing-Richtlinien sollten so angepasst werden, dass Betriebs-Traffic von MPLS auf Internet-Tunnel verlagert wird 5. Dasselbe sollte beim nächsten Standort mit MPLS-Verbindung wiederholt werden 6. MPLS-Leitungen stilllegen

Alle für das Internet zur Anwendungsbereitstellung offenen Eingangsports schließen

Aufwand	**– Gering**
Beteiligte(s) Team(s)	• Network Engineering
Produkt(e)	**Zero Trust-Reverse-Proxys:** Akamai EAA, Cloudflare Access, Netskope, Zscaler Private Access (ZPA)
Zusammenfassung	Offene Eingangsports sind ein beliebter Angriffsvektor, können aber mittels Scanning aufgespürt werden. Zero Trust-Reverse-Proxys ermöglichen die sichere Offenlegung einer Webanwendung ohne das Öffnen von Eingangsports. Der DNS-Eintrag der Anwendung ist ihr einziger öffentlich sichtbarer Eintrag. Er wird durch Zero Trust-Richtlinien geschützt. Als zusätzliche Sicherheitsmaßnahme kann ein internes / nicht öffentliches DNS mit einem Zero Trust-Netzwerkzugang eingesetzt werden (nähere Einzelheiten finden Sie weiter unten).
Maßnahmen	1. Einen Anwendungskonnektor für Reverse-Proxys installieren, wobei es sich normalerweise um einen Daemon oder eine virtuelle Maschine im selben Netzwerk handelt 2. Die Reverse-Proxy-Anwendung mit dem Anwendungskonnektor verbinden 3. Alle Eingangsports des nicht öffentlichen Netzwerks mittels einer Firewallregel schließen

Anwendungen

Damit sind alle Ressourcen gemeint, auf denen sich Firmendaten befinden oder Geschäftsabläufe durchgeführt werden. Unternehmen müssen sich zunächst ein umfassendes Bild von den vorhandenen Anwendungen machen und anschließend für jede von ihnen Zero Trust-Richtlinien erstellen oder gegebenenfalls unzulässige Applikationen sperren.

E-Mail-Anwendungen überwachen und Phishing-Versuche herausfiltern

Aufwand	– Gering
Beteiligte(s) Team(s)	• Das Team, das für die Konfiguration des E-Mail-Providers zuständig ist (normalerweise das IT-Team)
Produkt(e)	**Cloudbasierte E-Mail-Sicherheit:** Cloudflare Area 1 Email Security, Mimecast, TitanHQ **Browserisolierung:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation
Zusammenfassung	E-Mails sind einer der wenigen Kommunikationskanäle, über die Angreifer uneingeschränkten Zugang zu den Beschäftigten haben. Der Einsatz eines sicheren E-Mail-Gateways ist daher wichtig, um sicherzustellen, dass bösartige oder fragwürdige E-Mails die Mitarbeitenden gar nicht erst erreichen. Darüber hinaus sollte die IT-Sicherheit die Möglichkeit in Erwägung ziehen, Links in einem isolierten Browser unter Quarantäne zu stellen, wenn diese nicht verdächtig genug erscheinen, um sie vollständig zu blockieren.
Maßnahmen	1. MX-Einträge der Domain so konfigurieren, dass diese auf einen sicheren E-Mail-Gateway-Dienst verweisen 2. In den ersten Wochen auf Fehlalarme hin überprüfen 3. (Zusatz) Eine linkbasierte Browserisolierung für E-Mail-Links konfigurieren, die sich im Graubereich ansiedeln

Alle Firmenanwendungen inventarisieren

Aufwand	– Mittel
Beteiligte(s) Team(s)	• IT-Sicherheit
Produkt(e)	**Secure Web Gateway und CASBs mit Aufspüren von Schatten-IT:** Cloudflare Gateway, Microsoft Defender for Cloud Apps, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)

Alle Firmenanwendungen inventarisieren (Fortsetzung)

Zusammenfassung	Für die IT-Sicherheit ist es ausschlaggebend, sich einen Überblick über sämtliche von einem Unternehmen eingesetzte Anwendungen zu verschaffen. Häufig stellt man fest, dass nicht genehmigte oder bislang unbekannte Anwendungen – oft als „Schatten-IT“ bezeichnet – unternehmensweit im Einsatz sind. Ein Secure Web Gateway mit TLS-Entschlüsselung kann zur Erkennung von Anwendungen eingesetzt werden. Damit können auch nicht genehmigte Applikationen oder Anwendungsmandanten (z. B. private Dropbox-Konten) gesperrt werden.
Maßnahmen	1. Scanning zum Aufspüren von Schatten-IT im Secure Web Gateway aktivieren 2. Sicherstellen, dass der Secure Web Gateway-Client auf Nutzergeräten installiert ist 3. Nutzer-Datenverkehr für zwei bis drei Wochen zulassen 4. Die Liste erkannter Anwendungen überprüfen 5. Nicht genehmigte Anwendungen durch Secure Web Gateway-Richtlinien sperren 6. Zugelassene Anwendungen durch Zero Trust-Richtlinien schützen

Zero Trust-Richtlinien für Anwendungen durchsetzen

Aufwand	– **Gering** (bei den meisten wichtigen Anwendungen) – **Hoch** (bei allen Anwendungen)
Beteiligte(s) Team(s)	• IT-Sicherheit • Anwendungsentwicklung • IT
Produkt(e)	**Zero Trust-Reverse-Proxys:** Azure App Proxy, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA) **Zero Trust Network Access (ZTNA):** Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA) **CASB:** Cloudflare CASB, Netskope CASB, Zscaler CASB **Remote Browser Isolation:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation

Zero Trust-Richtlinien für Anwendungen durchsetzen (Fortsetzung)

Zusammenfassung	Anwendungen müssen durch Zero Trust-Richtlinien geschützt werden, die zur Authentifizierung und Autorisierung die Nutzeridentität sowie Geräte- und Netzwerkkontext heranziehen. Für die Applikationen sollten hochpräzise Richtlinien gelten, die dafür sorgen, dass Nutzern die geringsmöglichen Rechte eingeräumt werden – insbesondere bei Anwendungen, die sensible Daten beherbergen. Man unterscheidet im Wesentlichen zwischen drei Anwendungsarten und für jede von ihnen ist ein anderes Zero Trust-Sicherheitsmodell zu wählen. Es handelt sich um: 1. Nicht öffentliche selbstgehostete Anwendungen (nur im Firmennetzwerk adressierbar) 2. Öffentliche selbstgehostete Anwendungen (über das Internet adressierbar) 3. SaaS-Anwendungen **Hinweis:** Falls Gerätekontext oder Compliance-Status von der Sicherheitsrichtlinie verlangt werden, ist normalerweise Client-Software auf dem Gerät erforderlich.
Maßnahmen	**Nicht öffentliche selbstgehostete Anwendungen** 1. Einen verschlüsselten Tunnel zwischen der Anwendung und der Schicht mit der Zero Trust-Richtlinie aufbauen; normalerweise handelt es sich um einen „Anwendungskonnektor“, einen GRE- oder IPSec-Tunnel 2. Den nicht öffentlichen DNS-Resolver für Nutzer des ZTNA-Geräte-Clients verfügbar machen 3. Richtlinien auf Grundlage von Nutzer-, Geräte- und Netzwerkkontext erstellen, mit denen festgelegt wird, wer auf die Anwendung zugreifen kann **Öffentliche selbstgehostete Anwendungen** 1. Autoritatives DNS oder CNAME-Eintrag in den Anwendungs-Reverse-Proxy verlagern 2. Sicherstellen, dass alle Eingangsports für das Anwendungsnetzwerk geschlossen sind 3. Richtlinien auf Grundlage von Nutzer-, Geräte- und Netzwerkkontext erstellen, mit denen festgelegt wird, wer auf die Anwendung zugreifen kann **SaaS-Anwendungen** Es gibt verschiedene Möglichkeiten zur Durchsetzung von Zero Trust-Richtlinien für SaaS-Anwendungen **Identitäts-Proxy** Cloudflare, Netskope und Zscaler stellen Identitäts-Proxys bereit, die die gleiche Richtliniendurchsetzung erlauben wie eine selbstgehostete Anwendung mit Reverse-Proxy. Dafür muss der Identitäts-Proxy als SSO-Anbieter der SaaS-Anwendung eingerichtet sein 1. Gegebenenfalls bestehende SSO-Integration für die SaaS-App entfernen 2. Identitäts-Proxys mit der SaaS-Anwendung integrieren 3. Vergewissern, dass die richtigen SAML-Attribute zur Erstellung und Aktualisierung eines Nutzerprofils übermittelt werden 4. Richtlinien auf Grundlage des Nutzer-, Geräte- und Netzwerkkontexts erstellen

Zero Trust-Richtlinien für Anwendungen durchsetzen (Fortsetzung)

Maßnahmen	**Secure Web Gateway und Single Sign-on** Die andere Möglichkeit besteht darin, auf einen bereits genutzten Single Sign-on-Anbieter zurückzugreifen, um zu kontrollieren, welche Nutzer auf eine SaaS-Applikation zugreifen können und welche nicht. Dann kann durch das Secure Web Gateway mit einer eigenen IP-Adresse sichergestellt werden, dass nur Nutzer von verwalteten Diensten mit Traffic-Überprüfung Zugang zu der SaaS-Anwendung erhalten. 1. SaaS-Anwendung beim SSO-Dienstleister eintragen lassen 2. Richtlinien zur Bestimmung der autorisierten Nutzer erstellen 3. IP-Adresse der Secure Web Gateway-Instanz zur IP-Zulassungsliste der SaaS-Anwendung hinzufügen (die meisten SaaS-Applikationen unterstützen IP-Zulassungslisten in ihren Grundeinstellungen für Sicherheit) 4. Secure Web Gateway-Richtlinie erstellen, um darüber zu bestimmen, welche Nutzer auf die SaaS-Anwendung zugreifen dürfen

Anwendungen vor Angriffen auf Schicht 7 (DDoS, Injection, Bots usw.) schützen

Aufwand	**– Gering**
Beteiligte(s) Team(s)	• IT-Sicherheit • Anwendungsentwicklung
Produkt(e)	Akamai, AWS, Azure, Cloudflare, GCP
Zusammenfassung	Jede selbstgehostete Applikation kann Opfer eines Angriffs auf Schicht 7 werden, was DDoS-Attacken ebenso umfasst wie Code Injection, Bots und vieles mehr. Die IT-Sicherheit sollte eine Web Application Firewall und DDoS-Schutz vor allen selbstgehosteten nicht öffentlich und öffentlich adressierbaren Anwendungen in Stellung bringen.
Maßnahmen	1. Eintrag eines autoritativen DNS einer beliebigen öffentlichen Anwendung hinzufügen 2. Web Application Firewall und DDoS-Schutz aktivieren

HTTPS und DNSSEC durchsetzen

Aufwand	– **Gering**
Beteiligte(s) Team(s)	• IT-Sicherheit • Anwendungsentwicklung
Produkt(e)	Akamai, AWS, Azure, Cloudflare, GCP
Zusammenfassung	Jede selbstgehostete Webanwendung sollte HTTPS und DNSSEC nutzen. Dadurch wird Packet Sniffing oder Domain-Hijacking unterbunden.
Maßnahmen	1. Eintrag eines autoritativen DNS einer beliebigen öffentlichen Anwendung hinzufügen 2. HTTPS auf „Strict“ setzten und DNSSEC aktivieren

DLP und Protokollierung

Wenn alle Komponenten der Zero Trust-Architektur bis zu diesem Punkt eingerichtet wurden, wird diese Architektur große Mengen an Daten über die Vorgänge innerhalb des Netzwerks generieren. Nun ist es Zeit, Schutz vor Datenverlust (Data Loss Prevention – DLP) und Protokollierung einzuführen. Dafür sind eine Reihe von Verfahren und Tools erforderlich, deren Schwerpunkt darauf liegt, das Abwandern sensibler Daten aus dem Unternehmen zu verhindern und daher auf jede potenzielle Gefahr eines Datenlecks aufmerksam zu machen. Unternehmen müssen sich zunächst einen umfassenden Überblick darüber verschaffen, wo sich ihre sensiblen Daten befinden. Dann können sie Zero Trust-Kontrollmechanismen einführen, um den Zugriff und das Ausschleusen solcher Daten zu unterbinden.

Verfahren zur Protokollierung und Überprüfung des Datenverkehrs sensibler Anwendungen einführen

Aufwand	– **Mittel**
Beteiligte(s) Team(s)	• IT-Sicherheit
Produkt(e)	**Secure Web Gateway (SWG):** Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) **Security Incident and Event Monitoring (SIEM):** DataDog, Splunk, SolarWinds
Zusammenfassung	Secure Web Gateway-Lösungen sind in der Lage, Protokolle zu Nutzerdatenverkehr an ein SIEM-Tool weiterzuleiten. Mitarbeitende der IT-Sicherheit sollten Traffic-Protokolle für sensible Applikationen regelmäßig überprüfen. In dem SIEM können spezielle Warnmeldungen im Falle von ungewöhnlichem oder schädlichem Traffic eingerichtet und im Lauf der Zeit angepasst werden.
Maßnahmen	1. Vergewissern, dass der gesamte für sensible Anwendungen bestimmte Nutzer-Traffic mittels SWG über einen Proxy-Server geleitet wird 2. Protokollübertragung oder Protokollabruf zwischen SWG und SIEM aktivieren 3. Ein festes Zeitintervall für die regelmäßige Überprüfung der Traffic-Protokolle durch das Sicherheitsteam festlegen 4. Konfiguration der Warnmeldungen im SIEM auf Grundlage der im Lauf der Zeit gewonnenen Erkenntnisse anpassen

Sensible Daten definieren und ermitteln, wo sie sich befinden

Aufwand	– **Mittel**
Beteiligte(s) Team(s)	• IT-Sicherheit • Compliance / Recht
Produkt(e)	**Security Incident and Event Monitoring (SIEM):** DataDog, Splunk, SolarWinds

Sensible Daten definieren und ermitteln, wo sie sich befinden (Fortsetzung)

Zusammenfassung	Die Definition des Begriffs „sensible Daten“ kann von Branche zu Branche stark variieren. Technologieunternehmen wollen ihren Quellcode schützen, während etwa bei Anbietern im medizinischen Bereich der Fokus auf der sicheren Speicherung von Gesundheitsdaten liegt. Unternehmen müssen sich deshalb darüber klarwerden, was sie unter sensiblen Daten verstehen und wo sich diese befinden. Eine genaue Definition und Inventarisierung solcher Daten gibt dann bei der Implementierung von DLP-Tools die Richtung vor.
Maßnahmen	1. Traffic-Protokolle in den SIEM-Tools oder direkt in einem Secure Web Gateway auswerten, um Zielanwendungen und Datenspeicherorten zu identifizieren 2. Vorhandene sensible Daten inventarisieren

Das Abfließen sensibler Daten aus Anwendungen unterbinden

Aufwand	– **Hoch**
Beteiligte(s) Team(s)	• IT-Sicherheit • IT • Compliance / Recht
Produkt(e)	**Data Loss Prevention (DLP) innerhalb des Netzwerkpfads:** Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)
Zusammenfassung	DLP-Lösungen, die innerhalb des Netzwerkpfads arbeiten, überprüfen den Nutzer-Traffic sowie hoch- oder heruntergeladene Dateien auf sensible Daten. Die sensiblen Daten sind in gut bekannten vordefinierten Listen (z. B. PII, SSNs, Kreditkarten usw.) oder spezifischen Mustern erkennbar, die von einem Administrator manuell konfiguriert werden können. DLP-Kontrollen sollten für sensible Anwendungen aktiviert werden und können auf den gesamten Nutzerdatenverkehr ausgeweitet werden.
Maßnahmen	1. Client-Software des DLP-Anbieters installieren 2. Vergewissern, dass kein vorhandenes VPN oder ein anderes Tool Verbindungsstörungen verursacht 3. Sicherstellen, dass TLS-Entschlüsselung aktiviert und auf jedem Nutzerrechner ein Root-Zertifikat vorhanden ist 4. DLP-Kontrollen aktivieren 5. DLP-Blockiervorfälle beobachten und überprüfen, ob diese berechtigt waren oder es sich um einen Fehlalarm handelte

Fehlkonfigurationen und öffentlich übermittelte Daten in SaaS-Tools identifizieren

Aufwand	– Gering
Beteiligte(s) Team(s)	• IT-Sicherheit
Produkt(e)	**API-basierte Cloud Access Security Broker (CASB):** Cloudflare CASB, DoControl, Netskope, Zscaler CSPM
Zusammenfassung	CASBs verfügen über Integrationen mit großen SaaS-Anwendungen per API. Der CASB scannt die SaaS-Applikation auf bekannte Sicherheitsfehlkonfigurationen und öffentlich übermittelte Daten. Ein Sicherheitsteam sollte in regelmäßigen Abständen die vom CASB gewonnenen Erkenntnisse auswerten.
Maßnahmen	1. Jede SaaS-Applikation mithilfe der Anleitung des Providers zur API-Integration verbinden 2. Scans für jede SaaS-Anwendung durchführen 3. Die Ergebnisse auswerten und mit der Problembehebung in jeder SaaS-Applikation beginnen, sofern angemessen

Security Operations Center (SOC) zur Auswertung von Protokollen, Aktualisierung von Richtlinien und Gefahrenabwehr schaffen

Aufwand	– Mittel
Beteiligte(s) Team(s)	• IT-Sicherheit
Produkt(e)	**Keine**
Zusammenfassung	Ein SOC ist ein wesentlicher Baustein für ein Sicherheitsteam innerhalb eines Zero Trust-Systems. Dabei sollte der Fokus auf der Überprüfung der Protokollinformationen und der Sicherheitswarnmeldungen sowie auf der Abstimmung der Zero Trust-Richtlinien für alle wichtigen Sicherheitsprodukte liegen.
Maßnahmen	1. Protokolle im SIEM oder direkt in der Sicherheitslösung auswerten 2. Warnmeldungen oder außergewöhnliche Aktivitäten identifizieren 3. Zero Trust-Richtlinien für jedes Tool auf Grundlage der Erkenntnisse aktualisieren

Bezüglich bekannter Gefahrenquellen auf dem neuesten Stand bleiben

Aufwand	– Gering
Beteiligte(s) Team(s)	• IT-Sicherheit
Produkt(e)	**Anbieter von Bedrohungsdaten:** Cloudflare Radar, CISA, OWASP
Zusammenfassung	Es gibt mehrere Anbieter, die auf die Erstellung von Listen bekannter Bedrohungen und bösartiger Websites spezialisiert sind. Diese können automatisch in ein Secure Web Gateway geladen werden, um Nutzer vor Angriffen zu schützen.
Maßnahmen	1. Bedrohungsinformationen in das Secure Web Gateway einbinden 2. Bedrohungsschutz im DNS und HTTP-Filterung aktivieren

Dauerzustand

Wurde die Zero Trust-Architektur für alle anderen Bereiche des Unternehmens aufgebaut, können ein paar Maßnahmen ergriffen werden, um Zero Trust im Unternehmen in einen Dauerzustand zu überführen. Auf diese Weise wird die künftige Harmonisierung mit der Architektur gewährleistet.

DevOps-Ansatz zur Durchsetzung von Richtlinien bei allen neuen Ressourcen anwenden

Aufwand	– Hoch
Beteiligte(s) Team(s)	• IT-Sicherheit • Anwendungsentwicklung
Produkt(e)	**Infrastruktur-Automatisierung:** Ansible, Puppet, Terraform
Zusammenfassung	Tools zur Automatisierung der Infrastruktur erlauben es Entwicklern, Zero Trust-Sicherheitsprinzipien im Rahmen ihres Anwendungs-Entwicklungsprozesses automatisch anzuwenden. Es sollten interne Überprüfungen eingeführt werden, die immer dann durchgeführt werden, wenn eine Anwendung mit Zero Trust-Reverse-Proxy-Schutz implementiert wird.
Maßnahmen	1. Eine Standardrichtlinie für neue Applikationen definieren 2. Tests in das Verfahren für die Anwendungsimplementierung integrieren, die Zero Trust-Reverse-Proxy-Schutz erfordern

Automatische Skalierung für On-Ramping-Ressourcen implementieren

Aufwand	– Hoch
Beteiligte(s) Team(s)	• IT-Sicherheit • Anwendungsentwicklung
Produkt(e)	**Load Balancer:** Akamai, Cloudflare **Infrastruktur-Automatisierung:** Ansible, Puppet, Terraform

Automatische Skalierung für On-Ramping-Ressourcen implementieren (Fortsetzung)

Zusammenfassung	Load Balancer können wirksame Werkzeuge sein, um sicherzustellen, dass die Infrastruktur jeder einzelnen Anwendung nie überlastet wird. Außerdem kann damit für eine gewisse Redundanz gesorgt werden, falls sich der Ausfall eines Anwendungsservers abzeichnet. Tools zur Infrastrukturautomatisierung können eingesetzt werden, um neue Ressourcen in Betrieb zu nehmen, wenn der Traffic bestimmte Schwellenwerte überschreitet.
Maßnahmen	1. Load Balancer vor dem Anwendungskonnektor des Zero Trust-Revese-Proxys konfigurieren 2. Lastverteilungsregeln auf Grundlage der Datenverkehrsmenge und / oder des geografischen Nutzerstandorts definieren 3. Richtlinien für die Infrastrukturautomatisierung implementieren, sodass neue virtuelle Maschinen bereitgestellt werden, wenn für bestimmte Anwendungen eine ausreichend hohe Last generiert wurde

Zeitplan für eine Implementierung (Beispiel)

Jede Einführung einer Zero Trust-Architektur ist individuell, doch bestimmte Schritte werden bei den meisten Vorhaben vorgenommen. Abgebildet ist ein empfohlener Zeitplan für ein Unternehmen, das mit der Implementierung einer Zero Trust-Architektur gerade erst beginnt.

Zeitplan		Ziel	Relevante Produkte
1. Phase	☐	**Globale DNS-Filterung einsetzen**	Cisco Umbrella DNS, Cloudflare Gateway, DNSFilter, Zscaler Shift
	☐	**Eingehende E-Mails überwachen und Phishing-Versuche herausfiltern**	**Cloudbasierte E-Mail-Sicherheit:** Cloudflare Area 1 Email Security, Mimecast, TitanHQ **Browserisolierung:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation
	☐	**Fehlkonfigurationen und öffentlich übermittelte Daten in SaaS-Tools erkennen**	Cloudflare CASB, DoControl, Netskope, Zscaler CSPM
2. Phase	☐	**Eine Unternehmensidentität schaffen**	Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin
	☐	**Einfache MFA für alle Anwendungen durchsetzen**	**Identitätsanbieter:** Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin **Reverse-Proxys für Anwendungen:** Microsoft Azure AD App Proxy, Akamai EAA, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA)
	☐	**HTTPS und DNSSEC durchsetzen**	Akamai, AWS, Azure, Cloudflare, GCP
	☐	**Durch SSL verborgene Bedrohungen blockieren oder isolieren**	**TLS-Entschlüsselung:** Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) **Browserisolierung:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation
	☐	**Zero Trust-Richtlinien für öffentlich adressierbare Anwendungen durchsetzen**	**Zero Trust-Reverse-Proxys:** Azure App Proxy, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA)
	☐	**Anwendungen vor Angriffen auf Schicht 7 schützen**	Akamai, AWS, Azure, Cloudflare, GCP
	☐	**Alle für das Internet offenen Eingangsports zur Anwendungsbereitstellung schließen**	Akamai EAA, Cloudflare Access, Netskope, Zscaler Private Access (ZPA)
3. Phase	☐	**Alle Firmenanwendungen inventarisieren**	**Secure Web Gateway und CASBs mit Offenlegung von Schatten-IT:** Cloudflare Gateway, Microsoft Defender for Cloud Apps, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)
	☐	**Zero Trust-Richtlinien für SaaS-Anwendungen durchsetzen**	**Zero Trust Network Access (ZTNA):** Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA) **CASB:** Cloudflare CASB, Netskope CASB, Zscaler CASB

	☐ **Netzwerkzugang von Nutzern segmentieren**	**Zero Trust Network Access (ZTNA):** Cloudflare Zero Trust (Kombination von Access und Gateway), Netskope Private Access, Zscaler Private Access (ZPA)
	☐ **ZTNA für wichtige nicht öffentlich adressierbare Anwendungen**	Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA)
	☐ **MDM/UEM zur Kontrolle von Firmengeräten implementieren**	**Mac:** Jamf, Kandji **Windows:** Microsoft Intune
	☐ **Sensible Daten definieren und ermitteln, wo sie sich befinden**	DataDog, Splunk, SolarWinds
	☐ **Security-Token versenden**	**Security-Token:** Yubico
	☐ **Bezüglich bekannter Gefahrenquellen auf dem neuesten Stand bleiben**	Cloudflare Radar, CISA, OWASP
4. Phase	☐ **MFA mit Security-Token durchsetzen**	**Security-Token:** Yubico
	☐ **Zero Trust-Richtlinien durchsetzen und ZTNA für alle Anwendungen anwenden**	Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA)
	☐ **SOC zur Protokollauswertung, Richtlinienaktualisierung und Migration schaffen**	Keine Angaben
	☐ **Endpunktschutz implementieren**	VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender
	☐ **Alle Geräte, APIs und Services des Unternehmens inventarisieren**	**Geräteinventarisierung:** VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender, Oomnitza **API/Service-Inventarisierung:** Anwendungskonnektor von Cloudflare, Zscaler Private Access (ZPA)
	☐ **Breitbandinternet für Verbindungen zwischen Firmenzweigstellen nutzen**	Cloudflare Magic WAN, Cato Networks, Aryaka FlexCore
	☐ **Verfahren zur Protokollierung und Überprüfung der Aktivitäten von Mitarbeitenden für sensible Anwendungen einführen**	**Secure Web Gateway (SWG):** Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) **Security Incident and Event Monitoring (SIEM):** DataDog, Splunk, SolarWinds
	☐ **Das Abfließen sensibler Daten aus Anwendungen (z. B. PII, Kreditkarten, SSNs usw.) unterbinden**	Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)
	☐ **DevOps-Ansatz zur Durchsetzung von Richtlinien bei allen neuen Ressourcen anwenden**	Ansible, Puppet, Terraform
	☐ **Automatische Skalierung für On-Ramping-Ressourcen implementieren**	**Load Balancer:** Akamai, Cloudflare **Infrastruktur-Automatisierung:** Ansible, Puppet, Terraform

CLOUDFLARE

+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

REV:BDES-3584.2022AUG09