E-BOOK

CLOUDFLARE

Sieben Tipps für das mobile Arbeiten

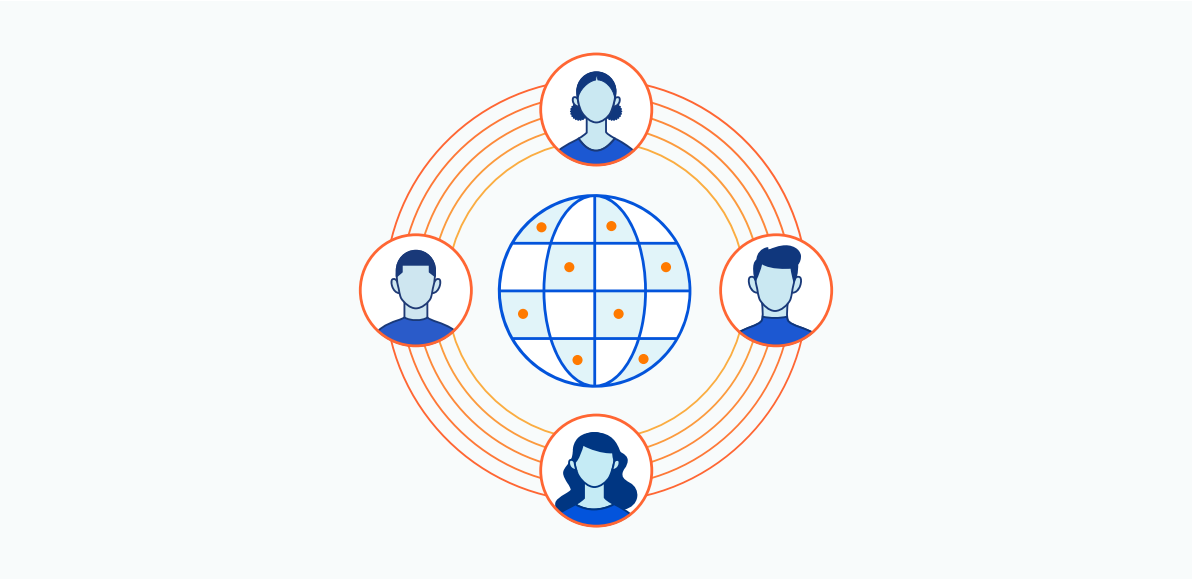
Sicherheit und Performance für das Büro der Zukunft

Moderne virtuelle Team sind vielfältig besetzt – nicht selten arbeiten interne Mitarbeiter mit externen Auftragnehmern und Kooperationspartnern zusammen. Trotzdem müssen alle Teammitglieder auf dieselben Tools zugreifen können. Und wenn Ihr Unternehmen entscheidet, von wo aus seine Belegschaft zukünftig arbeiten kann, müssen Sie wirksame Sicherheitskontrollen für die neuen Zugriffsorte der Mitarbeiter etablieren. Wie gelingt es Ihnen angesichts dieser Veränderungen, Ihre Firmendaten zu schützen, ohne die Performance zu beeinträchtigen?

Dieses E-Book stellt sieben bewährte Methoden vor, die dazu beitragen, dass die globalen Mitarbeiter leistungsstarker Unternehmen gut geschützt zusammenarbeiten können, ohne Abstriche bei der Produktivität machen zu müssen.

INHALT

EINLEITUNG



Die Zeiten, in denen Büroarbeit vornehmlich an den Firmenstandorten verrichtet wurde, sind lange vorbei. Damals war der Zugriff auf interne Systeme von einem anderen Ort aus eher die Ausnahme und erfolgte über ein VPN, das entsprechende Geschwindigkeitseinbußen mit sich brachte.

Mittlerweile hat sich das Bild grundlegend gewandelt. Die Mobilität und geografische Verteilung der Belegschaft hat sich drastisch erhöht und immer mehr Angestellte arbeiten heutzutage von zu Hause aus. Früher war es noch zielführend, Unternehmensressourcen durch einen schützenden Perimeter abzuschirmen, doch in Zeiten von SaaS, Cloud-Computing und mobilem Arbeiten ist dieser Ansatz wirkungslos. Das moderne Unternehmensnetzwerk basiert auf dem Internet und sein Schutz erfordert eine radikal neue Herangehensweise.

In diesem Leitfaden erhalten Sie grundlegende Informationen, mit denen Sie Ihr Unternehmen auf aktuelle und zukünftige Herausforderungen in Sachen Online-Sicherheit vorbereiten können. Sie lernen grundlegende Konzepte wie das Zero-Trust-Sicherheitsmodell kennen, werfen einen Blick auf neue Lösungen für alte Probleme und gewinnen die nötigen Kenntnisse, um Ihrem Team in dieser sich rasant wandelnden Bedrohungslandschaft eine sichere Zusammenarbeit zu ermöglichen.

KAPITEL 1

Netzwerksicherheit im Wandel

In letzter Zeit hat die Remote-Arbeit noch einmal rasant zugenommen, doch die Entwicklung moderner Teams hin zu mehr Mobilität und breiterer geografischer Verteilung hatte schon vorher eingesetzt. Schon lange ermöglicht das Internet weltumspannende Kooperationen über Landesgrenzen und geografische Gegebenheiten hinweg. Aber diese verstärkte Streuung stellte gleichzeitig die bisherige Grundannahme der Sicherheitskonzepte von IT-Teams infrage: die Vorstellung, dass Datenwege und -sicherheit vom physischen Standort des Mitarbeiters abhängen sollten.

In der Vergangenheit bedeutete Sicherheit, adäquate physische Sicherheitskontrollen an den Bürostandorten zu definieren und durchzusetzen: Ein Mitarbeiter musste sich an seinem Büroschreibtisch befinden, um sich im Netzwerk anmelden und auf die Anwendungen und Dienste zugreifen zu können, die er für seine Arbeit benötigte. Firewalls vor Ort filterten den Datenverkehr der Mitarbeiter und protokollierten die über das Netzwerk ein- und ausgehenden Anfragen. Und der Zugriff auf SaaS-Anwendungen wie Office 365 erfolgte über benutzerdefinierte private Links, die besonders schnelle Privatverbindungen über das Firmennetzwerk aufbauten.

Doch dann kam es weltweit zu einem rasanten Anstieg der Zahl der Mitarbeiter, die sich nicht mehr am Standort einloggten. IT-Teams mussten nun neue Wege finden, um Belegschaft und Kunden zusammenzubringen. Kürzlich hat Forrester Consulting im Rahmen einer von Cloudflare in Auftrag gegebenen Studie Entscheidungsträger im Bereich IT-Sicherheit befragt, welche Faktoren sich im Jahr 2020 am stärksten auf ihre Sicherheitsprogramme ausgewirkt haben – 52 % der Umfrageteilnehmer nannten das mobile Arbeiten.

Heute überlegen viele Arbeitgeber, wie sie die Mitarbeiter wieder in die Büros zurückholen können. In den meisten Fällen wird die neue Normalität wohl so aussehen, dass ein Teil der Belegschaft zurückkehrt, andere aber weiterhin von zu Hause aus arbeiten werden.

Angesichts der anstehenden Herausbildung dieses hybriden Arbeitsumfelds stehen Sicherheitsteams vor neuen Fragen:

- Wie lässt sich zukünftig auch beim mobilen Arbeiten ein sicherer Zugriff auf interne Ressourcen gewährleisten, ohne dass dabei Geschwindigkeitseinbußen in Kauf genommen werden müssen?
- Welche Sicherheitskontrollen müssen an den Standorten beibehalten werden und welche Investitionen sind zukünftig nicht mehr sinnvoll?
- Wie kann angesichts der Vielzahl der Verbindungsmöglichkeiten dafür gesorgt werden, dass die Netzwerkaktivitäten der Mitarbeiter transparent bleiben?
- Wie kann ein einheitliches Sicherheitsmodell aussehen und wie können beim Routing des Datenverkehrs unnötige Hops vermieden werden?

KAPITEL 1

Viele IT-Teams stehen angesichts dieser Fragen vor drängenden Herausforderungen, die sie wahrscheinlich nur mit ganz neuen Lösungsansätzen meistern können. Doch Veränderungen sind immer schwierig und oft ergeben sich dabei auch neue Möglichkeiten, ein Unternehmen besser aufzustellen. In diesem E-Book erfahren Sie mehr über neue Modelle im Bereich der Unternehmenssicherheit; außerdem geben wir Ihnen sieben bewährte Verfahren für die Implementierung dieser neuen Ansätze mit auf den Weg.

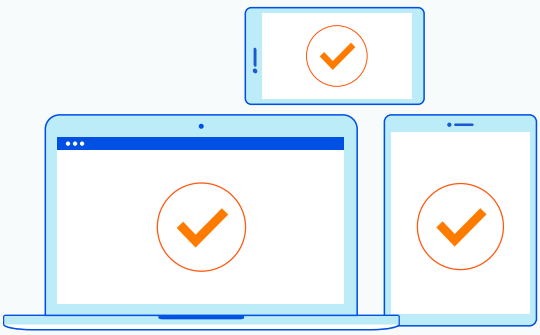
Das Büro von morgen: Ein Internetcafé

Vor dem Aufkommen des mobilen Arbeitens dienten die physischen Bürostandorte den Teams als Zentren, in denen sie sich gefahrlos vernetzen konnten. Die im öffentlichen Internet leicht verfügbaren Ressourcen galten demgegenüber als zu unsicher und zu langsam für den professionellen Einsatz. Dementsprechend erwies es sich auch als sinnvoll, private Direktverbindungen vom Standort zum Internet, zu SaaS-Applikationen und zu den Rechenzentren des Unternehmens einzurichten. Nicht weniger einleuchtend war außerdem die Installation von lokalen Firewalls als zusätzliche Verteidigungslinie.

Heute hingegen ziehen Entscheidungsträger im Bereich Netzwerk- und Sicherheitstechnologie die Sinnhaftigkeit dieser Investitionen in Zweifel und favorisieren stattdessen einen gerätebasierten Ansatz. Bei diesem Modell werden die einzelnen Büros nicht mehr als Komponenten einer Hub-and-Spoke-Architektur des Unternehmens betrachtet, sondern lassen sich eher mit Internetcafés vergleichen: Es gibt Wlan, aber für die nötige Sicherheit sorgt das Gerät des Mitarbeiters. Das heißt auch, dass die Mitarbeiter sich wirklich überall einloggen können und ihnen dabei stets die gleiche hervorragende Nutzererfahrung geboten wird.

Auf dem Weg zu einem gerätebasierten Sicherheitsmodell

Die wichtigste Voraussetzung der Freiheit, von jedem Ort aus risikofrei arbeiten zu können, sind sichere Mitarbeitergeräte. Wenn sie effizient verwaltet und geschützt werden, lassen sich auf ihnen viele Sicherheitsfunktionen umsetzen, die früher ausschließlich auf der Netzwerkebene zur Verfügung standen.



Bei einem gerätebasierten Modell wird das Equipment der Mitarbeiter mithilfe der folgenden Kontrollfunktionen vernetzt und geschützt:

- **Geräteverwaltung**: Mithilfe einer Geräteverwaltungsplattform sorgen Administratoren für die Registrierung der Rechner in einem Unternehmenssicherheitsprogramm. Die Mitarbeiter verwenden Firmengeräte und sind dabei an bestimmte Bedingungen gebunden; als Gegenleistung profitieren sie von erhöhter Konnektivität. Wenn Mitarbeiter das Unternehmen verlassen, können sensible Unternehmensdaten über das Verwaltungsprogramm sofort von dem Gerät gelöscht werden.
- **Schließen von Sicherheitslücken**: Ein zentrales Geräteverwaltungsprogramm sorgt dafür, dass die Betriebssysteme des Equipments automatisch mit den neuesten Updates gepatcht werden. Auch aktuelle Fehlerbehebungen werden automatisch aufgespielt.
- **Filterfunktionen**: Die Geräte senden ihren gesamten ausgehenden Traffic zur Analyse und Richtlinienanwendung über ein Secure Web Gateway (SWG). Unternehmensrichtlinien werden auf Geräteebene durchgesetzt, um die Nutzung von Schatten-IT-Anwendungen oder den zweckwidrigen Austausch von Informationen zu unterbinden.
- **Isolation**: Das Browsing erfolgt auf den Mitarbeitergeräten in einem isolierten Container bzw. einer sicheren Sandbox. Sollten Zero-Day-Bedrohungen auftreten, wirken sie sich niemals direkt auf das Mitarbeitergerät aus.
- **Virenschutz**: Die Geräte werden regelmäßig auf Viren und andere Schaddateien durchsucht. Wenn Viren entdeckt werden, werden sie isoliert und beseitigt.
- **Überwachung**: Der gesamte Datenverkehr des Geräts wird für die Triage des Administrators zentral protokolliert.

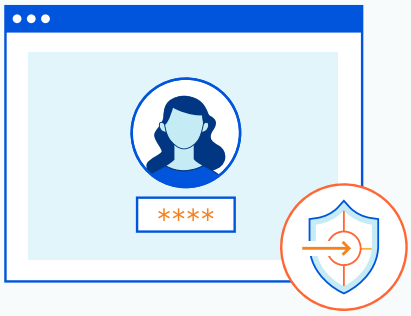
Tipp 1: Stellen Sie die Mitarbeitergeräte und nicht die Bürostandorte in den Mittelpunkt Ihrer Sicherheitsstrategie.

Professionelle Geräteverwaltung ist der erste Schritt hin zu moderner Zero-Trust-Sicherheit. Mit rundum geschützten Geräten wird auch Ihr Netzwerk sicherer.

Wenn Sicherheitsfragen auf der Geräteebene und nicht mehr in Abhängigkeit vom Netzwerkstandort adressiert werden, dann können die Mitarbeiter an jedem beliebigen Ort sicher und effizient arbeiten. Gleichzeitig werden die Firewalls und sonstigen Sicherheitsvorrichtungen, die bisher für den Schutz der Firmenstandorte unabdingbar waren, bedeutungslos.

Wenn der Idee des Internetcafés die Zukunft gehört, dann stellt sich die Frage, wie IT-Sicherheitsteams dieses Konzept umsetzen können.

KAPITEL 2



Zero-Trust-Sicherheit: Ein Modell für ein neues Zeitalter

Im Laufe der letzten Jahre hat im Bereich der Online-Sicherheit ein neuer Ansatz die Art und Weise verändert, wie sich Unternehmen in der modernen, vernetzten Welt schützen. Im Mittelpunkt steht dabei ein Konzept mit der Bezeichnung Zero-Trust-Sicherheit.

Bei dem traditionellen, auf VPNs basierenden Modell wird jedem Nutzer, der sich erfolgreich Zugriff auf eine interne Anwendung verschafft hat, automatisch vertraut. Bei Zero Trust hingegen muss der Anwender stets beweisen, dass er vertrauenswürdig ist. Wann immer eine Anfrage an eine Anwendung eingeht, wird sie unabhängig von Herkunft und Ziel einer Sicherheitsprüfung unterworfen.

Das Zero-Trust-Modell wurde zuerst von Google in einer 2016 veröffentlichten Forschungsarbeit vorgestellt. Darin beschreibt der Technikgigant, wie er sein internes Sicherheitsmodell so umgestaltet hat, dass „sowohl interne als auch externe Netzwerke vollständig als nicht vertrauenswürdig eingestuft werden“.[2] Seitdem haben viele andere führende Unternehmen Zero Trust übernommen und umgesetzt.

Bei Zero Trust handelt es sich nicht um ein Produkt oder eine Produktgruppe. Mit der Bezeichnung meint man vielmehr eine Denkweise, die zu bestimmten Entscheidungen hinsichtlich der Sicherheitsarchitektur führt. Im Zentrum steht dabei das Prinzip, dass kein Nutzer einen Vertrauensvorschuss erhält – auch dann nicht, wenn er sich bereits innerhalb des Netzwerks befindet.

Es gibt zwar bestimmte bewährte Herangehensweisen, an denen man sich bei der Umstellung auf das Zero-Trust-Modell orientieren sollte, aber im Kern geht es darum, die richtigen Gepflogenheiten zu etablieren, mit denen Sie spezifische Ziele erreichen können. Zum Beispiel werden Sie zwar mit der Einführung einer Multi-Faktor-Authentifizierung das Risiko eines bösartigen Zugriffs auf Ihre Anwendungen noch nicht vollständig beseitigen, aber Sie schaffen damit durchaus eine solide Grundlage für ein vorbildliches Sicherheitskonzept.

Tipp 2: Setzen Sie auf die Geräte als Schlüssel zu Ihren vertraulichen Daten.

Mit kontextabhängigen Zugriffskontrollen können Sie gewährleisten, dass bestimmte Applikationen und Daten nur über verwaltete Geräte aufgerufen werden können.

KAPITEL 2

Das Auslaufmodell VPN

VPNs haben sich ihren Platz in der Geschichte der Netzwerktechnik redlich verdient. Seit Jahrzehnten leisten sie einen Beitrag zur Sicherheit von Unternehmen und auch heute noch verlassen sich viele Firmen auf sie.

Doch leider weisen VPNs auch massenweise Schwachpunkte auf.

An erster Stelle steht dabei die mangelnde Benutzerfreundlichkeit: Es ist bekannt, dass sich die Bereitstellung und der Einsatz von VPNs immer wieder als schwierig erweisen. Angesichts von Konfigurationshürden, Unzuverlässigkeiten und alles andere als schlanken Login-Applikationen werden VPNs durch die Bank als lästig empfunden. In den IT-Abteilungen führt das nicht selten zu enormen Zusatzbelastungen.

Doch selbst wenn Ihr VPN einmal wie vorgesehen funktioniert, verursacht es Latenz, die sich manchmal nur als kleines Ärgernis erweist, zu anderen Zeiten die Arbeitsfähigkeit aber massiv beeinträchtigt. Die meisten VPNs sind so konzipiert, dass sie den gesamten Datenverkehr durch ein und dieselbe Leitung schicken. Wenn also Ihre Mitarbeiter mobil arbeiten, muss jedes Datenpaket zurück zu Ihrer VPN-Hardware in der Unternehmenszentrale geroutet werden, bevor es seine Reise zur vorgesehenen Zieladresse antreten kann. Insbesondere für global verteilte Teams verursacht das Latenz und damit Frustrationen.

Tipp 3: Ersetzen Sie Ihr VPN mit einem Zero-Trust-Zugriff.

Zero-Trust-Plattformen schützen Ihre Anwendungen vor unbefugten Zugriffen. Authentifizierungsanfragen werden nicht einfach nur anhand der Lokalisierung eines VPN bewertet, sondern auf der Grundlage von Identität und Kontext.

Und damit nicht genug: VPNs setzen ein Sicherheitsmodell ein, mit dem man neue Bedrohungen nicht mehr bekämpfen kann. Sobald es nämlich einem Nutzer gelungen ist, sich mit einem Unternehmens-VPN zu verbinden, gilt er als vertrauenswürdig: Nach der ersten erfolgreichen Anmeldung finden keine weiteren Sicherheitsüberprüfungen mehr statt. Zu dieser allzu niedrigen Hürde gesellt sich ein weiteres Sicherheitsproblem in Form einer unzureichenden Protokollierung: VPNs können zwar die IP-Adresse der Nutzer erfassen, nicht aber die Anwendungen oder Daten, auf die zugegriffen wurde. Das erschwert die Arbeit von Sicherheitsteams, wenn es darum geht, Protokolle von Benutzeraktivitäten für Compliance-Zwecke zu erstellen – und wenn wirklich einmal der Verdacht besteht, dass ein Konto missbraucht wurde, ist es fast unmöglich, die Aktivitäten des Angreifers nachzuvollziehen.

Laut einer Studie von Forrester Consulting hatten 46 % aller Unternehmen im Jahr 2020 beim Einsatz von VPNs mit Latenzproblemen zu kämpfen.[1]

Der erste Schritt hin zu einem Zero-Trust-Modell besteht darin, VPN-Verbindungen durch einen Zero-Trust-Netzwerkzugang (Zero Trust Network Access, ZTNA) zu ersetzen. Dies ist ein geeigneter Ansatz, um die genannten Herausforderungen zu bewältigen, indem man das Prinzip der geringsten Zugriffsrechte auf geschäftskritische Applikationen anwendet. Mit ZTNA können Sie jede Anwendung mit einem Microperimenter zu umgeben, Anwendungen hinter verschlüsselten Verbindungstunneln verbergen und jede Anfrage protokollieren: Sie vereinfachen Ihre Prozesse rund um das Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM), Ihre Entwickler haben mehr Zeit für andere Aufgaben und das Risiko eines Datenverlusts wird erheblich reduziert.

Wenn der Anwendungszugriff in Ihrem Unternehmen derzeit auf einem VPN basiert, empfehlen wir, ZTNA zuerst im Rahmen eines Pilotprojekts mit einer Handvoll Anwendungen und einer kleinen Benutzergruppe zu testen.

Man könnte zum Beispiel mit den folgenden Applikationen beginnen:

- Auf HTTPS basierende Anwendungen
- Anwendungen ohne Schutz durch bestehende SSO-Lösungen
- Anwendungen, die nur von 5-10 % der Mitarbeiter genutzt werden

Ist die Bereitstellung erfolgreich abgeschlossen, werden die Benutzer einen Unterschied feststellen, wenn sie sich bei ihren Anwendungen anmelden. Dokumentieren Sie positives Feedback und nutzen sie es, um Ihr Zero-Trust-Transformationsprojekt voranzubringen.

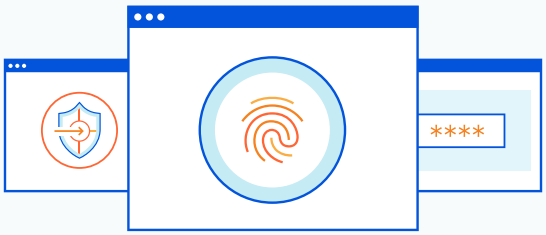
KAPITEL 3

Implementierung einer Zero-Trust-Anwendungskontrolle

Jedes Unternehmen steht vor der großen Herausforderung, zu gewährleisten, dass jedem Mitarbeiter genau diejenigen Tools und Daten zur Verfügung stehen, die er benötigt – nicht mehr, aber auch nicht weniger. Und je größer ein Team ist, desto komplexer gestaltet sich diese Aufgabe. Nicht weniger wichtig ist es, Zugriffsberechtigungen möglichst schnell wieder zu entziehen, wenn Mitarbeiter das Unternehmen verlassen oder die Zusammenarbeit mit Auftragnehmern endet.

Die Verwaltung dieser Zugriffskontrollen erweist sich für IT-Abteilungen auf der ganzen Welt oftmals als Herausforderung – und das Problem verschärft sich noch einmal deutlich, wenn jeder Mitarbeiter über mehrere Konten für verschiedene Tools in unterschiedlichen Umgebungen verfügt.

Mit dem richtigen Authentifizierungssystem verlaufen Onboarding und Offboarding viel reibungsloser. Jedes neue Teammitglied und jeder neue Auftragnehmer erhält schnell und unkompliziert die Zugangsrechte für die benötigten Anwendungen und kann mithilfe eines Launchpads problemlos darauf zugreifen. Verlässt jemand das Team, lässt sich eine einzelne Konfigurationsänderung auf alle Anwendungen übertragen, sodass keine Ungewissheit mehr zurückbleibt.



Sicherer Zugriff – auch für Auftragnehmer

Viele Unternehmen benötigen auch eine sichere Methode zur Verwaltung der Zugriffsrechte von Auftragnehmern und anderen Dritten. Langwierige On- und Offboarding-Prozesse können dazu führen, dass so mancher Vorteil, den man sich von einer Kooperation mit Externen versprochen hat, wieder verlorengeht. Und wie bei internen Mitarbeitern ist es auch bei Auftragnehmern und Drittanbietern wichtig, dass ihnen nur Zugriff zu denjenigen Daten und Tools gewährt wird, die sie wirklich brauchen, und dass ihnen die entsprechenden Rechte entzogen werden, sobald diese Voraussetzung nicht mehr gegeben ist.

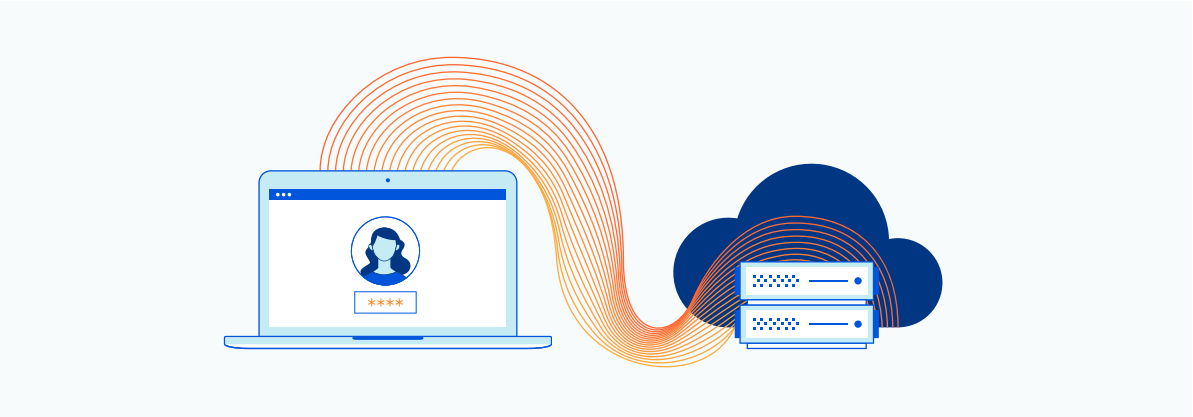
Moderne Authentifizierungslösungen erlauben Ihren Auftragnehmern, sich mit Konten anzumelden, die sie bereits haben – z. B. Gmail, Facebook oder LinkedIn. Was ihre Sicherheit, Protokollierungen und abgestuften Berechtigungen betrifft, bleiben diese Lösungen nicht hinter den Ergebnissen zurück, die Sie mit einer zeitaufwendigen Einrichtung von neuen Konten auf Ihren eigenen Systemen erzielen würden.

Manche Authentifizierungssysteme unterstützen auch Einmal-Zugangscodes: Der Auftragnehmer erhält einen temporären Code per E-Mail, der ihm befristeten Zugriff auf bestimmte Systeme ermöglicht. Auch diese Methode trägt dazu bei, die Workflows Ihrer Dienstleister zu vereinfachen, ohne dass Sie gleichzeitig Kompromisse bei der Sicherheit eingehen.

Tipp 4: Vereinfachen Sie den Zugriff Ihrer Auftragnehmer auf Ihre Systeme.

Mit den meisten IAM-Systemen gestaltet sich die Verwaltung externer Nutzer als schwierig. Bescheren Sie Ihren Auftragnehmern eine erstklassige Benutzererfahrung, indem Sie eine Plattform einsetzen, die ihnen den Zugriff erleichtert.

KAPITEL 4



Sicherheit für den ein- und ausgehenden Datenverkehr

Ähnlich wichtig wie die Einführung eines modernen Authentifizierungssystem ist es, die Kontrolle über den ein- und ausgehenden Datenverkehr des Netzwerks zu behalten.

In der Vergangenheit ging der gesamte Online-Traffic aller Zweigstellen an ein Rechenzentrum, das sich im Unternehmenssitz oder in dessen unmittelbarer Nähe befand. Administratoren gewährleisteten, dass der Datenverkehr eine sichere Hardware-Firewall durchlief, die alle Anfragen registrierte, einer Inline-SSL-Prüfung unterzog, mit einem DNS-Filter bearbeitete sowie das Firmennetzwerk vor Sicherheitsbedrohungen schützte. Diese Lösung funktionierte gut, solange die Mitarbeiter vom Büro aus auf geschäftskritische Anwendungen zugriffen und diese sich nicht in der Cloud befanden.

Doch durch das Aufkommen von SaaS wurde dieses Modell obsolet, denn nun waren Cloud-Applikationen der neue Standard für geschäftliche Anwendungen. Diese Verlagerung in die Cloud führte zu einer Zunahme der internetgebundenen Anfragen aus allen Niederlassungen. Auch die Kosten stiegen an. Das bisherige Modell, bei dem der gesamte Internetverkehr immer über zentrale Standorte geleitet wurde, passte nicht mehr zu dem Prozess der digitalen Transformation, den alle Unternehmen heute noch durchlaufen.

Besonders deutlich werden die Defizite des bisherigen Ansatzes, wenn der von geografisch breit gestreuten Niederlassungen und Mitarbeitern im Homeoffice erzeugte Netzwerk-Traffic lange Wege zur Hardware-Firewall zurücklegen muss, etwa weil sich die Zentrale des Unternehmens womöglich am anderen Ende der Welt befindet.

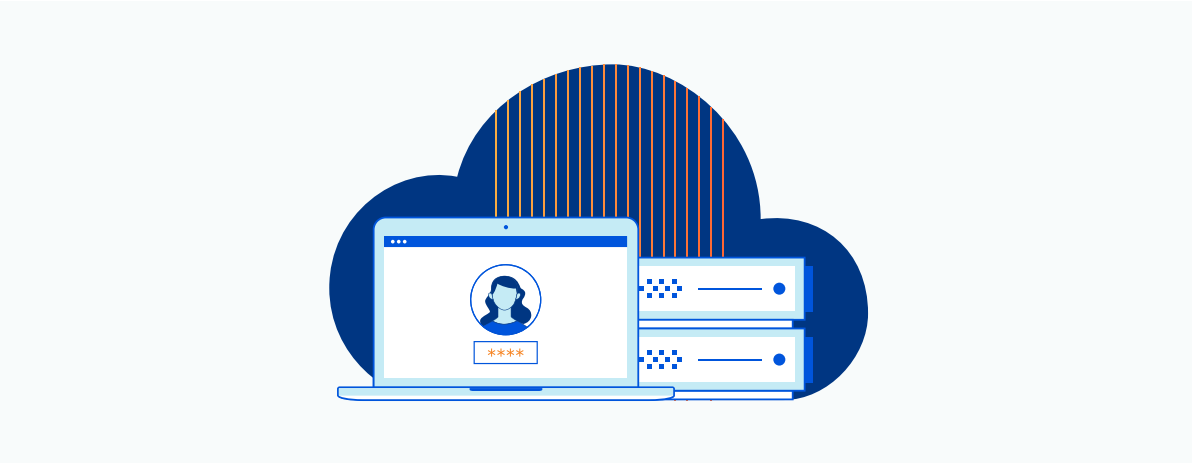
Ein weiteres Problem bei älteren Hardware-Firewalls besteht darin, dass sie nicht für die Bedrohungslandschaft des modernen Internets konzipiert wurden, die einem ständigen Wandel unterworfen ist.

Zum Beispiel kommen Monat für Monat rund 1,5 Millionen neue Phishing-Websites hinzu[3] und ältere Hardware-Firewalls können ihre statischen Regeln nicht schnell genug aktualisieren, um diese Phishing-Angriffe wirksam zu verhindern. Die sich ständig verändernden Sicherheitsbedrohungen im Internet überfordern die überkommenen Hardware-Geräte, was dazu führt, dass die Mitarbeiter gegen neue Bedrohungen nicht ausreichend geschützt sind.

Tip 5: Filtern Sie den Datenverkehr.

Legen Sie Unternehmensrichtlinien für den Internetzugriff fest und filtern Sie bösartige und unangemessene Websites heraus.

KAPITEL 4



Heute setzt man gerne auf **Secure Web Gateways**, um diesen unsteten Bedrohungen zu begegnen. Die Bereitstellung von SWG erfolgt meist in Form von SaaS-Sicherheitsplattformen, die den Traffic der Mitarbeitergeräte abfangen können. Dann wendet das Gateway Filterregeln auf den ein- und ausgehenden Datenverkehr an.

Anstatt sich bei der Abwehr von Bedrohungen auf ein statisches Modell verlassen zu müssen, können Administratoren über die SWG-Plattformen auf Tools zugreifen, die es ihnen erlauben, umgehend ihre eigene Regeln zu implementieren. Integrierte Funktionen zur Bedrohungserkennung und benutzerfreundliche Kategorien ermöglichen es ihnen, neue Gefahren ganz einfach abzuwehren, sobald sie auftauchen.

Über denselben Filtermechanismus können sie auch Richtlinien festlegen, die den Umgang der Benutzer mit Unternehmensdaten steuern.

Die Möglichkeiten sind schier endlos. Mithilfe von SWG-Richtlinien kann ein Administrator zum Beispiel ...

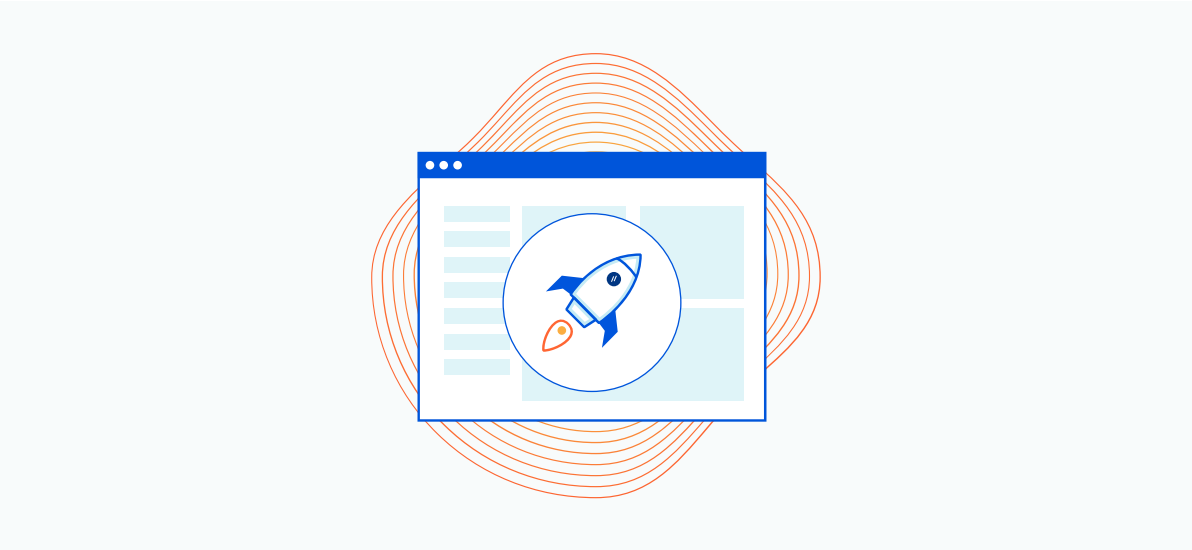
- als Phishing-Websites identifizierte Inhalte blocken
- Vorgänge in SaaS-Anwendungen protokollieren und überwachen
- Marketing-Mitarbeitern den Zugriff auf das Admin-Portal einer unternehmenseigenen CRM-Anwendung verwehren
- den Datenaustausch mit nicht genehmigten Cloud-Speicherdiensten wie zum Beispiel Dropbox begrenzen

Tipp 6: Protokollieren Sie alles.

Anhand von Aktivitätsprotokollen, die per zentralem Security Information and Event Management (SIEM) oder in einem Cloud-Storage-Bucket erfasst werden, können Sie bestimmte Muster im Datenverkehr besser verstehen und Auffälligkeiten erkennen.

Solange der zuständige Administrator geeignete Regeln und Richtlinien zum Schutz des Unternehmens festlegt, erweisen sich Secure Web Gateways als leistungsfähige Tools. Zwar wird es selbst mit den besten Vorkehrungen nie gelingen, wirklich jeden Angriff aus dem Internet von Ihrem Unternehmen fernzuhalten. Aber zumindest was neue Bedrohungen betrifft, kann sich isoliertes Browsing als letzte Verteidigungslinie bewähren.

KAPITEL 4



Ein neues Konzept: Browser-Isolation

Der Webbrowser ist diejenige Anwendung, mit der die Benutzer auf das gesamte Internet zugreifen, und damit möglicherweise auch auf Inhalte, die sich als schädlich erweisen können. Im Prinzip stellt er ein Einfallstor für fast alle Online-Systeme der Welt dar – das ist einerseits beeindruckend, andererseits aber auch sehr beunruhigend.

Gleichzeitig spielen Browser eine immer wichtigere Rolle. Über sie laufen schon jetzt die meisten Anwendungen, die wir benutzen, und dieser Anteil wird weiter steigen. Für viele Unternehmen ist ein Firmenlaptop heute im Grunde nichts anderes mehr als ein verwalteter Rechner zum Betrieb eines Web-Browsers.

Um die Daten zu schützen, die diese Geräte speichern oder abrufen, setzen immer mehr Unternehmen die sogenannte Browser-Isolierung ein. Sie bewirkt, dass der Browser selbst nicht auf dem Rechner ausgeführt wird, sondern auf einer virtuellen Maschine in der Cloud läuft. Und dadurch, dass er nicht mehr auf dem physischen Gerät betrieben wird, bleiben auch von ihm ausgehende Bedrohungen auf die virtuelle Maschine begrenzt.

Tipp 7: Isolieren Sie riskante Internet-Zugriffe.

Wehren Sie browserbasierte Exploits und Datensicherheitsverletzungen so früh wie möglich ab, damit die Geräte Ihrer Nutzer und Ihr Firmennetzwerk gar nicht erst ins Fadenkreuz der Angreifer geraten.

Gemäß dem Zero-Trust-Sicherheitsmodell gilt, dass eine Website, die ein Nutzer bereits 99-mal ohne Sicherheitsprobleme aufgerufen hat, beim hundertsten Mal trotzdem noch ein Risiko darstellen kann. Browser-Isolation ist eine Möglichkeit, dieses Prinzip in die Tat umzusetzen.

Es wäre vermutlich übertrieben, wenn Unternehmen sofort in jede verfügbare Zero-Trust-Technologie investieren. Doch indem sie sich zuerst auf kritische Schwachstellen konzentrieren, können sie ein Umdenken anstoßen, das auf längere Sicht zu höherer Sicherheit führt.

KAPITEL 5

Die Cloudflare-Lösung: Cloudflare for Teams

Cloudflare for Teams

Wenn Ihnen die in diesem E-Book beschriebenen Probleme bekannt vorkommen, ist es gut möglich, dass Cloudflare for Teams die Lösung ist, nach der Sie suchen.

Mit Rechenzentren in 200 Städten und über 90 Ländern betreibt Cloudflare eines der größten Netzwerke der Welt, das rund 25 Millionen Websites und Webapplikationen bereitstellt. Cloudflare bietet eine Vielzahl von Diensten zur Steigerung der Sicherheit, Performance und Zuverlässigkeit. Zu unseren Kunden gehören viele weltbekannte Marken und unter anderem auch ein Zehntel der Fortune-1000-Unternehmen.

Mit Cloudflare for Teams können Sie sich die Leistungsfähigkeit des globalen Edge-Netzwerks von Cloudflare zunutze machen, um Ihre Teams, Ihr Firmennetzwerk und Ihre Daten zu schützen.

Zero-Trust-Zugriff nutzen	Ersetzen Sie Ihre pauschalen Sicherheitsperimeter durch Überprüfungen jeder einzelnen Anfrage, die bei Ihren Ressourcen eingeht, und sorgen Sie für die Durchsetzung von Zero-Trust-Regeln, wann immer eine Verbindung zu Ihren Firmenanwendungen aufgebaut wird – unabhängig von Identität und Standort der Nutzer. Weitere Informationen zu Cloudflare Access
Internet-Traffic absichern	Gerade wenn sich die Bedrohungen im Internet schnell weiterentwickeln, ist es wichtig, dass Sie ihnen mit Abwehrmaßnahmen immer einen Schritt voraus sind. Cloudflare for Teams schützt Mitarbeiter vor Gefahren aus dem Internet und setzt Richtlinien durch, die verhindern, dass wertvolle Unternehmensdaten in die falschen Hände geraten. Weitere Informationen zum Cloudflare Gateway
Zero-Day-Angriffe durch Browser-Isolation stoppen	Wehren Sie browserbasierte Exploits und Datensicherheitsverletzungen so früh wie möglich ab, damit die Geräte Ihrer Nutzer und Ihr Firmennetzwerk gar nicht erst ins Fadenkreuz der Angreifer geraten. Weitere Informationen über Browser-Isolation

ENDNOTEN

1. Forrester Opportunity Snapshot: Eine Studie im Auftrag von Cloudflare, Oktober 2020
2. BeyondCorp: A New Approach to Enterprise Security – Google Research
3. Webroot Quarterly Threat Trends Report – Webroot