WHITEPAPER

Neuer Kurs für Anwendungszugriff:

So managen Sie eine moderne Belegschaft

Akamai

Zusammenfassung

Der Paradigmenwechsel, der in Unternehmenstechnologie und Unternehmen stattfindet, wird von Tag zu Tag spürbarer. Der Übergang zum Cloud Computing steht kurz vor dem Wendepunkt. Fusionen und Übernahmen haben zugenommen. Angesichts der wachsenden Anzahl von Endnutzern außerhalb der Unternehmensumgebung müssen IT-Abteilungen ein immer vielfältigeres, verteiltes und anspruchsvolles Nutzerökosystem bereitstellen.

Die Bereitstellung eines sicheren, anwendungsspezifischen Zugriffs auf Unternehmenssysteme und -daten ist heute wichtiger denn je – und anspruchsvoller.

Der herkömmliche zentralisierte Sicherheitsstack (z. B. VPNs, RDPs, Proxys) liefert Unternehmen Risiken aus, erhöht die Komplexität und verursacht Performanceprobleme. Und wenn Integrationsherausforderungen durch schnelle, kurzfristige Konfigurationen gelöst werden, ziehen sie Ihre IT-Ressourcen von vorausschauenden Initiativen ab und sorgen für technische Einbußen.

Dieses Whitepaper:

- *zeigt, wie sich Mitarbeiter, Geschäftsumgebung und IT verändern.*
- *untersucht die Herausforderungen bei der Bereitstellung eines sicheren Anwendungszugriffs mithilfe vorhandener Technologien.*
- *erörtert, warum eine Zero-Trust-Sicherheitsarchitektur Ihre Angriffsfläche in der modernen IT-Umgebung minimieren kann.*

Mit einer cloudbasierten Zero-Trust-Plattform, die an der Edge bereitgestellt wird, können Sie Nutzern einen angemessenen, intelligenten und anpassungsfähigen Zugriff mit der verlangten Einfachheit bieten. Und das auf dem Gerät ihrer Wahl, unabhängig davon, ob es sich im Governance-Bereich des Unternehmens befindet. Gleichzeitig kann Ihr Unternehmen die Angriffsfläche verkleinern und die Nutzer-Provisioning/-Deprovisioning, Fehlerbehebung, Verwaltung und Administration für Nutzer vereinfachen.

> *„Cloud Computing befindet sich an einem wichtigen Wendepunkt seiner Entwicklung. Während 20 % der Geschäftsprozesse bereits in die Cloud verlagert wurden, laufen 80 % der geschäftskritischen Workloads und sensiblen Daten aufgrund von Performance- und behördlichen Anforderungen immer noch auf firmeninternen Geschäftssystemen. Im Jahr 2019 wird der Prozentsatz dieser Workloads, die in der Cloud ausgeführt werden, auf über 40 % ansteigen …“*
>
> *– Roy Illsley, Distinguished Analyst, Ovum[1]*

Neue und sichere Wege für den Zugriff auf Anwendungen

Unternehmen sehen sich heute mit einer massiven Unterbrechung konfrontiert: bei der Bereitstellung von IT-Services, bei der Zusammensetzung ihrer Mitarbeiter und nicht zuletzt auch in Ihren Unternehmensstrukturen. Sie müssen ein vielfältiges Nutzerökosystem mit kalibriertem Zugriff auf Unternehmensanwendungen und -daten bereitstellen, die sich sowohl vor Ort als auch zunehmend in der Cloud befinden. Diese neuen IT- und Mitarbeiterstrukturen bedeuten, dass Unternehmen sich nicht mehr auf vorhandene Architekturen und Lösungen am Netzwerkübergang für den Anwendungs- und Datenzugriff verlassen können.

Ältere Zugriffslösungen und Sprichwörter wie „Vertrauen, aber überprüfen" sind problematisch. Herkömmliche VPNs, Proxys und Remote-Desktops erfordern von Natur aus das Vertrauen seitens des Unternehmens. Zwar wird ein Nutzer oder Gerät verifiziert, aber danach ist der Zugriff auf das gesamte Netzwerk offen. Die gesamte Sicherheitslast lastet auf dem Netzwerk; Nutzern wird sofort vertraut, sobald sie Zugriff haben. Anwendungen, Daten, Nutzer und Geräte wurden jedoch außerhalb des herkömmlichen Netzwerks verlegt. Ein netzwerkzentriertes Sicherheitsframework ist eigentlich unzureichend.

Selbst wenn Nutzer und Geräte, die Zugriff auf das Unternehmensnetzwerk anfordern, immer überprüft werden sollten, sollte ihnen niemals einseitig vertraut oder vollständiger Netzwerkzugriff gestattet werden, nur weil sie sich bereits innerhalb der Firewall befinden. Es steht zu viel auf dem Spiel. Unternehmen benötigen ein neues Zugriffsmodell, das ein Zero-Trust-Framework unterstützt.

Es sind mehrere Kräfte am Werk, die jeweils Auswirkungen auf die Anwendungs- und Datensicherheit des Unternehmens haben:

Neue Technologien

Die Einführung cloudbasierter Lösungen hat eine kritische Masse erreicht. Unternehmen jeder Größe und Art profitieren von den Vorteilen der Cloud und der Möglichkeit, Services jederzeit, überall, von jedem Gerät und auf Abonnementbasis zu nutzen. Sie sind dankbar, keine hohen Softwarelizenzgebühren und Wartungskosten zahlen, Hardware erwerben oder große IT-Teams einstellen zu müssen, um Systemimplementierung und -konfiguration, laufende Wartung und Verwaltung sowie Upgrades durchzuführen.

> *73 % der Unternehmen verfügen über mindestens eine Anwendung oder einen Teil ihrer Unternehmens-Computing-Infrastruktur in der Cloud.*[2]

Gleichzeitig müssen Unternehmen jedoch noch ihre firmeninternen Lösungen aufgeben. Die Mehrheit der Unternehmen verwendet eine hybride Umgebung mit mehreren Clouds und einer Kombination aus Architekturen vor Ort, Private Cloud und Public Cloud mit erstklassigen Ressourcen verschiedener Cloud-Anbieter. Hier müssen die Strategien für den Anwendungszugriff Schritt halten können.

Unternehmen, die ältere Systeme verwenden, führen häufig einen Backhaul des Cloud-Traffics über das WAN durch einen zentralen Sicherheitsstack durch und leiten den Traffic dann über direkte Verbindungen oder VPNs an den Infrastructure as a Service- und Internetanbieter zurück. Darunter leiden jedoch die Anwendungsperformance und das Nutzererlebnis, während Unternehmensrisiken und Kosten steigen – insbesondere, wenn Unternehmen ihre Stacks für unterschiedliche Standorte und Anbieter duplizieren. Unternehmen benötigen Zugriffslösungen, die den Technologiestack vereinfachen und die problemlose Einführung cloudbasierter Lösungen ermöglichen.

Die Belegschaft ändert sich

In den letzten Jahrzehnten hat sich viel verändert: Einzelpersonen bleiben während ihrer beruflichen Laufbahn nicht mehr nur bei einem einzigen Unternehmen und sitzen dort auch nicht von 9:00 bis 17:00 Uhr an ihren Schreibtischen. Viele Mitarbeiter sind nicht einmal mehr angestellt. Das Personal ist heute eine Mischung aus internen und externen Ressourcen, die sowohl vor Ort als auch remote arbeiten.

Mitarbeiter arbeiten zunehmend:

Mobil: *Mitarbeiter sitzen nicht mehr ausschließlich an Schreibtischen in ihren Büros. Sie verbinden sich von zu Hause, vom Flughafen, im Flugzeug oder Zug, während sie im Urlaub, in einem Hotel oder Café sind – egal, wo das Leben oder Geschäft sie gerade hinführt – mit dem Unternehmensnetzwerk.*

Remote: *Immer mehr Mitarbeiter arbeiten für einen größeren Teil der Arbeitswoche remote. Eine Studie von IWG aus dem Jahr 2018 ergab, dass 70 % der Mitarbeiter mindestens einen Tag in der Woche Telearbeit machen, während 53 % mindestens die Hälfte der Woche remote arbeiten.[3] Laut Glassdoor verfügen einige Unternehmen mittlerweile zu 100 % über virtuelle Mitarbeiter.[4] Und derzeit wird sogar diese Kultur erwartet: Viele würden keinen Job übernehmen, bei dem sie ohne eine erhebliche Gehaltserhöhung immer in einem Büro arbeiten müssten.*

Freiberuflich: *Viele Arbeitskräfte sind überhaupt keine Betriebsangehörigen. Laut einer Studie von 2018 sind ungefähr 56,7 Millionen US-Bürger freiberuflich tätig – eine Zunahme von 3,7 Millionen nur in den letzten fünf Jahren.[5] Mithilfe dieser Freiberufler können Unternehmen spezialisierte Mitarbeiter schnell unter Vertrag nehmen und einsetzen, um ihre Geschäftsziele zu erreichen.*

Über Dritte: *Viele Unternehmen verlassen sich bei der Bereitstellung ihrer Waren und Dienstleistungen auf ein digitales Ökosystem aus Anbietern, Lieferanten, Partnern und sogar Kunden. Einige befinden sich möglicherweise in Regionen, die eine Zugriffs- oder Sicherheitsherausforderung darstellen, z. B. China, während andere möglicherweise auch mit einem Mitbewerber des Unternehmens zusammenarbeiten.*

Alle diese Gruppen gelten als Unternehmensnutzer und benötigen Zugriff auf Unternehmensanwendungen und -daten, unabhängig von ihrem Standort, dem verwendeten Gerät oder dem Kontrollbereich der IT-Abteilung. Unternehmen können es sich jedoch nicht leisten, diesen Nutzern uneingeschränkten Zugriff zu gewähren, sobald sie sich im Netzwerk befinden. Sie dürfen nur Zugriff auf die spezifischen Anwendungen und Daten gewähren, die für einen bestimmten Job erforderlich sind.

Anspruchsvolle Nutzer

Auch wenn die Belegschaft immer vielfältiger geworden ist, hat die IT-Konsumerisierung die Anforderungen der Endnutzer erhöht.

Die Grenzen zwischen privatem und beruflichem Leben der modernen Belegschaft verschwimmen zunehmend. Nutzer recherchieren, wählen und kaufen ihre eigenen Geräte, und sie erwarten, dass sie diese Geräte für den Zugriff auf die Anwendungen und Daten des Unternehmens verwenden können. Unternehmensgeräte und private Unterhaltungselektronik, die mit dem Unternehmensnetzwerk verbunden werden, werden auch für den Zugriff auf nicht verwaltete Onlinedienste wie webbasierte E-Mails, Datenspeicherplattformen, Tools zur Zusammenarbeit und Dateifreigabe, Instant-Messaging-Dienste und soziale Netzwerke verwendet – alles außerhalb der Kontrolle und Sichtweite von IT-Teams.

Außerdem erwarten Mitarbeiter, dass Unternehmensanwendungen die gleichen einfachen, praktischen Erlebnisse bieten, die ihre Verbraucheranwendungen bieten. Um diese Nutzeranforderungen zu erfüllen, muss die IT einen nahtlosen, effizienten und sicheren Zugriff auf ihre Anwendungen und Daten von jedem Gerät aus ermöglichen, ohne den Nutzer in komplexe Prozesse zu verwickeln.

Fusionen und Übernahmen

Unternehmen ändern ihre Größe und strategische Ausrichtung schnell. Die Zahl der Fusionen und Übernahmen nimmt in der heutigen Unternehmenslandschaft zu. 79 % der Führungskräfte erwarten, dass die Anzahl der Geschäftsabschlüsse und die Größe der Transaktionen im kommenden Jahr zunehmen werden.[6] Damit diese Fusionen und Übernahmen überhaupt möglich und einfacher zu realisieren sind, müssen Unternehmen in der Lage sein, ihre Infrastrukturen schnell und einfach zu konsolidieren. Cloudbasierte Architekturen und Lösungen ermöglichen dieses Wachstum und diese Veränderung und reduzieren Komplexität und Kosten. Drastische Aktualisierungen der IT-Stacks sind dabei nicht nötig: Hardware, Software, Netzwerkstacks, IAM-Plattformen, Konfigurationen für den Nutzerzugriff und vieles mehr. Gleichzeitig müssen Unternehmen Standardsicherheitskontrollen auf alle vorhandenen und neu erworbenen Ressourcen anwenden.

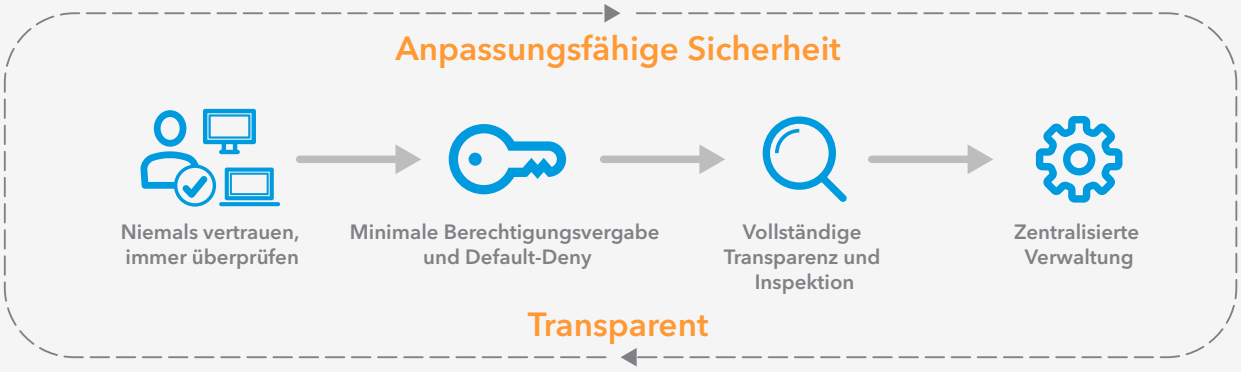
79 % der Führungskräfte sind der Ansicht, dass die Anzahl und der Umfang von Fusionen und Übernahmen im nächsten Jahr steigen werden.

Sicherheit durch eine Zero-Trust-Sicherheitsarchitektur

Wie wir gesehen haben, muss eine Zugriffslösung für Unternehmen jedem Mitarbeiter, unabhängig von den Umweltfaktoren, sicheren Zugriff auf relevante Unternehmensanwendungen und -daten gewähren. Doch aufgrund der Vielfalt Ihres Nutzerökosystems und der Realität der heutigen Bedrohungslandschaft kann dieser Zugriff nicht mehr nur ein „Alles-oder-Nichts"-Angebot sein.

Während eine Führungskraft über die Berechtigung zum Zugriff auf vertrauliche Prognosen und Pläne verfügen sollte, sollte das ein Drittanbieter oder ein Auftragnehmer auf untergeordneter Ebene nicht. Und wenn Malware die externen Firewallschutzmaßnahmen durchbricht, darf der Angreifer auf keinen Fall auf Systeme und Daten im gesamten Unternehmen zugreifen können. Ihr Unternehmen muss die Kontrolle über Anwendungen und Daten sorgsam abstimmen.

Um die Anforderungen des modernen Zugriffs zu erfüllen, ist ein Zero-Trust-Sicherheitsansatz erforderlich. Zero Trust implementiert eine „Überprüfen, niemals vertrauen"-Richtlinie. Damit haben autorisierte Nutzer und Geräte nur Zugriff auf die von ihnen benötigten internen Anwendungen und nicht auf das gesamte Unternehmensnetzwerk. Jede Zugriffsanfrage wird authentifiziert und autorisiert, bevor Anwendungen oder Daten bereitgestellt werden. Dieser Zugriff auf Anwendungsebene ist vorübergehend. Im Gegensatz zu älteren Systemen wie herkömmlichen VPNs kontrolliert ein Zero-Trust-Sicherheitsframework alle direkten Pfade zu Anwendungen.



Grenzen der herkömmlichen Zugriffskontrolle

Unternehmen verwenden häufig VPNs und eine Vielzahl von virtuellen oder Hardware-Appliances, z. B. Load Balancer, VPN-Konzentratoren, Application Delivery Controller und Proxys, um den Zugriff der Mitarbeiter zu kontrollieren. Der Versuch, Zugriff über diesen veralteten zentralisierten Sicherheitsstack bereitzustellen, ist ineffizient, setzt das Unternehmen aufgrund von Integrationsherausforderungen mehr Bedrohungen aus und entzieht IT-Ressourcen von vorausschauenden Initiativen.

Unternehmen, die sich zum Schutz der Unternehmensanwendungen auf ein Netzwerk verlassen, fordern das Schicksal heraus. Die Angreifer von heute sind geschickt darin, durch Hacking oder Social Engineering in das Unternehmen einzudringen. Und gestohlene Anmeldedaten ermöglichen Kriminellen einen einfachen Zugriff. Sobald sie sich innerhalb des Netzwerks befinden, können sie Regeln nutzen, durch die Nutzern standortabhängig implizit vertraut wird. Darüber hinaus können herkömmliche Netzwerkressourcen Nutzer und Geräte, die außerhalb des Kontrollbereichs des Unternehmens betrieben werden, nicht sichern, und auch cloudbasierte Anwendungen können nicht angemessen gesichert werden.

Bei der Entwicklung traditioneller appliancebasierter Firewalls und Gateways wurde die Cloud nicht berücksichtigt. Da cloudnative Sicherheits- und Zugriffskontrollen fehlen, sind IT-Teams sehr konservativ, wenn sie Partnern, Lieferanten, Kunden – sogar Mitarbeitern – Zugriff auf neue Cloudservices gewähren. Dies könnte einen breiten, lateralen Netzwerkzugriff bedeuten.

Diese herkömmlichen Zugriffslösungen stellen folgende Herausforderungen dar:

Komplexität und Kosten der Integration

Unternehmen benötigen einen Stack, der aus vielen Systemen besteht, um das VPN zu unterstützen und Konnektivität, Onboarding, Offboarding und allgemeine Überwachung bereitzustellen. All diese Komponenten lassen sich nur schwer integrieren. Unternehmen, die schnelle, einfache und provisorische Konfigurationen zur kurzfristigen Integration verwenden, riskieren langfristig eine umfangreiche – und teure – Verwaltung sowie eine erneute Integration. Alternativ können sie im Voraus investieren, um einen zusammenhängenden Stack zu konfigurieren, der möglicherweise länger betriebsbereit bleibt, um technische Schulden zu vermeiden. Letztendlich haben sie jedoch Zeit und Geld in eine Sicherheitslösung investiert, durch die das Unternehmen Risiken ausgesetzt wird.

Außerdem müssen diese Stacks Redundanz und eine hohe Verfügbarkeit über die verschiedenen Regionen und Rechenzentren hinweg aufweisen. Sie müssen jede dieser Komponenten an jedem Standort separat erwerben, installieren, konfigurieren und bereitstellen, was zu höheren Kapital- und Betriebskosten führt. Zur Erweiterung des Schutzes auf Cloudanwendungen führen Unternehmen häufig einen Backhaul des Cloud-Traffics über das WAN durch einen zentralen Sicherheitsstack durch und leiten den Traffic dann über direkte Verbindungen oder VPNs an den Infrastructure as a Service- und Internetanbieter zurück. Dies führt nicht nur zu noch mehr Komplexität und höheren Kosten, sondern beeinträchtigt auch die Performance.

64 %

der weltweiten IT-Budgeterhöhungen werden zur Aufrüstung veralteter IT-Infrastruktur verwendet.[7]

Zeitaufwändige Verwaltung

Mit zunehmender Anzahl der zu schützenden Anwendungen und der Anzahl der verteilten, anspruchsvollen Nutzer steigt auch der Verwaltungsaufwand. Administratoren müssen mehr Zeit damit verbringen, diese komplexen Sicherheitsstacks intern zu verwalten, fortlaufend zu überwachen, Fehler zu beheben und Patches und Upgrades anzuwenden. Jedes Mal, wenn sie das Netzwerk ändern oder eine Firewall-Regel aktualisieren, muss die IT-Abteilung mit einem brüchigen Netzwerkstack kämpfen. Und natürlich sind IT-Ressourcen begrenzt; die Zeit, die zur Verwaltung herkömmlicher, unhandlicher Zugriffstacks aufgewendet wird, lenkt von anderen Initiativen ab.

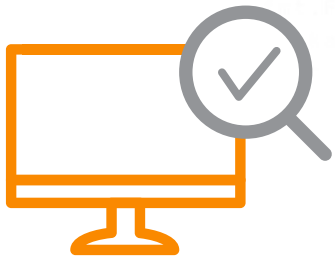
Schlechtes Nutzererlebnis

Herkömmliche VPNs und andere ältere Technologien sind anfällig für Verbindungsfehler, Latenz und Timeouts, was zu einer geringen Akzeptanz von Anwendungen und einer Flut von Helpdesk-Tickets führt. Das Fehlen eines nahtlosen Single Sign-on (SSO) für alle Anwendungen, einschließlich Software as a Service, führt zu Frustrationen bei den Nutzern und beeinträchtigt die Produktivität, wenn sie Passwörter erneut eingeben müssen. Wenn unzusammenhängende Authentifizierungs- und Autorisierungsprozesse den Nutzerzugriff fälschlicherweise verweigern, werden sowohl Nutzer als auch IT-Teams zur Fehlerbehebung aufgerufen. Zudem versuchen Nutzer, das Problem zu umgehen, wodurch das Unternehmen möglicherweise einem zusätzlichen Risiko ausgesetzt wird.

Schlechte Sicherheit

Herkömmliche VPNs stellen naturgemäß ein Loch in der Netzwerkfirewall dar. Sie wurden in erster Linie dafür entwickelt, die interne Infrastruktur eines Unternehmens über externe, nicht vertrauenswürdige Netzwerke zu verbinden – nicht für Unternehmenssicherheit und Datenschutz. Sie bieten in der Regel uneingeschränkten Netzwerkzugriff. Wenn also ein Sicherheitsverstoß auftritt, können Angreifer seitlich auf Anwendungen und Daten zugreifen, die über die zulässigen Richtlinien des Unternehmens hinausgehen.

Klassischen VPNs fehlt es außerdem an nötiger Intelligenz. Häufig können sie ein kontinuierlich adaptives Go/No Go basierend auf Multi-Faktor-Authentifizierung (MFA) nicht bereitstellen. Stattdessen prüfen sie, ob die Anmeldedaten korrekt oder falsch sind. Außerdem können VPNs das Geräteprofil nicht überprüfen, sodass sie nicht bestätigen können, ob das Gerät den Integritätsstandards entspricht, bevor es eine Verbindung mit dem Netzwerk herstellen kann.



Das Geräteprofil muss überprüft werden, bevor der Zugriff gewährt wird.

Was Sie bei Ihrer Lösung beachten sollten

Unternehmen benötigen eine Zugriffslösung, die reibungslos skaliert sowie schnell konfiguriert und bereitgestellt werden kann. Eine cloudbasierte Lösung, die an der Edge bereitgestellt wird, ist daher ideal. Die Lösung sollte sich problemlos in andere Sicherheitslösungen integrieren lassen und ein nutzerfreundliches, konsistentes Nutzererlebnis bieten. Darüber hinaus muss eine moderne Zugriffslösung Sicherheitsrisiken reduzieren, Transparenz der Netzwerkaktivität bieten und die laufende Verwaltung sowie Administration vereinfachen.

Security as a Service an der Edge

Eine cloudnative Lösung, die alle eingehenden Firewallports schließt und über einen zentralen Kontrollpunkt verfügt, isoliert alle Anwendungen vom Internet und von öffentlichen Bedrohungen. Wenn Sicherheitsfunktionen an der Edge bereitgestellt werden, sind sie nicht nur skalierbar, sondern auch näher an den Nutzern als eine zentralisierte Cloudlösung. Dadurch werden Bedrohungen näher am Ursprungspunkt entschärft und die Performance und Sicherheit der Endnutzer verbessert.

Diese Sicherheitsfunktion sollte eine gegenseitig authentifizierte TLS-Verbindung (Transport Layer Security) innerhalb Ihres Rechenzentrums oder Ihrer Cloud verwenden, damit dem Nutzer erlaubte Anwendungen ohne unsichere Tunnel oder einen eindeutigen Pfad für Malware direkt zur Verfügung gestellt werden. Nutzer sollten über einen beliebigen Browser und ein beliebiges Gerät auf Anwendungen zugreifen können.

Cloudbereitstellung bedeutet, dass Ihr Unternehmen nicht mehr einen komplexen Gerätestack installieren muss, um jedes Rechenzentrum zu schützen oder den Backhaul Traffic zur Authentifizierung an einen zentralen Ort zu übertragen. Stattdessen profitieren Sie von einem einzelnen Service in der Cloud zum Schutz all Ihrer Anwendungen, Daten, Nutzer und Geräte. Dadurch wird der Betrieb rationalisiert, sodass Sie mehr aus Ihren vorhandenen IT-Ressourcen herausholen können.

Einfache Integration mit anderen Sicherheitslösungen

Um die Sicherheit zu erhöhen und gleichzeitig den Zugriff zu ermöglichen, sollte die Lösung den Zugriffstechnologiestack auf einen einzigen Service reduzieren, der Datenpfadschutz, SSO, Identitäts- und Zugriffsverwaltung, Anwendungssicherheit, Transparenz und Administration bietet. Durch eine solche integrierte Lösung ist es nicht mehr erforderlich, eine komplexe Verschmelzung von Geräten zu installieren. Auch gehören Wartezeiten bei der Sicherung der einzelnen Rechenzentren der Vergangenheit an. Außerdem können Nutzer über beliebige Geräte auf Anwendungen zugreifen, ohne dass hierfür zusätzliche Software wie VPNs oder Browser-Plug-ins erforderlich wären.

Nahtlose SSO- und MFA-Funktionen sowie eine konsistente Nutzeroberfläche tragen dazu bei, die Anforderungen der modernen Belegschaft zu erfüllen.

Nutzerfreundlichkeit und einheitliches Nutzererlebnis

Im Umgang mit anspruchsvollen Nutzern müssen Sie unpraktische Prozesse entfernen. Suchen Sie nach einer Lösung, die mehrere Passwörter überflüssig macht und einen einfachen Zugriff über ein zentrales Webportal bietet. Nutzer sollten sich über SSO nahtlos bei allen Anwendungen anmelden können, die sie benötigen, und zwar auf jedem Gerät und von überall aus. Sie sollten außerdem die Möglichkeit haben, zur Erhöhung der Sicherheit einfache, bequeme MFA bereitzustellen, ohne dass Nutzer sich an komplizierte Anmeldedaten erinnern und diese wiederholt eingeben müssen. Eine nutzerfreundliche Lösung mit einer konsistenten Nutzeroberfläche beschleunigt die Nutzerproduktivität, erhöht die Anwendungsakzeptanz und reduziert gleichzeitig die Anzahl der Helpdesk-Tickets.

Sicherheitsrisiko vermindern

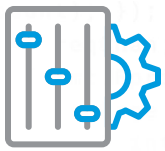
Der Anwendungszugriff, den jeder Nutzer benötigt, ist in der Regel ein Bruchteil dessen, was ein älterer VPN tatsächlich gewährt. Dieser irrelevante Zugriff stellt ein erhebliches, vermeidbares Risiko dar. Schlimmer noch: Nutzer greifen nur selten von nur einem Gerät aus auf das Netzwerk zu. Und damit wir die Angriffsfläche immer größer.

Die Lösung sollte nicht nur die Person authentifizieren und autorisieren, die Zugriff auf jede Anwendung anfordert, sondern auch das Gerät und den Kontext, in dem sie den Zugriff anfordert. Die Lösung sollte zuerst die Firewall oder Sicherheitsgruppe für sämtlichen eingehenden Traffic sperren und die IP-Adressen der Anwendungen vom Internet abschirmen. Dann sollte die Identität jedes Nutzers/Geräts und das Geräteprofil des Endpunkts über MFA zuverlässig validiert werden. Schließlich sollten Nutzer ständig basierend auf Identität, Gerät und Kontext, wie z. B. Standort, Uhrzeit, Authentifizierungsstatus, Gruppenmitgliedschaft und weitere Faktoren, überprüft werden. Diese Methoden verringern die Sicherheitsrisiken in Ihrem Unternehmen erheblich, indem sie die Angriffsfläche minimieren.

Mehr Transparenz

Ihr Unternehmen muss wissen, wer wann auf Ihr Netzwerk zugreift. Dies vereinfacht die Identifizierung echter Bedrohungen und reduziert False Positives, die bereits überlastete Sicherheitsressourcen verbrauchen. Das Managementportal sollte Transparenz bieten, indem es der IT einen zentralen Ort bereitstellt, an dem sie auf detaillierte Audit-, Kontroll- und Complianceberichte zugreifen können. Alternativ sollte es in Ihre vorhandenen SIEM-Tools (Security Information and Event Management) integriert werden.

80 %



der IT-Experten berichten, dass sie die Hälfte ihrer Zeit mit der Nachbearbeitung von Softwareprojekten verbringen.[8]

Einfachere Verwaltung und Administration

Die ideale Lösung reduziert die Belastung der IT und gibt ihnen Zeit für andere strategische Initiativen. Aus diesem Grund müssen IT-Mitarbeiter keine zusätzliche Software mit VPNs und Browser-Plug-ins installieren. Optimierte Authentifizierungs- und Autorisierungsprozesse für Nutzer und Geräte durch nahtloses SSO und MFA können Helpdesk-Anfragen wegen vergessener Passwörter, gesperrter Geräte oder Problemen mit dem Anwendungszugriff minimieren. Eine verbesserte Netzwerktransparenz beschleunigt die Erkennung echter Bedrohungen und reduziert False Positives. All diese Funktionen helfen der IT, schneller auf Sicherheitsvorfälle zu reagieren.

Schnelleres Nutzer-Provisioning und -Deprovisioning

Jeden Tag müssen Unternehmen ihr vielfältiges Nutzerökosystem mit sehr spezifischem Anwendungszugriff bereitstellen. Darüber hinaus müssen Unternehmen, die Fusionen und Übernahmen durchführen, schnell große Nutzergruppen in ihre vorhandenen und neu erworbenen Assets integrieren und gleichzeitig angemessene Sicherheitskontrollen sicherstellen.

Um die Belastung der IT zu reduzieren, sollte eine Lösung Sicherheitsexperten ermöglichen, neue Anwendungen zu installieren und Nutzern innerhalb von Minuten über ein einziges Webportal bereitzustellen, ohne Änderungen an Netzwerkattributen wie Firewallregeln oder IP-Adressen-Whitelists vorzunehmen.

Darüber hinaus sollte die IT mithilfe der Lösung einfach und schnell Richtlinien festlegen können, die Nutzer an bestimmte Anwendungen und Geräte binden, ohne Hardware-Upgrades und mühsame Änderungen am Netzwerk vornehmen zu müssen. Um optimale Sicherheit zu gewährleisten, sollten die Richtlinien Umgebungsfaktoren (Standort, Tageszeit usw.) sowie das Geräteprofil berücksichtigen (d. h. ob der Virenschutz aktuell ist oder EDR/EPP-Technologien (Endpoint Detection and Response)/(Endpoint Protection Platform) eingesetzt werden). Durch einfaches Nutzer-Provisioning und -Deprovisioning entfällt der Aufwand für die Implementierung aller Hardware- und Softwarekomponenten, die zur Bereitstellung des Zugriffs auf ein VPN erforderlich sind.

Fazit

Mit der Weiterentwicklung von Anwendungsplattformen und Mitarbeitern – und deren Struktur – benötigen Unternehmen eine Zugriffslösung, die mithalten kann. Unternehmen können es sich nicht mehr leisten, allen authentifizierten Nutzern vollständigen Zugriff auf das Netzwerks zu gewähren.

Eine Zero-Trust-Sicherheitsarchitektur, die an der Edge betrieben wird, kann Ihren vielfältigen, verteilten und anspruchsvollen Mitarbeitern einen korrekt kalibrierten Zugriff sowie ein komfortables und optimiertes Nutzererlebnis bieten – auf jedem Gerät, an jedem Standort, innerhalb oder außerhalb des Kontrollbereichs der IT. Und da die Lösung Helpdesk-Tickets minimiert, das Nutzer-Provisioning/-Deprovisioning vereinfacht, die Identifizierung von Bedrohungen beschleunigt und die laufende Verwaltung und Administration vereinfacht, hat die IT mehr Zeit für zukunftsorientierte strategische Initiativen.

Weitere Informationen zur Sicherung des Anwendungszugriffs in modernen Unternehmen und zur Unterstützung, die die cloudbasierte, an der Edge bereitgestellte Lösung von Akamai bieten kann, finden Sie unter akamai.com/eaa.

Weitere Informationen

QUELLEN

1) https://www.prnewswire.com/news-releases/ibm-unveils-worlds-first-multicloud-management-technology-300731206.html
2) https://www.idg.com/tools-for-marketers/2018-cloud-computing-survey/
3) https://www.cnbc.com/2018/05/30/70-percent-of-people-globally-work-remotely-at-least-once-a-week-iwg-study.html
4) https://www.glassdoor.com/blog/100-percent-remote-companies/
5) https://www.slideshare.net/upwork/freelancing-in-america-2018-120288770/1
6) https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-mna-trends-report-2019-us-dealmaker-optimism-hits-three-year-high.html
7) https://www.spiceworks.com/marketing/state-of-it/report/
8) https://www.geneca.com/why-up-to-75-of-software-projects-will-fail/