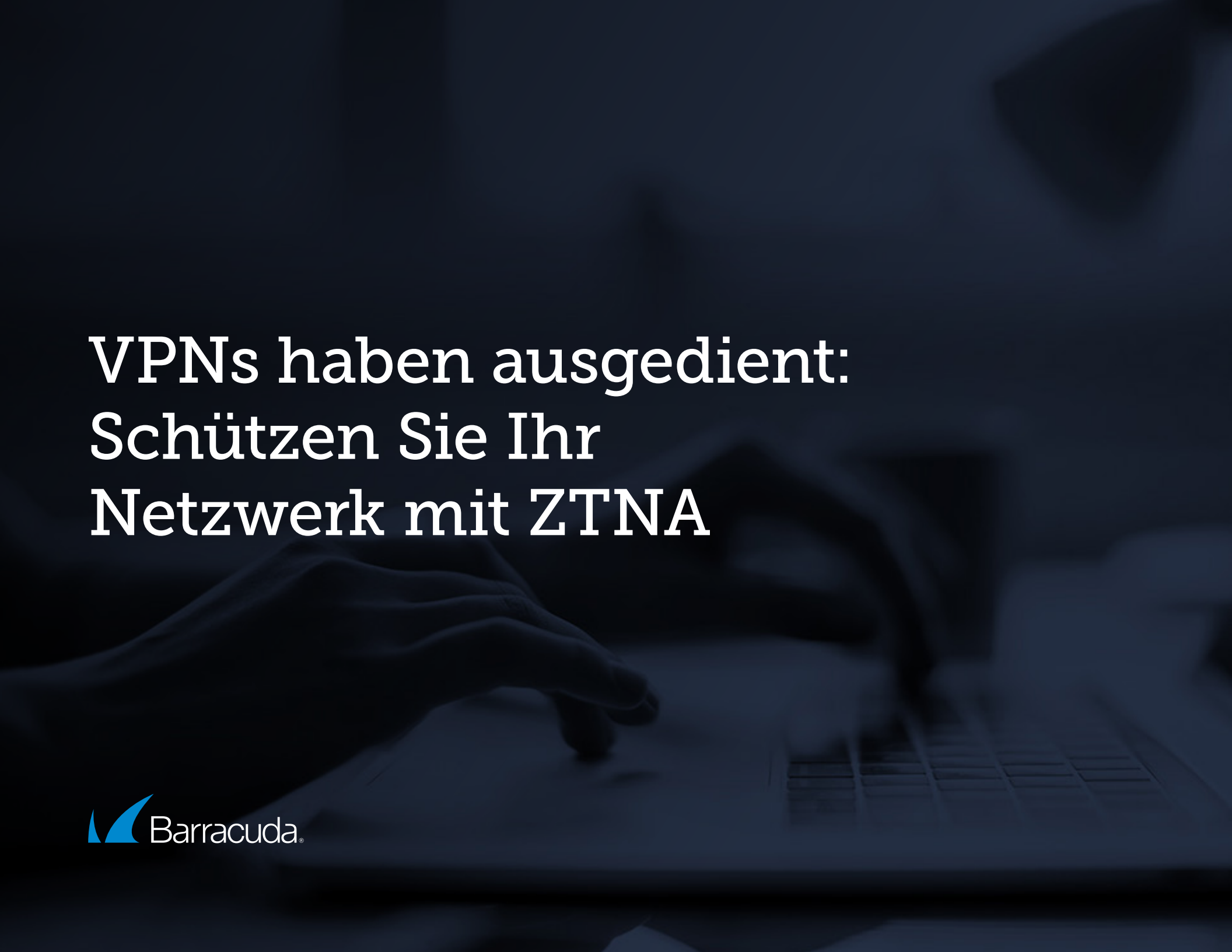

VPNs haben ausgedient: Schützen Sie Ihr Netzwerk mit ZTNA

Barracuda

VPNs gestern und heute

Seit dem Aufkommen des Internets und dem breiteren Zugang zu Informationen und Geräten, versuchen Sicherheitsorganisationen, damit verbundene Geräte und Benutzer vor einer steigenden Anzahl böswilliger Online-Akteure zu schützen. Genau zu diesem Zweck wurde 1996 das Virtual Private Network (VPN) geschaffen, um die Verbindung zwischen dem Gerät eines Benutzers und dem Internet zu sichern. Ursprünglich hauptsächlich von Unternehmen genutzt, sind VPNs inzwischen einer breiten Masse zugänglich und werden aus Datenschutz- und Sicherheitsgründen regelmäßig von Privatpersonen genutzt. Im Unternehmenskontext sind beide Anwendungsfälle von entscheidender Bedeutung.

Unternehmen nutzen VPNs schon seit Jahrzehnten, um einen sicheren Zugriff auf ihre Netzwerke zu ermöglichen. Aber viele Unternehmen begannen sie nach der Pandemie noch häufiger zu nutzen, als Remote-Arbeit und „Arbeiten von überall“ in aller Munde war. Eine Umfrage von Coupon Follow aus dem Jahr 2021 ergab, dass allein im März 2020 die VPN-Nutzung im Vergleich zum Vormonat um 142% gestiegen war. Die durch den fehlenden Zugang zu den Büros erforderlichen „Bring-your-own-device“-Praktiken führten dazu, dass eine Vielzahl von Mitarbeitern, die ihre eigenen Computer verwendeten, schnelle und einfach zu implementierende Sicherheitsprotokolle benötigten, um Ihre Verbindungen zum Unternehmensnetzwerk abzusichern.

VPNs reichen für eine sichere Netzwerkverbindung nicht mehr aus

Obwohl VPNs als hervorragende Überbrückung in einer Krisensituation dienten, sind sie nicht mehr optimal, um Unternehmen vor einer Sicherheitsverletzung zu schützen. Mike Vizard von der Techstrong Group erklärt: „Es besteht kein Zweifel, dass VPNs während der Pandemie eine entscheidende Rolle spielten, als sie den Mitarbeitern das Arbeiten von zu Hause ermöglichten. Aber es ist einfach an der Zeit, auf eine flexiblere Netzwerkarchitektur umzusteigen, die auch sicherer ist." Die National Security Agency warnte Unternehmen, die VPNs nutzen, auch davor, dass diese, sofern nicht ordnungsgemäß gesichert, anfällig für Netzwerk-Scans, Brute-Force-Angriffe und Zero-Day-Schwachstellen seien.

Cybersicherheitsexperten sind sich einig, dass es an der Zeit ist, sich von VPNs zu verabschieden, egal wie nützlich sie in der Vergangenheit waren. Zusätzlich zu den Sicherheitsrisiken erfüllen VPNs oft nicht die Compliance-Anforderungen, können Ihr Netzwerk gefährden, wenn sie nicht richtig konfiguriert sind und sind in der Regel eher langsam, wenn sie mit Benutzern überlastet sind, was sich auf das Benutzererlebnis auswirken kann. Aber wie lassen sich dann die Online-Aktivitäten von Unternehmen absichern, insbesondere im Zuge einer grundlegenden Verlagerung weg vom Büro und hin zur Remote-Arbeit?

Zero Trust Network Access als Lösung

Die Lösung für das VPN-Problem liegt im Zero Trust Network Access (ZTNA). ZTNA ist kein einzelnes Produkt oder eine Lösung — es ist eine Philosophie rund um die Frage, welchen Zugriff man verschiedenen Benutzern gewährt. Doch dazu kommen wir gleich. Die Zero Trust Philosophie ist ein Grundsatz des Secure Access Service Edge (SASE), den Gartner wie folgt definiert:

„Ein neues Paket an Technologien, das Kernfähigkeiten wie Software-definiertes WAN (SD-WAN), Secure Web Gateway (SWG), Cloud Access Security Brokers (CASB), Zero Trust Network Access (ZTNA) und Firewall as a Service (FWaaS) umfasst, die sensible Daten oder Malware identifizieren und Inhalte in Leitungsgeschwindigkeit entschlüsseln können, mit kontinuierlicher Überwachung von Sitzungen auf Risiko- und Vertrauensstufen."

Das Ziel von SASE besteht darin, eine vielseitig Tool-Suite bereitzustellen, um die IT-Landschaften von Unternehmen in der heutigen hybriden Multi-Cloud-Welt zu schützen, in der Benutzer und Geräte sich fast überall aufhalten können. Da unsere Gesellschaft mittlerweile unter Hybrid-/Remote-Arbeit nicht „Arbeiten von zu Hause", sondern „Arbeiten von überall" versteht, ist die Möglichkeit, Geräte überall dort zu sichern, wo sie sich befinden, umso wichtiger. Und genau das können SASE und ZTNA bieten.

Nun zurück zum ZTNA. Während die klassische Netzwerksicherheit nach dem Prinzip „Vertrauen und Kontrolle" funktioniert, arbeitet das neue ZTNA-Modell nach dem Motto „Vertrauen ist gut, Kontrolle ist besser." Dieser Ansatz wird Prinzip der geringsten Berechtigung genannt. Es bedeutet, dass ein Unternehmen alle Benutzer gleichermaßen kritisch prüft und einem Benutzer niemals automatisch Zugriff auf Netzwerke oder Assets gewährt. Stattdessen werden Berechtigungen so verwaltet, dass Benutzer nur Zugriff auf die Daten, Assets und Applikationen haben, die sie persönlich brauchen. Durch kontinuierliches Überprüfen wird sichergestellt, dass der Benutzer der ist, für den er sich ausgibt und das Risiko einer Netzwerkverletzung und der lateralen Ausbreitung von Bedrohungen verringert sich.

Wie ZTNA funktioniert

Der Begriff „Zero Trust“ mag misstrauisch wirken, aber in der heutigen Cyber-Bedrohungslandschaft, die immer komplexer wird, ist dieser Verifizierungsgrad absolut notwendig. Auch wenn „Zero Trust“ vielleicht negativ klingt, geht es bei diesem Modell eigentlich um Befähigung und nicht um Einschränkung. Es ermöglicht einen besseren Fernzugriff, sorgt für verbesserte Performance, höhere Produktivität und optimierte Sicherheit.

Man kann ZTNA zum Beispiel mit den Sicherheitsabläufen auf einem Flughafen vergleichen. Kommt ein Passagier zum Check-In-Schalter, muss er oder sie die Identität anhand des Reisepasses bestätigen. Das bringt sie auf ihrer Reise ins Ausland einen Schritt weiter. Damit erhalten sie jedoch noch nicht die Erlaubnis, in das Flugzeug zu steigen: Sie benötigen noch eine Boarding-Karte. Ohne diese beiden Dokumente wird ihnen der Zutritt verwehrt. Umgelegt auf ZTNA heißt das, wenn Sie nicht sowohl Ihre Identität bestätigen — mit dem Reisepass — als auch nachweisen können, dass Sie über die erforderlichen Berechtigungen für den Netzzugang verfügen — mit der Boarding-Karte — können Sie Ihre Reise nicht fortsetzen. So wie einzelne Passagiere bei der Sicherheitskontrolle gründlich überprüft werden und ihre Identität sowie ihre Berechtigung nachweisen müssen, um passieren zu dürfen, verlangt Zero Trust dies von jedem Benutzer, der versucht auf Ihr Netzwerk zuzugreifen.

Neben dem Vorteil, Benutzer gründlich zu identifizieren und zu überprüfen, bevor ihnen Netzwerkzugriff gewährt wird und so die Wahrscheinlichkeit einer Sicherheitsverletzung gering zu halten, ist ein weiterer, vielleicht nicht sofort offensichtlicher, wichtiger Vorteil von ZTNA, sein zuverlässige Aufzeichnungssystem. Wenn Benutzer versuchen, auf das Netzwerk zuzugreifen, werden das Gerät, der Standort und die Identität jedes Einzelnen aufgezeichnet. Daraus ergibt sich ein Prüfprotokoll und eine automatisierte Rückverfolgbarkeit, die andere Lösungen nicht bieten. Neben dem Sicherheitsvorteil kann die Aufzeichnung von Zugriffsversuchen auch für Compliance- und Audit-Anforderungen nützlich sein. Weitere Vorteile sind die Zeitersparnis durch automatisierte Abläufe und der Wegfall von IT-Tickets oder von Genehmigungen durch die Geschäftsleitung für den Netzwerkzugriff.

VPNs können mit der Sorgfalt und dem gründlichen Prüfungsprozess, den ZTNA ermöglicht, nicht mithalten. Das Maß an Granularität, mit dem Sie Berechtigungen verwalten können, ist nur mit einer Lösung wie ZTNA möglich und kann nicht mit einem VPN reproduziert werden. Während VPNs den Datenverkehr zunächst über mehrere Server und anschließend über einen zentralen Standort innerhalb des Unternehmensnetzwerks leiten, verbindet ZTNA den Benutzer direkt mit den Anwendungen, ohne dass er über diese zentrale Stelle geleitet werden muss, was auch die Latenz reduziert. Angesichts der steigenden Anzahl der von Unternehmen genutzten Cloud-Anwendungen, führt die verbesserte Performance dieser Anwendungen zu einem spürbaren Effizienzunterschied, sowohl was den Zeitfaktor als auch die Benutzerfreundlichkeit angeht.

Die Zeit ist reif für den Einsatz von ZTNA

Da die Nutzung privilegierter Konten in den letzten Jahren so viele erfolgreiche Datenpannen verursacht hat, müssen Unternehmen Maßnahmen zur sicheren Verwaltung der Berechtigungen und des Netzwerkzugriffs ergreifen, bevor es zu spät ist.

Testen Sie Barracuda CloudGen Access kostenlos 14 Tage lang und überzeugen Sie sich selbst davon, wie leicht es ist, Ihre Compliance zu vereinfachen, Zero Trust Network Access zu implementieren und den Zugriff Dritter auf Ihre Systeme zu sichern. Wenn Sie Fragen haben, können Sie uns auch gerne. kontaktieren de.barracuda.com/company/contact.

Barracuda

Über Barracuda

Barracuda ist bestrebt, die Welt zu einem sichereren Ort zu machen und überzeugt davon, dass jedes Unternehmen Zugang zu Cloud-fähigen Sicherheitslösungen auf höchstem Niveau verdient, die einfach zu erwerben, zu implementieren und zu nutzen sind. Wir schützen E-Mails, Netzwerke, Daten und Anwendungen mit innovativen Lösungen, die im Zuge der Customer Journey wachsen. Mehr als 200.000 Unternehmen weltweit vertrauen auf Barracuda und darauf, dass wir sie auch vor Risiken schützen, die ihnen möglicherweise gar nicht bewusst sind. Daher können sich diese Unternehmen ganz auf ihr Wachstum konzentrieren. Weitere Informationen finden Sie auf de.barracuda.com.