Sicher daheim arbeiten

Siegfried Plommer

VPN-Verbindungen bieten im Homeoffice keinen ausreichenden Schutz vor Cyber-Angriffen. Um diesen zu gewährleisten, setzen viele Hersteller deshalb auf Zero Trust Network Access.

Vor der Corona Krise waren nur etwa vier Prozent aller Arbeitenden ganz oder überwiegend im Homeoffice tätig. Im Jahr 2022 pendelte sich die Zahl bei circa 20 Prozent ein. Studien zeigen, dass der Trend New Work anhalten wird. Das wirft Fragen nach der IT-Sicherheit, dem Schutz Kritischer Infrastrukturen (KRITIS) und personenbezogener Daten gemäß der Datenschutz-Grundverordnung (DSGVO) auf. Die Pandemie und der Zwang, von zu Hause aus zu arbeiten, haben ein bereits bestehendes Problem verschärft: Wie schützt man Arbeitsplätze, die sich außerhalb des abgesicherten Unternehmensnetzwerks befinden?

Aus der Not heraus wurden bewährte Techniken auf das Homeoffice und mobile Arbeitsplätze angewendet. In der Praxis kam deshalb überwiegend die VPN-Technologie zum Einsatz (Virtual Private Network). Eine VPN-Verbindung ist dann sinnvoll, wenn sie als Standortvernetzung innerhalb besser zu sichernden Umgebungen dient. Bei mobilen Arbeitsplätzen ist die gleiche Technologie jedoch durch die Vielzahl der Endpunkte höchst problematisch. Der Grund: Durch eine VPN-Verbindung wird der mobile Arbeitsplatz Mitglied im Kommunal- beziehungsweise Unternehmensnetzwerk. Damit steht der Zugang zu allen darin befindlichen Systemen offen.

Beharrt man auf einer VPN-Verbindung zur Anbindung externer Geräte, müssen diese überwacht und kontrolliert werden. Nur so lässt sich vermeiden, dass Schad-Software automatisch eingeschleust oder unerwünscht auf das Gerät zugegriffen wird. Dafür werden auf den Endgeräten, von denen die Verbindung ausgeht, verschiedene Clients und Tools installiert, die der Absicherung dienen sollen. Zusätzlich sind weitere Maßnahmen im Intranet notwendig, um etwa die Zugriffsrechte der einzelnen Anwender zu überwachen. Hinzu kommt, dass durch den Einsatz einer VPN-Verbindung kritische Verwaltungs- und Unternehmensdaten auf den Endgeräten der Anwender landen, wo die Verwaltung sie nicht mehr kontrollieren kann. Unter diesen Umständen weiterhin die DSGVO-Richtlinien einzuhalten, ist äußerst schwierig.

Deshalb sind Lösungen zu bevorzugen, die den Zugriff auf Systeme und Anwendungen mit granularen Zugriffsrechten absichern und die Abwanderung von Daten auf Clients außerhalb des Netzwerks verhindern. Dies gewährleisten Zwei-Faktor-Authentifizierungslösungen, die eine Voraussetzung für so genannte Zero-Trust-Network-Access (ZTNA)-Strategien darstellen. Zero Trust Network Access geht davon aus, dass keinem Benutzer oder Endgerät, das sich mit dem internen Netzwerk verbinden will, vertraut werden darf. Darüber vergibt ZTNA nur stark eingeschränkte Zugriffsrechte. Dieses Prinzip widerspricht deshalb in großen Teilen üblichen VPN-Verbindungen. Um die ZTNA-Vorgaben erfüllen zu können, rücken viele Hersteller von den Firewalls der klassischen VPNs ab. Stattdessen bevorzugen sie alternative Zugriffslösungen, die kostengünstiger und weniger komplex sind. Wenn man die jüngsten Vorfälle genauer betrachtet, springt eine Tatsache ins Auge: Eine Software allein schützt nicht hundertprozentig vor Cyber-Angriffen. Die Schwachstelle Mensch muss in die Sicherheitsbewertung einbezogen werden. Deshalb empfiehlt es sich, Schulungen durchzuführen. Nur so lassen sich die Nutzer für jede Art von betrügerischen Angriffen sensibilisieren. Erst die Verbindung aus erfahrenen Benutzern, einer Firewall und einer beherrschbaren, klar strukturierten Remote-Access-Lösung kann einen nahezu hundertprozentigen Schutz gewährleisten – und sie kostet kein Vermögen.

Siegfried Plommer ist Geschäftsführer der beyond SSL GmbH.