So funktioniert der Zugriff auf Fachanwendungen ohne VPN oder Reverse Proxy

Wer seinen Mitarbeitenden ausserhalb der eigenen Büroräumlichkeiten Zugriff auf lokale Fachanwendungen gewähren will, tut dies herkömmlicherweise mit VPN oder einem Reverse Proxy. Von Microsoft gibt es mittlerweile eine für viele Unternehmen kostengünstigere und benutzerfreundlichere Alternative.

DER AUTOR

Severin Freund
System Administrator Mobility Specialist, Nomasis

Den Beitrag finden Sie auch online
www.netzwoche.ch

Für Unternehmen gehört es zur Normalität, Mitarbeitenden den Zugriff auf lokale Anwendungen zu ermöglichen, wenn sich deren Arbeitsgeräte nicht im firmeneigenen Netzwerk befinden. Dies ist nicht erst seit der steigenden Verbreitung von Homeoffice infolge der Covid-19-Pandemie der Fall. Eine nomadische Nutzung von Endgeräten, die über die Verwendung von E-Mail, Kalender und Office-Anwendungen hinausgeht und auch den mobilen Zugriff auf Fachanwendungen umfasst, war schon vor Corona für viele Unternehmen eine Selbstverständlichkeit. Im Zuge des «New Normal» hat aber die Thematik weiter an Bedeutung gewonnen. Dabei kommen bei nomadischer Nutzung mit Smartphone oder Tablet oder im Homeoffice mit dem Laptop vor allem zwei Technologien zum Einsatz: Die Geräte verbinden sich entweder über eine virtuelle, private Verbindung mit dem Unternehmens-Server (VPN) oder über einen Reverse Proxy, einem Rechnernetz innerhalb des Unternehmensnetzes selbst, das den externen Client mit den Servern verbindet. Bei beiden Varianten kommunizieren Endgerät und Server in beide Richtungen miteinander, was der IT entsprechendes Security-Fachwissen und Ressourcen abverlangt. Zum Beispiel gibt es bei VPN Unterschiede zwischen den gängigen Betriebssystemen Windows 10, MacOS, Apples iOS und Android in Bezug auf den Funktionsumfang, die Benutzerfreundlichkeit und die technische Implementierung der Lösungen. Ausserdem kann es sein, dass für beide Lösungen ein zusätzliches Produkt benötigt wird, wodurch zusätzliche Lizenzkosten anfallen.

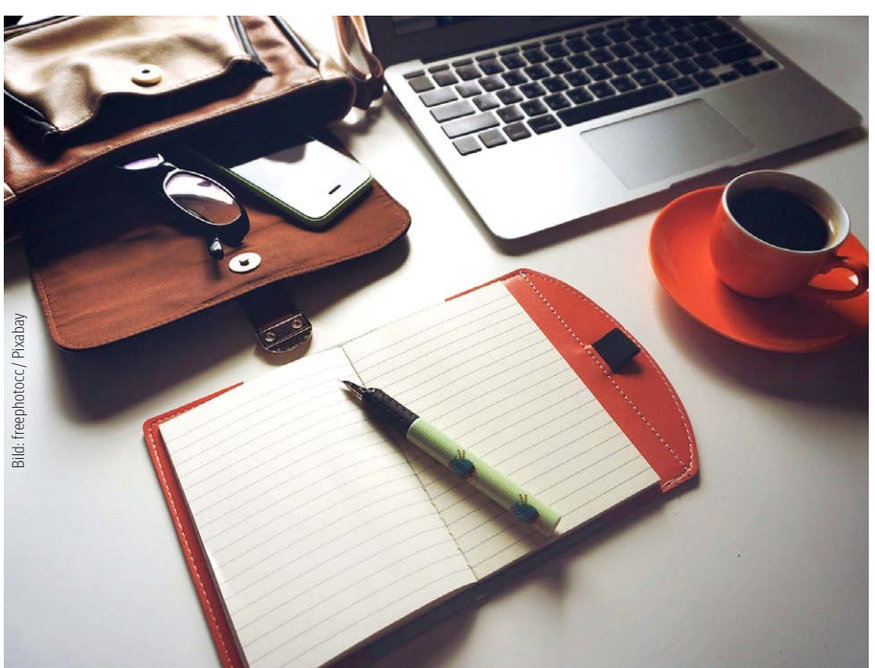

Bild: freephotocc/ Pixabay

Die Lösung steckt im bereits bezahlten Lizenzpaket

Von Microsoft gibt es für dieses Problem eine mögliche Alternative. Der Hersteller liefert dafür Funktionen innerhalb eines Lizenzpakets mit, die Kunden zwar bezahlen, aber je nachdem noch nicht nutzen. Die Rede ist von Azure AD Application Proxy, einer Funktionalität des Identitäts- und Zugriffsverwaltungsdiensts Azure AD. Viele Firmen nutzen Azure AD bislang eingeschränkt, etwa lediglich für den Zugriff auf Microsoft-365-Anwendungen, und fahren für die Remote-Arbeit auf lokalen Anwendungen nach wie vor die herkömmliche Schiene mit VPN oder Reverse Proxy. Sie riskieren dabei, die genannten Problematiken wie die Notwendigkeit von zusätzlichem Know-how für Systemadministration und Support und unnötige Kosten für Lizenzen in Kauf zu nehmen.

Keine externen Geräte im Firmennetz

Der Anwendungsproxy arbeitet im Gegensatz zu den herkömmlichen Lösungen ohne das Öffnen zusätzlicher Firewall-Ports für den eingehenden Datenverkehr und ohne eine umständliche Steuerung der Authentifizierung und Autorisierung auf Anwendungsebene. Er regelt Letzteres quasi als externer Endpunkt des Netzes selbst, sodass sich der Anwender oder die Anwenderin nur einmal in der Azure-Cloud anmelden muss. Lediglich die von der lokalen Anwendung im Firmennetz ausgehenden Verbindungen werden durch die Firewall hindurch in die Azure-Cloud aufgebaut. Ausserdem sind so neue Anwendungsfälle möglich, weil nicht mehr jedes einzelne Gerät ins Firmennetz eingebunden werden muss. Einziger Wermutstropfen ist die Tatsache, dass dies nur bei Webanwendungen möglich ist. Ältere, firmeneigene, nicht browserfähige Applikationen hingegen bleiben hier aussen vor. Eine Analyse der Möglichkeiten lohnt sich indes trotzdem. Gerade für Unternehmen, die ihren Fokus auf Microsoft-Lösungen legen, spielen neben tieferen Lizenzkosten auch die Sicherheit der Firmendaten und die Benutzerfreundlichkeit (Single Sign-on) eine Rolle.