FORTINET

Ermitteln der Sicherheitsanforderungen für die umfassende Umstellung auf Homeoffices

Wie Sie ein Security-Konzept für Telearbeit entwickeln

Inhaltsverzeichnis

Zusammenfassung 3

Einleitung 4

Erfüllen grundlegender Anforderungen für die Arbeit im Homeoffice 4

Unterstützen von Powerusern im Homeoffice 7

Security und Stabilität im Hauptsitz 9

Fazit 12

Zusammenfassung

Unternehmen sollten die Arbeit im Homeoffice als Teil ihres Business-Continuity-Plans unterstützen. Ein solcher Plan für die Aufrechterhaltung eines kontinuierlichen Geschäftsbetriebs sollte auch Szenarien abdecken, bei denen der Großteil oder die gesamte Belegschaft auf Telearbeit umgestellt werden muss. Dies bringt jedoch neue Netzwerk- und Security-Probleme mit sich, da Remote-Worker das Unternehmensnetzwerk vollkommen anders als Mitarbeiter in der Firma nutzen.

Für den Schutz einer im Homeoffice arbeitenden Belegschaft müssen Security-Lösungen gefunden und implementiert werden, die sowohl die Anforderungen der Mitarbeiter als auch des Netzwerks in der Unternehmenszentrale erfüllen. Der Großteil der Mitarbeiter braucht lediglich einen sicheren Zugriff auf das Unternehmensnetzwerk und cloudbasierte Anwendungen, was sich mit einem VPN-Zugang und einer Multi-Faktor-Authentifizierung (MFA) regeln lässt. Netzwerk-Administratoren und Führungskräfte dürften wahrscheinlich umfassendere Netzwerk-Anforderungen haben, wie z. B. eine dauerhafte Verbindung zum Unternehmensnetzwerk und eine sichere Telefonie-Lösung. Weiter muss das Unternehmensnetzwerk in der Zentrale die eingehenden Netzwerk-Verbindungen von großen Teilen der Belegschaft unterstützen und schützen können, wofür eine robuste Benutzerauthentifizierung und eine stärkere Sicherheit am Netzwerkrand – Stichwort „Perimeter-Security“ – notwendig ist.

Einleitung

Die Fähigkeit, Remote-Worker zu unterstützen, kann den Business-Continuity-Plan eines Unternehmens entscheidend verbessern. Unternehmen sichern sich damit eine flexible Anpassungsfähigkeit, wenn unvorhergesehene Umstände wie Naturkatastrophen oder eine Pandemie es Mitarbeitern unmöglich machen, im Firmensitz zu arbeiten.

Unter diesen Umständen kann ein Unternehmen gezwungen sein, die Belegschaft größtenteils oder vollkommen auf die Arbeit im Homeoffice umzustellen. Bei der Gestaltung und Implementierung einer Telearbeitslösung müssen jedoch nicht nur die Netzwerk-Anforderungen, sondern auch die neuen Sicherheitsfragen geklärt werden, die mit dem Remote-Working einhergehen.

Erfüllen grundlegender Anforderungen für die Arbeit im Homeoffice

Ungeachtet unterschiedlichster Mitarbeiteranforderungen an die Remote-Umgebung müssen für die Arbeit im Homeoffice einige Grundlagen erfüllt sein, damit Telearbeiter über sichere, authentifizierte Verbindungen zum Unternehmensnetzwerk verfügen. Dazu gehören der Zugriff auf ein virtuelles privates Netzwerk (VPN) und eine starke Authentifizierungslösung, um Nutzerkonten vor Kompromittierungen zu schützen.

Virtuelle private Netzwerke (VPN)

Bei der Telearbeit werden vertrauliche Unternehmensdaten im Heimnetzwerk eines Mitarbeiters verarbeitet. Um diese Daten vor Kompromittierungen zu schützen, muss jederzeit gewährleistet sein, dass die Verbindung des Remote-Workers zum Unternehmensnetzwerk sicher ist.

Telearbeiter müssen Zugriff auf ein VPN haben, das eine direkte, verschlüsselte Konnektivität zwischen ihrem Computer und dem Unternehmensnetzwerk herstellt. Dies schützt nicht nur die Vertraulichkeit und Integrität sensibler Unternehmensdaten während der Übertragung, sondern gewährleistet auch, dass der gesamte Datenverkehr zwischen dem Homeoffice des Mitarbeiters und dem öffentlich zugänglichen Internet von der Cyber-Security-Infrastruktur des Unternehmens überwacht und gesichert wird.

Multi-Faktor-Authentifizierung (MFA)

Arbeiten Mitarbeiter von zu Hause aus, besteht eine höhere Wahrscheinlichkeit, dass gestohlene Anmeldedaten ausgenutzt werden: Computer im Homeoffice sind oft unbeaufsichtigt, was den unbefugten Zugriff auf das geschäftliche Benutzerkonto erleichtert. Sicherheitsfunktionen zum Erkennen anomaler Zugriffsmuster – wie z. B. Ort und Zeit des Authentifizierungsversuchs – können in solchen Situationen versagen, da Mitarbeiter im Homeoffice oft andere Arbeitsgewohnheiten haben.

Um den Zugriff auf das Unternehmensnetzwerk, Ressourcen und Daten zu sichern, muss die Authentifizierung robuster sein als die übliche Kombination aus Benutzername und Passwort: Alle Telearbeiter sollten einen sicheren Authentifizierungstoken erhalten. MFA-Token für die Multi-Faktor-Authentifizierung gibt es als Hardware (z. B. Schlüsselanhänger) oder Software (z. B. als Smartphone-App). Solche Tokens überprüfen die Identität eines Benutzers, bevor er eine VPN-Verbindung zum Unternehmensnetzwerk herstellen oder auf andere sensible Unternehmensressourcen zugreifen darf.

Nach den PCI-DSS-Vorgaben für Telearbeit müssen sich Mitarbeiter für den Zugriff auf Daten von Karteninhabern über ein VPN authentifizieren und die Multi-Faktor-Authentifizierung verwenden.[1]

Unterstützen von Powerusern im Homeoffice

Während für viele Telearbeiter eine VPN-Verbindung und ein MFA-Token genügen, haben andere Mitarbeitergruppen zusätzliche Anforderungen. Poweruser wie Netzwerk-Administratoren und Führungskräfte benötigen ein erweitertes Homeoffice, um ihre Kernaufgaben zu erfüllen. Dazu gehören z. B. eine dauerhafte Verbindung zum Unternehmensnetzwerk und eine sichere Telefonie-Lösung.

Dauerhafte Verbindung zum Unternehmensnetzwerk

Einige Benutzer wie Netzwerk-Administratoren und Security-Teams benötigen einen flexibleren, ständigen Zugriff auf das Unternehmensnetzwerk. Diese Mitarbeiter müssen sich möglicherweise mit mehreren Geräten in das Unternehmensnetzwerk einloggen oder benötigen eine dauerhafte Verbindung ohne zeitlich begrenzte Sitzungen, die automatisch beendet werden (Stichwort „Session Timeouts“).

Die Homeoffice-Anforderungen von Powerusern lassen sich mit einem WLAN-Zugang realisieren, über den ein zuverlässiger VPN-Tunnel zum Unternehmensnetzwerk aufgebaut wird. Damit diese Verbindung auch wirklich sicher ist, sollte dieser Wireless Access Point mit einer NGFW-Softwarelösung kombiniert werden, um eine Überprüfung des Datenverkehrs, ein Zugangs-Management und einen intelligenten Bedrohungsschutz bereitzustellen.

Sichere Telefonie

Bei der Arbeit im Homeoffice ist es wichtig, dass Mitarbeiter – insbesondere Führungskräfte – über eine sichere Telefonie-Lösung verfügen, um vertrauliche Gespräche und Unternehmensdaten zu schützen. Andernfalls besteht die Gefahr, dass sensible Informationen durch Abhören von Mobilfunknetzen oder durch die Verwendung bösartiger Smartphone-Apps abgegriffen werden.

Eine effektive, sichere Telefonie-Lösung für externe Mitarbeiter lässt sich mit VoIP-Übertragungen (Voice-over-IP) schaffen: Besitzt ein Benutzer bereits Zugriff auf eine geschützte, dauerhafte und zuverlässige Internetverbindung, kann der Sprachverkehr ebenfalls darüber laufen. Ein solches Routing lässt sich mit minimalem Aufwand einrichten. Das Unternehmen kann so den Sprachverkehr überwachen und den Netzwerk-Rand auf potenziell schädliche Inhalte kontrollieren, die es auf anfällige VoIP-Software abgesehen haben.

Telefonie-Lösungen für Telearbeiter sollten den gleichen Funktionsumfang wie im Firmensitz bieten. Dies minimiert die Wahrscheinlichkeit, dass Mitarbeiter private Geräte für die Geschäftskommunikation verwenden. Zu den wichtigsten Funktionen gehören das Erhalten und Initiieren von Anrufen, der Zugriff auf Voicemails und das Telefonverzeichnis des Unternehmens sowie eine überprüfbare Anrufliste.

Ein CEO verbringt 72 % seines Tages in Meetings.
Eine sichere Telekommunikation im Homeoffice ist daher ein Muss.[2]

Security und Stabilität im Hauptsitz

Security-Lösungen für Remote-Mitarbeiter sind nicht auf die Client-Seite beschränkt. Steigt die Anzahl der Telearbeiter, kommen auf das Unternehmen auch im Hauptsitz neue Sicherheitsbedrohungen und Netzwerk-Anforderungen zu.

Bei einem Homeoffice-Konzept für einen kontinuierlichen Geschäftsbetrieb muss unbedingt sichergestellt werden, dass das Netzwerk in der Zentrale von außerhalb zugreifende Benutzer und Geräte authentifizieren und die erheblich größere Anzahl eingehender VPN-Verbindungen schützen und bewältigen kann.

Authentifizierung von Benutzern und Geräten

Ein sogenanntes „Zero-Trust"-Sicherheitsmodell ist quasi ein Muss, wenn ein Unternehmen eine größtenteils oder vollkommen im Homeoffice arbeitende Belegschaft unterstützen will. Mitarbeiter versuchen möglicherweise, über unbekannte oder private Geräte auf das Unternehmensnetzwerk zuzugreifen. Bei Systemen, die mit nicht vertrauenswürdigen Netzwerken verbunden sind, besteht jedoch eine höhere Wahrscheinlichkeit, dass sie von Cyber-Angreifern kompromittiert werden.

Um das Unternehmensnetzwerk und die darin enthaltenen vertraulichen Daten und Ressourcen zu schützen, müssen Benutzer und Geräte bei Verbindungsversuchen authentifizierbar sein. Das lässt sich z. B. mit einem zentralen Authentifizierungsserver mit Zugriff auf das Active Directory des Unternehmens mit LDAP (Lightweight Directory Access Protocol) und RADIUS (Remote Authentication Dial-In User Service) erreichen.

Dieser Server sollte skalierbar sein, um die Anforderungen einer größeren Remote-Belegschaft zu erfüllen, ohne die Benutzerproduktivität auszubremsen. Einmaliges Anmelden (Single-Sign-On, SSO), Zertifikatsverwaltung und Gäste-Management sollten unterstützt werden, um ohne zusätzliche Belastung der externen Mitarbeiter die Benutzerauthentifizierung sicherzustellen.

Sichern des Netzwerk-Perimeters

Arbeitet der Großteil oder die gesamte Belegschaft nicht mehr im Firmensitz, sondern im Homeoffice, steigt die Anzahl der VPN-Verbindungen, die das Unternehmen bewältigen muss. Im Büro sind Mitarbeiter direkt mit dem Unternehmens-LAN verbunden, im Homeoffice laufen dagegen alle Datenübertragungen über das VPN. Die NGFW des Unternehmens muss in der Lage sein, alle VPN-Verbindungen zu beenden und eine große Anzahl verschlüsselter Netzwerk-Verbindungen zu überprüfen. Da die Inspektion von verschlüsseltem Datenverkehr rechenintensiv ist, sollte die NGFW auch skalierbar sein, um den steigenden Bedarf zu erfüllen. Dazu sind NGFWs mit eigens für diesen Zweck entwickelten, modernen Security-Prozessoren notwendig, die Latenzzeiten minimieren und den Durchsatz maximieren – ein Muss, um Netzwerk-Engpässe zu vermeiden, die zu Lasten der Mitarbeiterproduktivität gehen.

NGFWs in der Unternehmenszentrale – am sogenannten „Headend“ oder auch „Kopfstation“ – müssen außerdem eine Layer-7-Inspektion des gesamten Datenverkehrs durchführen können. Diese Überprüfung ist zwar in jedem Unternehmenskontext wichtig, bei einer Belegschaft im Homeoffice muss jedoch bei eingehenden Remote-Verbindungen mit einer höheren Konzentration bösartiger Inhalte gerechnet werden. Das liegt daran, dass die Wahrscheinlichkeit von Malware-Infektionen steigt, wenn Mitarbeitercomputer mit privaten Netzwerken verbunden sind. Eingeschleuste Malware kann dann versuchen, seitlich in das Unternehmensnetzwerk vorzudringen. Eine Layer-7-NGFW kann erkennen, welche Anwendung ein eingehendes Paket erreichen will, und Pakete von Anwendungen mit bekannten Schwachstellen blockieren. Headend-NGFWs sollten zudem mit Sandbox-Funktionen integriert werden, um verdächtige Inhalte, die auf keine bekannte Bedrohung hindeuten, sicher analysieren zu können.

Bei der TLS/SSL-Inspektion (Transport Layer Security/ Secure Sockets Layer) sinkt der Firewall-Durchsatz im Durchschnitt um 60 %.[3]

Fazit

Bei einer schnellen, umfassenden Umstellung auf Homeoffices ist es wichtig, dass ein Unternehmen nicht nur den Geschäftsbetrieb aufrechterhalten kann, sondern auch die Sicherheit von Mitarbeitern im Homeoffice und der von ihnen verarbeiteten vertraulichen Daten gewährleistet.

Dazu muss das Unternehmen Security-Lösungen im Homeoffice bzw. am alternierenden Arbeitsplatz und im Hauptnetzwerk des Unternehmens implementieren. Entscheidend ist, dass die gewählten Lösungen die besonderen Infrastruktur- und Security-Anforderungen einer Remote-Belegschaft erfüllen. Muss in einer Ausnahmesituation oder im Katastrophenfall sofort reagiert werden, sollte die Lösung schnell und einfach implementierbar sein, um die Auswirkungen auf den Geschäftsbetrieb auf ein Minimum zu begrenzen.

[1] Emma Sutcliffe: „How the PCI DSS Can Help Remote Workers“. PCI Security Standards Council, 26. März 2020.

[2] Michael E. Porter and Nitin Nohria: „How CEOs Manage Time“. Harvard Business Review, Juli 2018.

[3] „NSS Labs Expands 2018 NGFW Group Test with SSL/TLS Security and Performance Test Reports“. NSS Labs, 24. Juli 2018.

www.fortinet.com/de

628535-0-0-DE

31. August 2020, 8:45 Uhr