WHITEPAPER

Work from Anywhere: Telearbeit und Homeoffices einfacher realisieren

So stellen Sie eine konsequente, einheitliche Security unabhängig vom Arbeitsort bereit

Zusammenfassung

In den letzten zehn Jahren wurden Technologien ständig weiterentwickelt, damit Mitarbeiter mehr Flexibilität bei verwendeten Geräten, Arbeitsorten und den Zugriff auf Ressourcen erhalten. Die geschäftliche Nutzung von Privatgeräten (BYOD, Bring Your Own Device) und die Umstellung auf Cloud-Anwendungen waren die ersten Schritte hin zu flexiblen Arbeitsmodellen.

Viele Unternehmen beschäftigten sich bereits vor der Pandemie mit Telearbeit- und Homeoffice-Konzepten, doch durch die weltweite Ausnahmesituation wurde die in den nächsten Jahren geplante Umsetzung einer Work-from-Anywhere-Strategie (WFA) zur dringenden Notwendigkeit. Mittlerweile fordern immer mehr Arbeitnehmer, dass Arbeitgeber eine WFA-Option anbieten. Die Herausforderung besteht nun darin, eine hybride Arbeitsumgebung zu schaffen, die die Produktivität und Sicherheit der Mitarbeiter an jedem Arbeitsort gewährleistet.

Laut dem Global Threat Landscape Report gab es von Juni 2020 bis Juni 2021 fast 1100 % mehr Ransomware-Vorfälle.[1]

Schutz einer hybriden Belegschaft

Beim Ausbruch der Pandemie waren nur wenige Unternehmen auf die Unterstützung von Remote-Arbeit vorbereitet. Plötzlich griffen Mitarbeiter aus schlecht geschützten Heimnetzwerken auf Unternehmensressourcen zu, verwendeten anfällige Endgeräte – und das alles mit unzureichenden Zugangskontrollen. Es überrascht daher kaum, dass Cyber-Kriminelle diese Schwachstellen schnell ausnutzen: Erst kürzlich berichtete Forrester, dass 67 % der Unternehmen einen Cyberangriff mit geschäftsschädigenden Folgen wegen Sicherheitslücken bei der Remote-Arbeit erlitten hatten.[2]

Mit Blick auf die Zukunft planen viele Unternehmen, große Teile der Belegschaft zumindest zeitweise weiterhin im Homeoffice arbeiten zu lassen. Da die Firmen bereits in Tools und Lösungen zur Sicherung der Mitarbeiterproduktivität investiert haben, spricht auch nichts gegen, diesem Wunsch vieler Arbeitnehmer nachzukommen.

Bei hybriden Arbeitsmodellen wird einige Tage in der Woche im Firmensitz und den Rest der Zeit von zu Hause oder anderen Remote-Arbeitsplätzen gearbeitet. Diese Hybrid-Worker und ihre Geräte müssen nahtlos zwischen verschiedenen Umgebungen wechseln und – unabhängig vom Standort – sicher auf Anwendungen und Ressourcen in der Cloud oder im Rechenzentrum zugreifen können.

Remote-Arbeit verlangt von Unternehmen nicht nur neue Sicherheitskonzepte. Auch müssen Lösungen bereitgestellt werden, die Anwender überall hin begleiten, sie schützen und ihre Produktivität erhalten. Hybrid-Worker brauchen einen soliden Endpunkt-Schutz, der mit einem Zero-Trust-Access (ZTA) und Zero-Trust-Network-Access (ZTNA) kombiniert wird. Weiter sind ein Secure Software-Defined Wide Area Networking (SD-WAN) und ein Secure Access Service Edge (SASE) für eine sichere Konnektivität notwendig. Unternehmen benötigen zudem so genannte Access Policy Engines – eine systematische Zugangsregelung, die Anwendern an jedem Standort einen angemessenen, sicheren Zugriff anhand der Benutzer- und Geräteidentität, des Standorts, des Gerätetyps und des Sicherheitsprofils gewährt.

Die meisten Unternehmen stehen nun vor der Herausforderung, WFA-Strategien mit vorhandenen Einzellösungen verschiedener Anbieter umzusetzen. Das Problem: Oft gibt es in Firmen für jede Sicherheitsfunktion – wie Endpunkt-Schutz, Endpoint Detection und Response (EDR) oder Identitätsprüfung – eine eigenständige Lösung, die mehr schlecht als recht mit anderen Sicherheitsprodukten funktioniert. Manchmal werden sogar unterschiedliche Firewall-Anbieter im Rechenzentrum, in Niederlassungen und auf diversen Cloud-Plattformen eingesetzt. Es ist nahezu unmöglich, mit diesem „Anbieter-Potpourri“ eine ineinandergreifende, zuverlässige Gesamtlösung für die Sicherheit zu entwickeln. Stattdessen wird auf komplexe Workarounds ausgewichen, damit die isolierten Einzelprodukte wenigstens in irgendeiner Form zusammenarbeiten – mit enormem Aufwand für das IT-Team, das die vielen Insellösungen ständig auf dem neuesten Sicherheitsstand halten muss.

Ein besserer Ansatz wäre die Bereitstellung von Lösungen als Teil einer vollintegrierten Cybersecurity-Plattform mit Mesh-Architektur. Dieser vernetzte Plattformansatz bietet nicht nur eine stärkere Sicherheit und vereinfacht das Management sowie die Orchestrierung, sondern hat auch deutlich geringere Gesamtbetriebskosten als isolierte Lösungen.

Schutz überall

Ein WFA-Konzept braucht eine Security, die überall funktioniert: am Arbeitsplatz im Hauptsitz, im Homeoffice, auf Geschäftsreisen und allen anderen Orten, an denen Mitarbeiter heutzutage arbeiten. Jeder dieser Standorte bringt eigene Herausforderungen mit sich und erfordert spezielle Sicherheitstechnologie, damit ein lückenloser Schutz jederzeit gegeben ist.

In der Fortinet Global Ransomware Survey gaben 67 % der Unternehmen an, Ziel von Ransomware-Angriffen gewesen zu sein.[3]

Arbeiten in Unternehmensstandorten

Der sichere Zugang zu geschäftskritischen Anwendungen – und der Schutz der Netzwerke und Geräte, mit denen darauf zugegriffen wird – ist nach wie vor eine zentrale Komponente einer mehrstufigen Verteidigung, selbst wenn Mitarbeiter im Büro arbeiten. In den meisten Unternehmensstandorten gibt es Kundendaten, Server, Anwendungen, Identitätsinformationen, Anmeldedaten von Benutzern und Quellcode, die Hacker stark interessieren. Der Schutz von Benutzern, Geräten und Servern im Büro beginnt mit Next-Generation-Firewalls (NGFW) als erste von vielen Abwehrmaßnahmen für diese kritische Informationsquelle. Unternehmen sollten aber NGFWs unbedingt durch eine integrierte Kombination aus Endpunkt-Security, Zero Trust und Identitätsmanagement ergänzen:

- NGFWs schützen den Zugang von außerhalb mit einer fortschrittlichen Sicherheit für das gesamte Unternehmensgelände, Rechenzentren und Niederlassungen.
- ZTNA-Agenten und Identitätsdienste kontrollieren und schützen den Zugang zu Anwendungen und anderen Ressourcen. Ein Zero-Trust-Netzwerkzugang (ZTNA) bietet interne Kontrolle, da er den Zugriff auf Anwendungen, verschlüsselte Tunnel im Büro und Benutzerüberprüfungen regelt.
- Eine Endpunkt-Security wie EDR-Lösungen für die Benutzer- und Gerätesicherheit ermöglicht den Schutz von Benutzergeräten und interagiert mit den kritischen Daten.

In Büroumgebungen sollte es außerdem Netzwerk- und Sicherheitslösungen wie ein Secure SD-WAN geben. Diese bieten fortschrittliche Netzwerk-Tools speziell für eine einheitliche Security-Plattform, die die WAN-Konnektivität zwischen Rechenzentren, Clouds, Niederlassungen und jedem Betriebsgelände mit einer gezielten Anwendungserkennung optimiert.

Telearbeit und Homeoffice

Remote- und Hybrid-Mitarbeiter melden sich in der Regel von einer Homeoffice-Umgebung aus mit einem Laptop an, an das häufig ein weiterer Monitor und eine externe Webcam angeschlossen sind. Diese Heimnetzwerke sind jedoch oft unzureichend geschützt, verwenden WLAN-Router der Consumer-Klasse und umfassen manchmal sogar anfällige IoT-Geräte (Internet der Dinge), die Hacker als Einstiegspunkt ausnutzen können. Zudem bringen Videokonferenzen und andere bandbreitenintensive Aktivitäten das Heimnetz von Mitarbeitern an die Belastungsgrenze. Wenn dann noch Haushaltsmitglieder Videos streamen oder online spielen, wird die Bandbreite derart verringert, dass an kein produktives Arbeiten mehr möglich ist. Mitarbeiter im Homeoffice benötigen daher folgende Sicherheitslösungen:

- Endpunkt-Security wie EDR zum Schutz des Mitarbeiters und seiner Geräte
- ZTNA-Agenten und Identitätsdienste für einen kontrollierten, sicheren Zugang auf Anwendungen und andere Ressourcen
- Security der Enterprise-Klasse für Heimnetzwerke, um einen sicheren Zugang auf das Unternehmensnetzwerk sowie Anwendungen in der Cloud und im Rechenzentrum zu gewährleisten (mit Traffic-Management, um den geschäftlichen Datenverkehr gegenüber Video-Streaming oder Online-Spielen zu priorisieren)

Eine Homeoffice-Lösung muss den Firewall-Schutz des Unternehmens auf das gesamte Heimnetzwerk erweitern. Sie sollte auch das Heimnetzwerk segmentieren, um dem IT-Team Einblick in den geschäftlichen Datenverkehr zu geben und die Bandbreite für Geschäftsanwendungen zu optimieren, während gleichzeitig die Privatsphäre der Mitarbeiter für den privaten Bereich des Netzwerks gewährleistet wird.

Mobiles Arbeiten

Benutzer, die außerhalb des Unternehmensbüros oder fern ihres üblichen Remote-Arbeitsplatzes arbeiten, sind oft besonderen Bedrohungen ausgesetzt. Unterwegs oder auf Geschäftsreisen verbinden sich Mitarbeiter womöglich mit unbekannten, ungeschützten Netzwerken und Access Points, um auf benötigte Anwendungen und Ressourcen zuzugreifen – und riskieren damit, dass sich Angreifer unbemerkt ins Unternehmensnetzwerk einschleichen. Mobile Benutzer brauchen daher folgende Sicherheitslösungen:

- Endpunkt-Security wie EDR zum Schutz des Anwenders und seiner Geräte
- ZTNA-Agenten und Identitätsdienste für einen kontrollierten, sicheren Zugang auf Anwendungen und andere Ressourcen
- Remote-Netzwerk-Security mit SASE-Lösungen, die Mitarbeiter außerhalb des Büro- oder Heimnetzwerks mit cloudbasierten Firewall-Funktionen schützen

Eine mobile Netzwerklösung sollte zudem eine Multi-Faktor-Authentifizierung, ein cloudbasiertes Secure Web Gateway (SWG) und einen Cloud Access Security Broker (CASB) umfassen.

Integrierte WFA-Sicherheit, gestärkt durch Bedrohungsinformationen

Um ein ortsunabhängiges Arbeiten mit einer WFA-Strategie zu unterstützen, brauchen Unternehmen eine Cybersicherheits-Mesh-Plattform mit Lösungen, die als integriertes System funktionieren und eine praxisnahe Threat Intelligence bieten. Nur so lassen sich Security-Produkte auf dem neuesten Stand halten und aktuelle Bedrohungsinformationen in allen Arten von Standorten bereitstellen. Ein solcher Plattform-Ansatz bedeutet, dass Zero-Trust-, Endpunkt- und Netzwerk-Sicherheit mit gemeinsamen APIs für die Anwendungsprogrammierung und Integrationspunkten vereinheitlicht werden können. Auf diese Weise wird sichergestellt, dass Anwender nahtlos zwischen Standorten wechseln und überall durch eine konsequente, nahtlose Security geschützt sind. Zugleich profitiert die IT von einer simpleren Cyber-Sicherheit mit einer Mesh-Architektur, die das Erstellen und Durchsetzen von Richtlinien vereinfacht, einheitliche Konfigurationen gewährleistet, das Management zentralisiert und die Überwachung und Kontrolle von Benutzern, Geräten, Daten, Anwendungen und Workflows ermöglicht.

WFA-Strategien sind seit der Pandemie zwar wichtiger geworden, aber tatsächlich wurde damit nur ein ohnehin bestehender Trend beschleunigt. Fakt ist: Hybride Arbeitsmodelle haben sich mittlerweile erfolgreich durchgesetzt und Unternehmen müssen diese neue Flexibilität in der Arbeitswelt auf sichere Weise realisieren.

[1] „Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs“. Fortinet, August 2021.

[2] „Beyond Boundaries: The Future Of Cybersecurity In The New World Of Work“. Forrester, 2021

[3] „The 2021 Ransomware Survey Report“. Fortinet, 3. November 2021.

FORTINET

www.fortinet.com/de

Mai 6, 2022 1:14 PM
1400814-0-0-DE