SOLUTION BRIEF

Work-from-Anywhere: Sichere ortsunabhängige Arbeitsmodelle mit der Fortinet Security Fabric

Zusammenfassung

Arbeitsmodelle haben sich grundlegend weiterentwickelt. Unternehmen müssen heute die Mitarbeiterproduktivität an mehreren Standorten gewährleisten und zugleich die Belegschaft überall schützen – ob im Büro, im Homeoffice, an Telearbeitsplätzen, beim Kunden oder auf Geschäftsreisen. Die Fortinet Security Fabric bietet die nötige Endpunkt-, Netzwerk- und Fernzugriffssicherheit, damit Mitarbeiter von überall aus arbeiten können – Stichwort „Work-from-Anywhere (WFA)". Diese Security-Plattform der Enterprise-Klasse sorgt für eine einheitliche Nutzererfahrung an allen Standorten dank umfassender Management- und Reporting-Funktionen.

67 % der Cyber-Angriffe mit Folgen für das gesamte Unternehmen richteten sich gegen Remote-Mitarbeiter.[1]

Die Arbeitswelt im Wandel

Die Sicherheit am Arbeitsplatz ändert sich ständig – manchmal sogar von heute auf morgen, wie z. B. durch die neue Arbeitssituation während der Pandemie. Viele Unternehmen hatten zwar schon jahrzehntelang Telearbeit und Homeoffices unterstützt, aber nur ein geringer Prozentsatz der Belegschaft arbeitete bis vor kurzem regelmäßig außerhalb eines Firmenstandorts. Obwohl Videokonferenzen seit langem machbar sind, konnte sich Remote-Arbeit wegen Bedenken der Chefetage kaum durchsetzen. Telearbeit und Homeoffice blieben meistens die Ausnahme, nicht die Norm. Die Pandemie von 2020/21 hat all das verändert: Plötzlich musste die überwiegende Mehrheit der Arbeitnehmer aus der Ferne arbeiten. Entgegen den Befürchtungen blieb die Produktivität davon unberührt und Mitarbeiter lernten die Vorteile der Remote-Arbeit in der Praxis kennen. Schon allein aus diesen beiden Gründen spricht auch nach der weltweiten Ausnahmesituation nichts mehr gegen ein ortsunabhängiges Arbeiten. Folglich werden Unternehmen künftig mehr Mitarbeiter unterstützen, die regelmäßig zwischen mehreren Arbeitsplätzen wie Büro und Homeoffice wechseln oder unterwegs arbeiten wollen. Diese neuen Arbeitsmodelle bringen jedoch eine wachsende Angriffsfläche mit sich, die Unternehmen mit einer einheitlichen, unternehmenstauglichen Security wirksam schützen müssen.

Einheitliche Security überall

Die Fortinet Security Fabric bietet einen Schutz der Enterprise-Klasse für Endpunkte, Netzwerke und Fernzugriff. Fortinet ist damit einzigartig positioniert, um Mitarbeiter im Büro, im Homeoffice, an alternierenden Arbeitsplätzen und unterwegs umfassend zu schützen. Mit diesem Plattform-Ansatz entfällt die komplexe Verwaltung und Abstimmung vieler verschiedener Einzelprodukte und standortabhängiger Richtlinien. Stattdessen erhalten Unternehmen mit der Fortinet Security Fabric das nötige Rüstzeug zur Unterstützung hybrider Arbeitsmodelle: unternehmensweit einheitliche Richtlinien, eine konsequente Durchsetzung dieser Richtlinien und zentrale Reporting-Funktionen.

Telearbeit und Homeoffice

Durch die massive Umstellung auf Telearbeit und Homeoffices wurden schnell die Vor- und Nachteile von Remote-Arbeit sichtbar. Obwohl die Produktivität durch den Wegfall der Fahrt zur Arbeit und flexible Arbeitszeiten stieg, wirkten sich schlecht geschützte Heimnetzwerke und die fehlende Netzwerk-Kontrolle negativ auf Unternehmen aus. Die FortiGuard Labs verzeichnetem einen massiven Anstieg der Angriffe auf extern arbeitende Mitarbeiter, als plötzlich Millionen Remote-Angestellte mit ihren anfälligen, schlecht geschützten Heimnetzwerken, Geräten und Browsern die Angriffsfläche praktisch von heute auf morgen erweiterten.[2]

Der erste Schritt hin zu einem sicheren Fernzugriff ist der Abschied vom klassischen virtuellen Privat-Netzwerk (VPN) und die Einführung eines Zero-Trust-Network-Access (ZTNA). Mit einem Zero-Trust-Netzwerkzugang erhalten Unternehmen eine gründlichere Überprüfung und Authentifizierung von Benutzern und Geräten als bei einem VPN. Zudem automatisiert ein ZTNA die verschlüsselten Tunnel und unterstützt einen granularen Anwendungszugriff, was sowohl die Sicherheit als auch die Benutzererfahrung verbessert. Bei Fortinet ist der ZTNA bereits als kostenlose Funktion im FortiClient Fabric Agent und im FortiGate-Betriebssystem enthalten: Zum FortiClient Fabric Agent gehört ein ZTNA-Agent, über den ein Endpunkt verschlüsselte Tunnel zum ZTNA-Proxypunkt in einer FortiGate-Firewall aufbauen kann.

Dieser ZTNA-Proxypunkt authentifiziert den Benutzer, das Gerät, das Sicherheitsprofil des Geräts und die Benutzerrechte für den Zugriff auf eine bestimmte Anwendung.

Bedrohungsakteure konzentrieren sich bei Ransomware-Angriffen vor allem auf Laptops, die nicht durch die in Unternehmensstandorten üblichen Sicherheitsstufen geschützt sind. Unternehmen sollten daher Laptops mit EDR-Lösungen (Endpoint Detection und Response) schützen, die aktivierte Malware automatisch erkennt, stoppt und das Laptop auf den Zustand vor der Infektion zurücksetzt. FortiEDR bietet diese Funktionen und kombiniert künstliche Intelligenz (KI) mit vordefinierten Playbooks für automatisierte Reaktionen. Anders als die unzähligen EDR-Lösungen, die IT-Teams mit zu vielen Fehlalarmen belasten – und damit eine zeitnahe, wirksame Reaktion verzögern –, verwendet FortiEDR cloudbasierte Analysen und Abwehrmaßnahmen auf Kernel-Ebene. Diese verhindern eine potenzielle Malware-Verbreitung, während das IT-Team den Sicherheitsvorfall untersucht. Außerdem werden Programme aus Backups vor der Infektion wiederhergestellt und die Malware wird entfernt.

Hybride Arbeitsmodelle werden immer mehr zu einer Realität, der sich Unternehmen stellen müssen: 75 % der Arbeitnehmer erwarten heute mehr Flexibilität bei der Berufsausübung.[3]

Für Unternehmen sind Heimnetzwerke unter Sicherheitsaspekten problematisch. Einerseits müssen diese Netzwerke geschützt werden, andererseits darf eine höhere Sicherheit nicht den Durchsatz und damit die Produktivität ausbremsen. Normalerweise besteht der einzige Schutz von Heimnetzwerken in den Sicherheitsfunktionen von WLAN-Routern der Consumer-Klasse. Dazu kommt, dass andere Haushaltsmitglieder über das gleiche Heimnetzwerk womöglich Filme streamen, online spielen oder mit anderen Aktivitäten viel Bandbreite belegen. Eine Security auf Consumer-Niveau und die gemeinsame Nutzung der Bandbreite gefährden Unternehmensgeräte in einem Heimnetzwerk, können Videokonferenzen stören und somit die Produktivität stark beeinträchtigen. Gemeinsam mit Linksys bietet Fortinet für solche Fälle die Lösung *Linksys HomeWRK for Business | Secured by Fortinet* an, die die einfache Bedienung von Linksys leistungsstarken WLAN-Routern für Heimnetzwerke mit den unternehmenstauglichen Security- und Management-Funktionen von Fortinet kombiniert. Die Idee dahinter: Unternehmen stellen *Linksys HomeWRK for Business* für Mitarbeiter im Homeoffice bereit und gewährleisten damit eine Sicherheit der Enterprise-Klasse für das gesamte Heimnetz mit Priorität auf den Datenverkehr für Videokonferenzen. Die Transparenz und Kontrolle für den geschäftlichen Netzwerk-Teil liegt beim Unternehmen, für den privat genutzten Teil ist der Mitarbeiter zuständig.

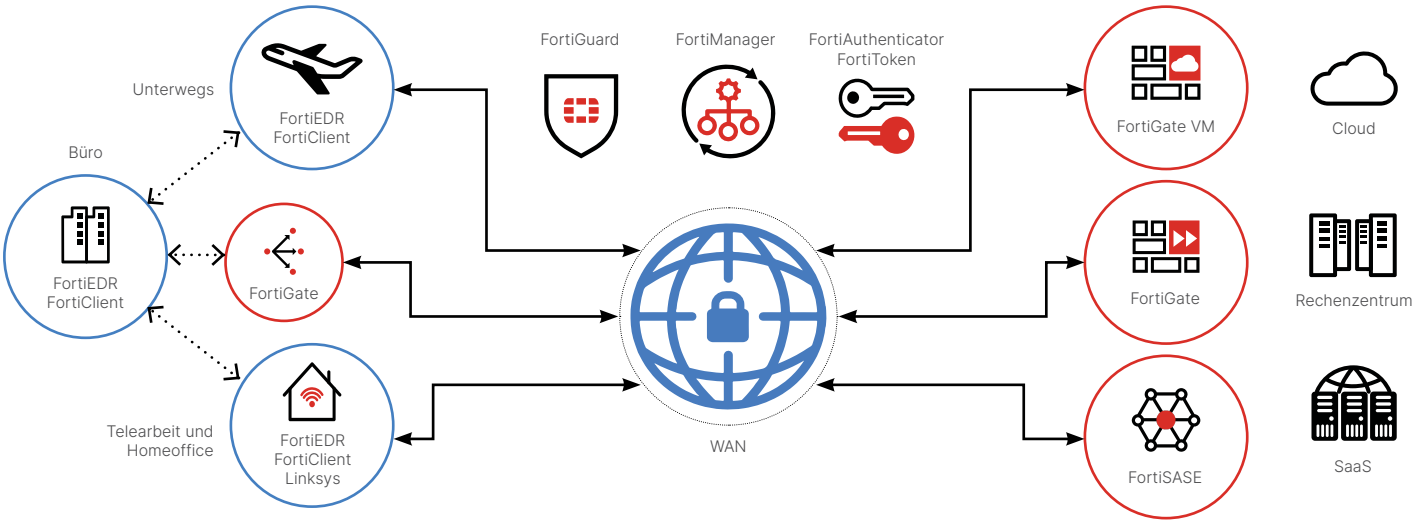

Abbildung 1: Work-from-Anywhere: Fortinet ermöglicht sicheres Arbeiten von überall aus.

Mobiles Arbeiten

Heutzutage wird nicht nur von einem einzigen Remote-Standort aus gearbeitet, sondern auch von anderen bürofernen Umgebungen wie Flughäfen, Hotelzimmern oder Cafés. In solchen Umgebungen müssen sich Mitarbeiter über nicht vertrauenswürdige Netzwerke mit Unternehmensressourcen verbinden. Für diese mobilen Anwender bieten die ZTNA- und EDR-Technologien von Fortinet die gleichen Vorteile wie für ein Heimnetzwerk: Die Lösungen kontrollieren den sicheren Zugriff auf Anwendungen und schützen Endgeräte vor Malware. Der ZTNA stellt den verschlüsselten Tunnel bereit, um die Kommunikation privat zu halten und den Benutzer und das Gerät zu authentifizieren – genau wie im Homeoffice. FortiEDR überwacht die Programme und Sitzungen auf dem Laptop und kann Maßnahmen ergreifen, wenn verdächtige Aktivitäten erkannt werden. Der Hauptunterschied zwischen dem Arbeiten im Homeoffice und dem mobilen Arbeiten ist das Netzwerk. Verbindet sich ein Mitarbeiter über ein Heimnetzwerk, kann sein Laptop mit zusätzlicher Hardware geschützt und kontrolliert werden, was unterwegs nicht möglich ist. Für mobile Remote-Mitarbeiter bietet daher eine cloudbasierte Security den besten Schutz: Hierbei verbindet sich der verschlüsselte ZTNA-Tunnel mit einem Point of Presence (POP), damit Sicherheitsdienste wie Firewalls, Secure Web Gateways, DLP, ZTNA-Proxy oder CASB den Benutzer und Datenverkehr schützen. Mit FortiSASE erhalten Unternehmen eine cloudbasierte Remote-Security mit dem gleichen Leistungsumfang wie bei FortiOS (dem Betriebssystem einer Fortinet FortiGate Firewall), nur eben als von Fortinet verwaltete Cloud-Instanz.

Arbeiten in Unternehmensstandorten

Büroumgebungen haben im Allgemeinen den stärksten Schutz mit verschiedenen Sicherheitsstufen für Mitarbeiter und vom Unternehmen gehostete Ressourcen. Aus gutem Grund: In Unternehmensstandorten befinden sich oft wichtige Geschäftsinformationen wie Betriebsgeheimnisse, Kundenlisten und Finanzdaten. Die meisten Unternehmen schützen daher Büros und Rechenzentren mit mehreren Next-Generation-Firewalls (NGFW), die Sicherheitsfunktionen wie eine Netzwerk-Segmentierung mit Richtlinien für die Anwendungssteuerung (Application Control), den Benutzerzugriff oder die Überprüfung des Datenverkehrs bieten. Fortinet FortiGates sind die weltweit am häufigsten installierten Next-Generation-Firewalls, weil Unternehmen jeder Größe damit eine umfassende Transparenz und Security erhalten. Zusätzlich zu diesen fortschrittlichen Sicherheitsfunktionen müssen Unternehmen aber auch den Anwendungszugriff und die im Büro verwendeten Laptops schützen und kontrollieren. Eine ZTNA- und EDR-Lösung empfiehlt sich ebenfalls für Büroumgebungen, damit Unternehmen in allen Standorten einheitliche Sicherheitsrichtlinien und eine mehrstufige Angriffsabwehr bereitstellen können.

Wesentliche unterstützende Technologien

Um Netzwerke, Endpunkte und den Anwendungszugriff zu schützen, müssen Sicherheitslösungen von bestimmten Schlüsseltechnologien unterstützt werden. Dazu gehört eine Identitäts- und Zugangsverwaltung mit Tools wie FortiAuthenticator und FortiToken, um eine Benutzeranmeldung mit einer Multi-Faktor-Authentifizierung (MFA) und unternehmensweiten Identitätsdiensten einzurichten. Ein weiteres Muss sind die FortiGuard Services, die FortiGate Next-Generation-Firewalls mit aktuellen Bedrohungsinformationen versorgen. Diese Threat Intelligence braucht die Firewall für ihre IPS-Engine und den Signaturabgleich, um bekannte Bedrohungen und Angriffe zu identifizieren. Management-Tools wie der FortiManager und FortiAnalyzer, die eine zentrale Transparenz und Kontrolle über die gesamte Plattform bieten, sind ebenfalls für den Schutz von Anwendern an jedem Standort notwendig – ob im Homeoffice, in Unternehmensstandorten oder unterwegs.

Neue Anforderungen verlangen neue Lösungen

Die Notwendigkeit, an mehreren Standorten arbeitende Mitarbeiter zu unterstützen, hat den Druck auf Netzwerk- und Security-Teams erhöht. Bisherige Technologien wie VPN-Verbindungen werden durch modernere Lösungen ersetzt, die sowohl die Sicherheit als auch die Nutzererfahrung verbessern. Das Besondere an Fortinet ist, dass sich mit diesem Security-Portfolio sämtliche Netzwerk- und Sicherheitstechnologien für ortsunabhängige Arbeitsmodelle bereitstellen lassen. Fortinet-Produkte stützen sich auf die Fortinet Security Fabric und schaffen so eine umfassende, integrierte und automatisierte Lösung, die alles schützt: von Endpunkten und Netzwerken bis hin zum Zugriff auf Anwendungen.

[1] „Beyond Boundaries: The Future Of Cybersecurity In The New World Of Work". Forrester, September 2021.

[2] Derek Manky: „Cyber Adversaries Are Exploiting the Global Pandemic at Enormous Scale". FortiGuard Labs, 12. August 2020.

[2] „Future of Work Reinvented: Returning to the Workplace – Differently". Gartner, 2021.

www.fortinet.com/de

20. Juni 2022, 00:39
1417262-0-1-DE