Avast Business

White paper

6 Gründe, weshalb Sicherheits-Appliances KMUs unzureichend schützen

16 September 2021

Avast Business

About the author

Rob Krug,
Senior Security Architect,
Avast Business

Rob has been in the network engineering and security space for over 30 years. His background includes extensive work with telecommunications, network design and management, and most importantly, network security. Specializing in security vulnerabilities, Rob has extensive experience in cryptography, ethical hacking, and reverse engineering of malware. Rob served in the U.S. Navy and also worked as a Data Security Analyst and Director of Engineering for multiple international service providers and vendors. Rob has designed, implemented, and maintained some of the most complex and secure networks imaginable.

Einführung

Vor einem Jahrzehnt war es für MSPs viel einfacher, mit UTMs und Sicherheits-Appliances den Schutz ihrer mittelständischen Kunden zu gewährleisten. Die Bedrohungen waren weniger komplex, darum wurden die meisten kleinen und mittleren Unternehmen (KMU) mit einer Kombination aus Virenschutz und Firewalls auf lokaler Basis geschützt. 2007 wurde die Unified Threat Management (UTM)-Appliance als fortschrittliche Firewall mit zusätzlichen All-in-One-Sicherheitsfunktionen eingeführt. Diese Appliances sollten KMUs helfen, ihren Unternehmensbereich kostengünstig zu schützen. Im Laufe der Zeit kamen bei UTMs Web-Content-Filterebenen hinzu, um Endpoints sowie Server und deren Daten vor webbasierten Bedrohungen zu schützen. Kurz nachdem die UTMs auf den Markt kamen, wurde eine neue Appliance namens Secure Web Gateway (SWG) entwickelt. SWGs waren eigenständige Appliances, deren Zweck vor allem der Schutz eines Unternehmens vor Web-Bedrohungen war.

Contents

Im Laufe der Jahre sind die UTM- und SWG-Appliance-Branchen stetig gewachsen und machen heute einen Jahresumsatz von insgesamt 4,9 Milliarden Dollar mit der Betreuung von Millionen von kleinen und mittleren Unternehmen, die anders als Konzerne nicht über Sicherheitsexperten und größere Budgets verfügen.

An dem Verkauf von UTM- und SWG-Appliances, Hot Spares, Upgrades und mehrjährigen Wartungsverträgen verdienen die Hersteller der Appliance-Branche Millionen. Vor 10 Jahren deckten diese Appliances einen großen

Avast Business

Bedarf ab, aber angesichts von Veränderungen in der Arbeitsweise und der mittlerweile erforderlichen Schutzmethoden für Daten sind sie heute veraltet.

Leider sind sich die meisten KMU-Verantwortlichen nicht bewusst, dass das Modell der lokalen KMU-Appliance implizite Sicherheitslücken aufweist, die zu einem Datenleck mit katastrophalen Folgen für das Unternehmen führen können. Dieses Whitepaper deckt die häufigsten Gründe auf, warum UTMs und Sicherheits-Appliances für MSPs und ihre KMU-Kunden nicht mehr ausreichen.

Grund Nr. 1: Appliances schützen nur einige Benutzer – und das nur zeitweise.

Die Zeiten, in denen Angestellte von 9 bis 17 Uhr im Büro saßen, sind größtenteils Geschichte. Durch die Verfügbarkeit von WLAN an fast jedem Ort ist es jetzt möglich, außerhalb des traditionellen Büroumfelds zu arbeiten. Zunehmend mehr Angestellte arbeiten von zu Hause aus, auf Geschäftsreisen, in Cafés oder Hotels – quasi überall, wo sie eine WLAN-Verbindung haben. Zusätzlich dazu haben auch Lieferanten, IT-Techniker, Freelancer und andere Personen Zugang zum Unternehmensnetzwerk, oft am Wochenende und außerhalb der Geschäftszeiten. Herkömmliche Appliances schützen nur die schwindende Zahl der festen Server und Workstations, die sich tatsächlich im Büro befinden. Laptops, private Geräte, Smartphones und Tablets, die zwischen Heim- und Unternehmensnetzwerk hin und her wechseln, sind nicht geschützt und bergen oft Risiken.

Ein weiterer Trend neben der erhöhten Mobilität ist das schrittweise Ersetzen großer Unternehmenszentralen zugunsten mehrerer, kleinerer Geschäftsstellen. Für die Vernetzung und Sicherung dieser Büros setzt die IT an jedem Standort meist auf eine Mischung aus MPLS-Standleitungen (Multiprotocol Label Switching), VPN-Leitungen oder redundante Sicherheits-Appliances. Dadurch wird der Schutz der einzelnen Geschäftsstellen naturgemäß teuer, ineffizient und komplex. Aus Unwissenheit oder um Zeit zu sparen, verbinden sich viele Mitarbeiter direkt mit dem Internet und umgehen dabei die interne Netzwerksicherheit. In diesem Fall verfügen die meisten über KEINERLEI Schutz, abgesehen von einem Antivirus-Programm.

Wie schützen Sie als IT-Service Provider die Mitarbeiter Ihrer Kunden außerhalb des Büros?

Grund Nr. 2: Appliances schützen nur einige Ihrer Daten.

Die Zeiten, in denen alle Unternehmensdaten zentral an einem Ort gespeichert waren, sind längst vorbei. In den letzten 10 Jahren hat eine große Verlagerung von lokalen Server- und zentralen Büroräumen zu den Cloud-basierten öffentlichen und privat gehosteten virtuellen Servern und virtuellen Rechenzentren stattgefunden. Im gleichen Zeitraum haben auch kleine und mittlere Unternehmen zunehmend Cloud-Anwendungen von Drittanbietern wie Office 365, Salesforce, Box und Hunderte anderer eingeführt.

Avast Business

Das heißt, dass Unternehmensdaten jetzt auf mehrere Server und Cloud-Rechenzentren verteilt sind. Neue 5G-Technologien werden den ohnehin schon rasanten Trend hin zu verteilten, Cloud-basierten Rechenzentren weiter fördern und beschleunigen.

In den meisten Unternehmen schützt die lokale Appliance heute nur noch einen Bruchteil der Unternehmensdaten, die früher vollständig vor Ort gespeichert wurden.

Wie schützen Sie als IT-Service Provider die Daten Ihrer Kunden außerhalb des Büros?

Grund Nr. 3: KMU-Appliances bieten keinen ausreichenden Schutz.

Während fast alle UTMs und SWGs über eine SSL/TLS-Entschlüsselungsfunktion verfügen, wird diese meist ausgeschaltet, weil sie häufig zu wenig performant ist, um den Anforderungen gerecht zu werden. Laut Gartner ist bei 90% der UTMs die SSL-Webinspektionsfunktion aufgrund von Latenzproblemen und/oder SSL-Zertifikatsfehlern deaktiviert. Dies verursacht eine klaffende Sicherheitslücke, durch die das Netzwerk nahezu völlig ungeschützt ist, da der überwiegende Teil des Geschäftsverkehrs (einschließlich Sicherheitsbedrohungen) heutzutage verschlüsselt ist!

Ohne aktivierte SSL-/TLS-Inspektion sind alle anderen Sicherheitsfunktionen der Appliance völlig nutzlos! Hinsichtlich SSL und den vielen anderen Konfigurationsoptionen sind die meisten Geräte falsch konfiguriert. Doch selbst wenn sie korrekt eingerichtet sind, erfordern sie Sicherheitsexperten, die sie ständig anpassen und Zertifikate aktualisieren, damit sie auf dem neuesten Stand bleiben und möglichst effektiv mit anderen Netzwerkgeräten zusammenarbeiten.

Ohne aktivierte SSL-/TLS-Inspektion sind alle anderen Sicherheitsfunktionen der Appliance völlig nutzlos!

Grund Nr. 4: KMU-Appliances verfügen nicht über die neuesten Sicherheitsinformationen.

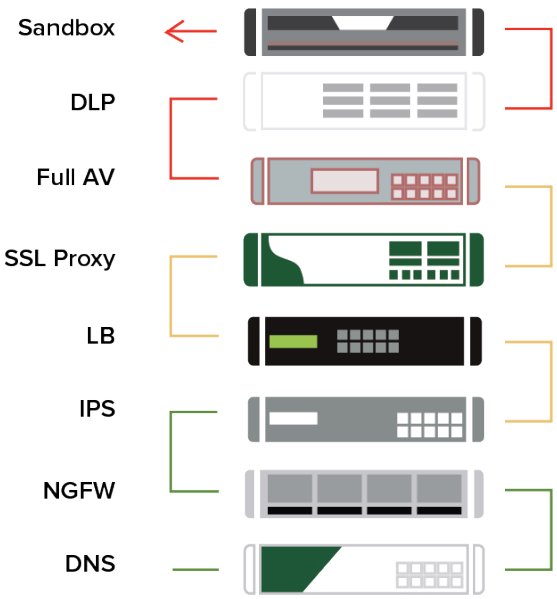
Die Abwehr gegen komplexe Bedrohungen sollte für ein KMU ebenso gut sein wie für ein großes Unternehmen, nur in einem kleineren, kostengünstigeren Umfang. Laut Small Business Trends werden KMUs zunehmend zur Zielscheibe für Hacker: **43% der Cyberangriffe richten sich gegen sie.**

Darüber hinaus gibt es täglich die unglaubliche Zahl von 125.000 neuen Bedrohungen. Leider werden bei den meisten lokalen Appliances nur selten Definitionsdateien heruntergeladen. Und diese neuen Varianten werden dann oftmals im Netzwerk zugelassen, bevor die Definitionsinformationen aktualisiert wurden.

Angesichts der Tausenden von neuen Bedrohungen pro Tag benötigen Service Provider Cloud-basierte Gateways, um zu gewährleisten, dass alle Kunden durch aktuelle Definitionen geschützt sind.

Avast Business

Grund Nr. 5: „All-in-One"-UTM-Appliances sind für Sie nicht ausreichend.



„All-in-One"-UTM-Appliances sind für Sie nicht ausreichend. UTMs werden zwar oft als „All-in-One"-Appliances angepriesen, sie enthalten allerdings nicht die verschiedenen Sicherheitsschichten, die zum Schutz kleiner und mittlerer Unternehmen erforderlich sind. UTMs bündeln mehrere Sicherheitsschichten in einer Lösung, dabei kommen Funktionsumfang, Features und Größe von Definitionsdateien jedoch oft zu kurz. Je nach Hersteller bieten die meisten UTMs keine integrierte E-Mail-Sicherheit, Antivirus-Endpoint Protection, Patch Management oder Identitäts- bzw. Passwortverwaltung – alles wichtige Komponenten einer umfassenden mehrschichtigen Sicherheitsstrategie für KMUs. Im Gegensatz dazu nutzt ein typisches Grossunternehmen mehrere, teure Lösungen zum Schutz jedes Bürostandorts, um Sicherheitslücken zu schließen. IT-Mitarbeiter in Grossunternehmen installieren in der Regel Punktlösungs-Appliances im Gegensatz zu einer All-in-One-UTM. Dabei handelt es sich quasi um leistungsstarke Computer, die auf eine bestimmte Sicherheitsschicht spezialisiert sind und damit verbundene Aufgaben meisterhaft ausführen.

Nicht zuletzt können ältere Appliances oft nicht mit dem Mitarbeiterwachstum und einer höheren Bandbreite Schritt halten. KMUs haben häufig einen 3- bis 5-jährigen Budgetzyklus und gefährden ihre Sicherheit und Produktivität, weil sie auf die nächste Gelegenheit zum Kauf warten.

Schon gewusst?

„Defense in Depth" – ein Ausdruck, der aus dem Militärbereich stammt – bezeichnet eine Strategie, die mehrere Sicherheitsmaßnahmen zum Schutz der Integrität von Informationen vorsieht. Bei diesem Konzept werden alle Aspekte der Unternehmenssicherheit abgedeckt – bei Bedarf absichtlich redundant. Wenn eine Abwehrlinie gefährdet ist, gibt es zusätzliche Abwehrschichten, die sicherstellen sollen, dass Bedrohungen nicht doch hindurchschlüpfen Diese Methode behebt die Schwachstellen, die unweigerlich in Technologie, bei Personal und im Betrieb innerhalb eines Netzwerks auftreten.

Die heutigen Cyberbedrohungen entwickeln sich fortlaufend und nehmen rasant zu. „Defense in depth" ist ein solider, umfassender Ansatz zur Nutzung einer Kombination aus fortschrittlichen Sicherheitstools, um kritische Daten zu schützen und Bedrohungen zu blockieren, bevor sie Endpoints erreichen.

ERFAHREN SIE MEHR ÜBER DEFENSE IN DEPTH UND MEHRSCHICHTIGE SICHERHEIT

Avast Business

Grund Nr. 6: Appliances sind mit versteckten Kosten verbunden.

Eine vorkonfigurierte Appliance kann natürlich attraktiv erscheinen. Die eigentliche Wahrheit ist jedoch, dass SWG- und UTM-Appliances nur einen kleinen Teil der Gesamtbetriebskosten ausmachen.

- Appliances haben in der Regel zusätzliche Support- und Wartungsverträge.
- Die Leistung der Appliance nimmt im Laufe der Zeit ab und sie muss in den meisten Fällen auf ein höheres Modell aufgerüstet werden, wenn:
    - SSL-Inspektion aktiviert wird zunehmend günstigere Bandbreite hinzugefügt wird, da die UTM dem Datenverkehr dann nicht mehr gewachsen ist neue Mitarbeiter und/oder Standorte hinzukommen
- Appliances sind ein „Single-point-of-failure". Wenn sie ausfallen benötigen Unternehmen, dann entweder Hot-Spare-Backups oder teure Verträge für Hochverfügbarkeit, um Ausfallzeiten zu reduzieren.
- Appliances erfordern IT-Experten vor Ort, die sie einrichten und regelmäßige Firmware- und Software-Upgrades durchführen. Ein gravierender Mangel an IT- und Sicherheitsexperten im KMU-Umfeld erhöht die Kosten zusätzlich.
- Zweigstellen benötigen entweder völlig neue Appliances oder teure MPLS-Standverbindungen, um den Datenverkehr über die Zentrale zu leiten.
- Appliances benötigen gesicherte Computerräume mit klimatisierten Racks, USV und Stromanschluss.

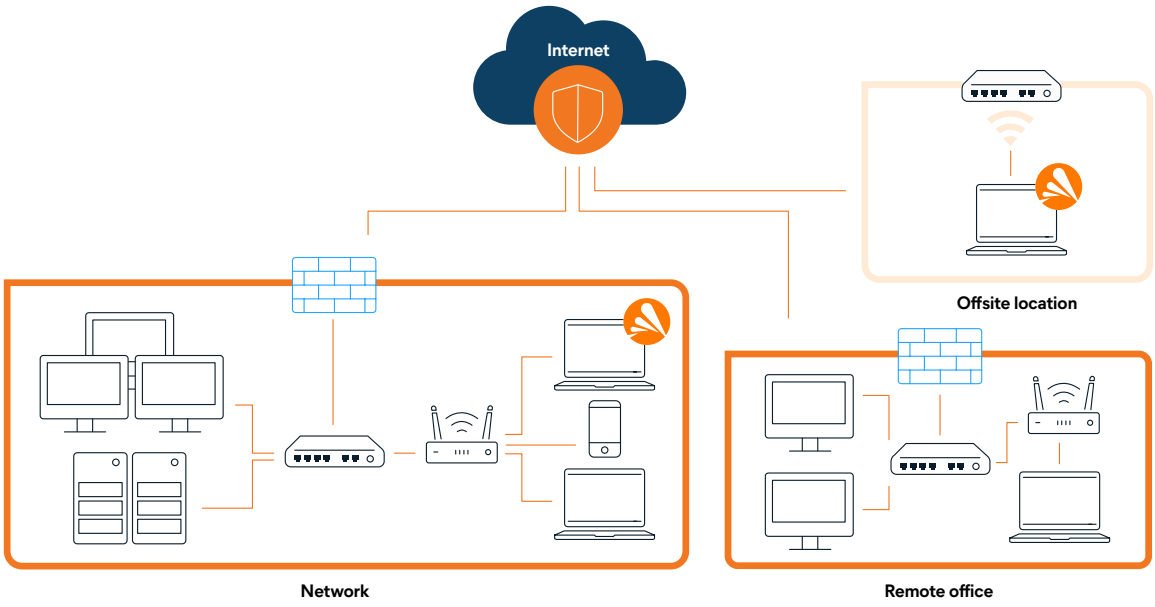
Alle diese Faktoren führen zu erhöhten Betriebskosten für Anbieter von Managed Services, ohne dass die KMU einen zusätzlichen Nutzen davon haben.

Alle diese Kosten sind allerdings gering verglichen mit dem potenziellen Schaden für Ihre Unternehmenstätigkeit aufgrund unzureichender Sicherheit!

Sicherheitslösungen für moderne KMU

Es ist klar, dass die gerätebasierten Sicherheitsmodelle der Vergangenheit – darunter die traditionellen Modelle „Burggraben" und „Nabe-Speiche" – aussterben. Komplexe, häufiger auftretende Bedrohungen plus die unaufhaltsame Verlagerung hin zu flexiblen Arbeitsmodellen, Cloud-basierten Servern und Cloud-Anwendungen machen es erforderlich, dass eine moderne Sicherheitslösung nicht an der Bürotür endet.

Avast Business



Letztendlich sind ältere Appliance-Modelle nicht so preiswert, wie es zunächst scheint. Außerdem können sie im Falle eines ernsthaften Datenlecks das Ende Ihres Unternehmens bedeuten.

Sicherheitsexperten sind sich einig, dass das Büro von heute das ganze Internet umfasst und deshalb auf neue und umfassende Art geschützt werden muss. Zum Glück gibt es ein aufkommendes Software-definiertes Sicherheitsmodell (SDSec), das die Sicherheitslücken herkömmlicher Methoden auf logischere, effizientere und wirksamere Weise schließt.

Wir von Avast Business wissen, dass die Cybersicherheit von heute schneller, intelligenter und zuverlässiger denn je sein muss. Wir bieten leistungsstarke, kostengünstige Sicherheitslösungen für kleine und mittlere Unternehmen, um sie vor Internetbedrohungen zu schützen.

Vereinbaren Sie einen Termin mit einem Business Security-Experten, um Antworten auf Ihre spezifischen Fragen zu erhalten und eine maßgeschneiderte Demo der Avast-Sicherheitslösung für KMU anzufordern.

DEMO ANFORDERN

Über Avast Business

Avast bietet All-in-One-Cyber Security-Lösungen für den modernen Arbeitsplatz von heute und bietet absolute Sicherheit. Avast bietet integrierte, 100% Cloud-basierte Endpoint- und Netzwerksicherheitslösungen für Unternehmen und ITDienstleister. Das Avast Business-Sicherheitsportfolio wird vom größten, weltweit am weitesten verbreiteten Netzwerk zur Erkennung von Bedrohungen unterstützt und macht es einfach und kostengünstig, komplexe Netzwerke zu sichern, zu verwalten und zu überwachen. Unsere einfach zu implementierenden Cloud-Sicherheitslösungen bieten maximalen Schutz, auf den sich Unternehmen verlassen können. Weitere Informationen zu unseren Cloud-basierten Cyber Security-Lösungen finden Sie unter **www.avast.com/business.**