Avast Business

White paper

Über die bisherigen Möglichkeiten hinausdenken:

Fünf Cybersicherheitsprobleme, die KMUs in Angriff nehmen müssen, um geschützt zu bleiben und wie MSPs helfen können

Das Argument, wieso KMUs auf erschwingliche, leicht zu implementierende, konzerntaugliche Sicherheitsmaßnahmen setzen sollten und wieso dies eine neue, interessante Chance für Managed Service Provider und MSSPs darstellt

27 September 2021

IDG CONNECT

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

Psychologen haben einen Begriff dafür. Optimistische Verzerrung. Dies beschreibt Menschen, die glauben, dass sie einer geringeren Wahrscheinlichkeit ausgesetzt sind, dass ihnen etwas Negatives widerfährt. Zu einem gewissen Grad sind die meisten kleinen und mittleren Unternehmen (KMUs), also Unternehmen mit bis zu 1000 Mitarbeitern dagegen nicht gefeit, insbesondere wenn es um Cybersicherheit geht.

Selbst diejenigen, die sich des Ausmaßes der Bedrohung bewusst sind, sind aus einem Mangel an Ressourcen und Know-How in Fragen Sicherheit für Hackerangriffe anfällig. Großkonzerne sind üblicherweise gut geschützt, da sie über ausgefeilte Cloud-basierte, Echtzeit-Erkennungssysteme verfügen, während KMUs häufig Gefahren ausgesetzt bleiben, was keineswegs unbemerkt bleibt.

Dem Verizon-Bericht über Verletzungen der Datensicherheit 2019 zufolge zielten 43 % aller Cyberangriffe auf kleine Unternehmen ab, da diese lediglich über einen rudimentären Schutz verfügen. Und für diese kleinen Unternehmen wird es nur noch schlimmer. Mit der Zunahme von Vertragsfirmen, Freiberuflern, mobilen Mitarbeitern und BYODs – die sich alle mit dem Unternehmensnetzwerk verbinden – steigt die Zahl der Bedrohungen und Sicherheitslücken erheblich

KMUs können es sich nicht leisten derart anfällig zu sein. Wie eine diesjährige Studie ergab, sind die mit Datenlecks verbundenen Kosten in den letzten 5 Jahren um 12 Prozent gestiegen und KMUs haben diese Kosten am schwersten getroffen. Der Studie zufolge haben Unternehmen mit weniger als 500 Mitarbeitern im Schnitt Verluste von über 2,5 Mio. US-Dollar hinnehmen müssen.

Was können also KMUs dagegen tun?

Zunächst einmal müssen sie diese Bedrohungen ernst nehmen und die Vorstellung beseitigen, dass KMUs nicht im Visier von Hackern stehen. Des Weiteren müssen sie mit dem Einsatz robuster, skalierbarer Abwehrmechanismen beginnen, die die mit der Änderung von Arbeitspraktiken und Geschäftsabläufen verbundenen Risiken bewältigen können.

Die Unterstützung von KMUs beim Aufbau eines besseren Schutzes stellt für Managed Service Provider (MSPs) und MSSPs eine riesige Chance dar, denn sie bringen Know-How mit und können durch die Bereitstellung von konzerntauglicher, auf KMUs zugeschnittener Sicherheitslösungen ein regelmäßiges Einkommen generieren.

Im Folgenden werden fünf grundlegende Probleme vorgestellt, die es zu berücksichtigen gilt, sowie eine glaubwürdige Lösung in Form unseres Secure Internet Gateway, oder kurz SIG.

Avast Business

1 Vergessen Sie, was Sie gestern gelernt haben.

Security Appliances sind für moderne Arbeitsgewohnheiten nicht mehr relevant

Die Zeiten haben sich geändert. Bei den modernen Arbeitskräften dreht sich alles um Mobilität, dezentrales Arbeiten und Flexibilität, damit die Arbeit getan wird. Das Risikopotenzial steigt, da Unternehmen sich zunehmend auf einzelne Geschäftseinheiten statt auf IT-Abteilungen verlassen, um zu bestimmen, welche Geräte und Anwendungen für ihre Angestellten am besten geeignet sind. Diese Dezentralisierung hat jedoch ihren Preis: den Verlust der Kontrolle und den Mangel an Sicherheitsüberwachung.

Unter Berücksichtigung von Strategien wie der Zunahme an BYOD, ist von KMUs zu bedenken, wie auf Geschäftsdaten heutzutage zugegriffen wird, und dass diese außerhalb der Firmenzentrale verwendet werden. Genauso wie Großkonzerne müssen sich KMUs mit der Idee anfreunden, dass es der Netzwerkperimeter durchbrochen ist und dieser Wandel erhebliche Konsequenzen für die Sicherheit hat.

Viele KMUs nutzen Security Appliances um ihre Netzwerke zu schützen, doch wir schätzen, dass heutzutage bis zu 73 Prozent des gesamten Web-Verkehrs diese Appliances umgehen, da die meisten UTMs keine Funktionen zur Überprüfung von SSL-Datenverkehr einsetzen. Solange KMUs keinen SSL-Datenverkehr untersuchen, sind alle anderen Sicherheitsfunktionen nutzlos!

„SSL/TLS-verschlüsselter Datenverkehr ist auf 73 Prozent gestiegen und die meisten UTMs verwenden keine Funktionen zur Untersuchung von SSL-Datenverkehr. Solange KMUs keinen SSL-Datenverkehr untersuchen, sind alle anderen Sicherheitsfunktionen nutzlos."

2 Behalten Sie den Durchblick mit der Cloud.

Der Wandel macht KMU-Schutzmaßnahmen redundant

Anwendungen, Daten und Infrastrukturverwaltung werden in die Cloud verlagert, sodass lokale Sicherheitslösungen schnell an Effizienz und Relevanz verlieren. Während KMUs Cloud-Computing-Ressourcen immer mehr Budget zuweisen, verlieren traditionelle Schutzmaßnahmen zunehmend an Effektivität.

Im besten Falle können Vor-Ort-Appliances nur einen Bruchteil der Unternehmensdaten schützen, was das Unternehmen angreifbar macht. Wir würden sogar soweit gehen und behaupten, dass UTMs nicht mehr sicher sind. Kleine Unternehmen von heute, die immer noch Büro-basierte Security Appliances verwenden sind einen Klick entfernt von einer Katastrophe oder vom finanziellen Bankrott.

„UTMs sind nicht mehr sicher – Kleine Unternehmen von heute, die immer noch Büro-basierte Security Appliances verwenden sind einen Klick entfernt von einer Katastrophe oder vom finanziellen Bankrott."

Avast Business

3 Vor-Ort-Appliances auf dem neusten Stand zu halten kann KMUs Kopfschmerzen bereiten

Die Tatsache, dass sich Arbeitsgewohnheiten naturgemäß weiterentwickeln sowie die Vielzahl an Geräten haben den Druck auf KMUs erhöht, wenn es darum geht ihre Sicherheit auf dem neusten Stand zu halten. Angesichts dessen, dass die Rate neuer Bedrohungsvarianten auf 125 000 pro Tag gestiegen ist, wird diese Aufgabe und unter Berücksichtigung der limitierten Ressourcen und knappen Budgets zu einem Ding der Unmöglichkeit.

Die meisten Vor-Ort-Appliances laden Bedrohungsdefinitionsdateien nicht umgehend herunter während immer neue Bedrohungsvarianten in den Umlauf kommen. Dies führt dazu, dass die Appliances selbst ungeschützt sind und diese Bedrohungsvarianten ins Netzwerk gelangen, bevor die Definitionslisten aktualisiert werden. Wie können also KMUs damit zurecht kommen?

Und dann gibt es noch das Problem der Skalierbarkeit. Wie stellen wachsende KMUs, die in neue Büros oder abgelegene Standorte expandieren, sicher, dass alle Standorte vollständig geschützt sind und dass das Netzwerk keinen Hackerangriffen ausgesetzt ist?

4 KMUs benötigen jede Menge Hilfe, auch wenn sie über die richtigen Sicherheitsfunktionen verfügen

Bei KMUs ist es keine Seltenheit, dass sie über einen Mix aus Sicherheitsanwendungen und Appliances verschiedener Anbieter verfügen. Dies hat jedoch nicht zwangsläufig dazu geführt, dass diese KMUs in der Vergangenheit immer geschützt waren, auch ohne die steigende Mobilität der Arbeitskräfte. Wie Gartner jüngst festgestellt hat, wurden selbst jene Unternehmen ausgeknipst, die über Appliances mit SSL-Funktionen verfügen.

Es handelt sich nicht unbedingt um Inkompetenz. Vielmehr ist es eine Frage eines Mangels an adäquaten Fertigkeiten. Das Problem der meisten KMUs besteht darin, dass es im Bereich Cybersecurity weltweit einen erheblichen Mangel an Fachkräften gibt. Eine jüngst veröffentlichte Studie hat ergeben, dass 74 Prozent aller Unternehmen von diesem Mangel betroffen sind und dass KMUs am meisten darunter leiden.

KMUs brauchen Know-How. Woher sollen KMUs die Sicherheit nehmen, dass sie in den immer komplexer werdenden Gefahrenumgebungen sicherheitstechnisch abgedeckt sind, ohne dafür ein Vermögen auszugeben? Hier sind Partner gefragt. MSPs und MSSPs haben die Möglichkeit sich weiterzuentwickeln und zu MSSPs zu werden, indem sie KMUs Dienstleistungen mit einem Mehrwert in Sachen Sicherheit anbieten. Und Avasts neues SIG kann das Herzstück davon sein, denn es bietet skalierbaren Cloud-basierten Schutz, frei von Hardware, auf den die führenden Unternehmen des Fortune Global 500-Rankings bereits umgestiegen sind. [see The Secure Internet Gateway (SIG) and why it matters].

Avast Business

5 Cyberkriminelle verlassen sich darauf, dass KMUs nichts tun

Wie zuvor erwähnt verlassen sich Cyberkriminelle darauf, dass KMUs an optimistischer Verzerrung leiden. Sie gehen davon aus, dass KMUs annehmen, dass ihnen nichts widerfahren wird, da sie so zu einem leichteren Ziel werden. Nichtstun ist daher keine Option.

KMUs müssen Ihren Schutz mithilfe von MSPs überdenken und ihn an moderne Geschäftspraktiken anpassen. Sie müssen ihre bestehenden Appliances überdenken und potentielle Schwachstellen in ihren Netzwerken und den Geräten ihrer Mitarbeiter identifizieren.

KMUs benötigen eine Strategie, die die Trends hin zu Mobilität und dezentraler Arbeit sowie die Nutzung von öffentlichen WLAN-Netzwerken in Hotels, Flughäfen und Cafés abdeckt. Sie brauchen ein besseres Verständnis für die Risiken, denen sie ausgesetzt sind, sowie Hilfe bei der Entwicklung einer Sicherheitslösung, die an ihr Budget und ihre Arbeitsgewohnheiten angepasst ist.

„KMUs benötigen eine Strategie, die die Trends hin zu Mobilität und dezentraler Arbeit sowie die Nutzung von öffentlichen WLAN-Netzwerken in Hotels, Flughäfen und Cafés abdeckt."

Secure Internet Gateway und warum es wichtig ist

Wie helfen wir MSPs ihren Kunden zu helfen? Indem wir eine skalierbare, konzerntaugliche, Cloud-basierte auf KMUs zugeschnittene Lösung anbieten, die Netzwerke vor Gefahren wie in SSL versteckten Bedrohungen, Zero-Day-Angriffen und Botnets, schützt, welche die herkömmlichen Sicherheitsperimeter leicht umgehen können.

Diese Verlagerung hin zu Mobilität und SaaS-Anwendungen innerhalb vieler KMUs hat zur Folge, dass immer mehr Mitarbeiter die traditionellen Netzwerksicherheitskontrollen umgehen. Wir haben Secure Internet Gateway (SIG) entwickelt, damit KMUs dieser Problematik effektiv und kosteneffizient entgegenwirken können.

SIG ist eine Cloud-basierte Lösung, die standortunabhängigen Echtzeitschutz anbietet. Es erfordert keine zusätzliche Vor-Ort-Hardware, was es kosteneffizient und skalierbar macht, während deutlich weniger Know-How erforderlich ist, wenn es darum geht, den Datenverkehr einfach ins Cloud-Firewall-Netzwerk zu leiten. Alles kann durch einen IT-Dienstleister eingerichtet und verwaltet werden. Hier sind die wichtigsten Features:

Avast Business

- SIG führt blitzschnelle intelligente Analysen von schwer zu untersuchendem verschlüsseltem SSL-/TLS-Datenverkehr durch und bietet somit besten Schutz und eine bessere Performance bei minimalem Verwaltungsaufwand.
- SIG bietet eine Cloud-basierte Sandbox für Zero-Day-Schutz, inklusive automatischen Scans von .exe- und .dll-Dateien von unbekannten Seiten auf Cyberbedrohungen. Wird eine Bedrohung erkannt, wird das jeweilige Objekt in die Sandbox verschoben und es wird über das gesamte Netzwerk hinweg automatisch eine Sperre darauf verhängt.
- Eine Cloud-basierte Firewall-Steuerung, die die Definition eines granularen Regelwerks für IPs, Ports und Protokolle ermöglicht
- Die Implementierung von SIG nimmt nur wenige Minuten in Anspruch und lässt sich einfach über mehrere Büros und Standorte hinweg skalieren.
- SIG schränkt die Durchsatzgeschwindigkeit in keinster Weise ein und eliminiert durch traditionelle UTM-Appliances verursachte Leistungsengpässe.
- SIG generiert übersichtliche Berichte.
- SIG ist leicht zu implementieren und konfigurieren, selbst wenn Sie an der Implementierung von Einstellungen zum erweiterten Schutz vor Bedrohungen interessiert sind, der verdächtige Inhalte, Phishing, Cookie-Diebstahl, Anonymisierer, Cross-Site-Scripting u.v.m. blockiert.
- In SIG haben Sie die Möglichkeit die Bandbreitensteuerung zu konfigurieren, um sicherzustellen, dass Anwendungen wie O365 priorisiert werden.

Die SIGnifikanz von KMU-Sicherheit

In Anbetracht der Zunahme an Bedrohungen, der geringeren IT-Kenntnisse und kleineren Budgets müssen MSPs und MSSPs konzerntaugliche, Cloud-basierte Sicherheitsdienste in Erwägung ziehen, die für ihre KMU-Kunden geeignet sind. Diese Security-Dienste sollten nicht nur den Standort schützen, sondern auch das gesamte Unternehmen.

Sicherheitsexperten sind sich einig, dass das Internet zum neuen Büro-Perimeter geworden ist. Hier ist ein umfassender Schutz erforderlich und MSPs sowie MSSPs können nun eine Antwort darauf haben, und zwar mit Know-How und einer konzerntauglichen Lösung zu einem KMU-freundlichen Preis.

Die Abwehr gegen komplexe Bedrohungen sollte für ein KMU ebenso gut sein wie für ein großes Unternehmen, doch es sollte nicht so kostspielig und einfacher in der Anschaffung, Bedienung, Implementierung und Aktualisierung sein. KMUs benötigen die Hilfe und das Know-How von Partnern, um das zu erreichen.

Avast Business

Dies ist eine Gelegenheit zu wachsen und neue Sicherheitslösungen für KMUs zu etablieren, die cloudbasierte Gateways wie Secure Web Gateway (SWG) mit SIG und erweiterter Endpoint-Sicherheit zu kombinieren. Es geht darum, über die bisherigen Grenzen hinauszudenken, vom Verkauf und der Wartung von Hardware wegzukommen, von einem MSP zu einem MSSP zu werden und die Gelegenheit kontinuierliche Einnahmen aus Cloud-basierten Lösungen beim Schopfe zu packen – und dabei Bedrohungen in Schach zu halten und Kunden glücklich zu machen.

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.**