Akamai

WHITEPAPER

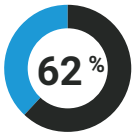
Kleine und mittelständische Unternehmen sind großen Bedrohungen ausgesetzt

Einführung

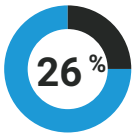
Cyberangriffe auf große Unternehmen sorgen zwar für Schlagzeilen, aber auch kleine und mittelständische Unternehmen (KMU) sehen sich zunehmend mit denselben Cybersicherheitsrisiken konfrontiert. Viele der heutigen Exploits unterscheiden nicht zwischen großen und kleinen Unternehmen, weil es den Angreifern ausschließlich um finanzielle Gewinne geht. Ihnen ist egal, wie groß ein Unternehmen ist, solange sie sich daran bereichern können. Kriminelle nutzen eine Vielzahl von Methoden, um Mitarbeiter und die Geräte, auf die sie angewiesen sind, anzugreifen – selbst weitverbreitete intelligente und vernetzte Geräte werden zum Ziel. Internetprovider sind gut aufgestellt, um KMU bei der Verteidigung gegen solche Angriffe zu unterstützen.

In diesem kurzen Artikel werden einige der häufigsten Bedrohungen, denen KMU ausgesetzt sind, und ihre Auswirkungen beschrieben.

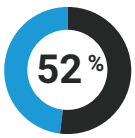
Die Technology and Small Business Survey der National Small Business Association zeigte einige interessante Statistiken auf:



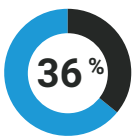
62 % der Kleinunternehmer gaben an, dass Cybersicherheit ein sehr wichtiges Anliegen sei, weitere 33 % gaben an, dass sie eher wichtig sei, und nur 5 % gaben an, dass sie überhaupt nicht wichtig sei



Nur 26 % der Unternehmer gaben an, dass sie verstanden hätten, wie man mit Cybersicherheitsproblemen umgeht



52 % sind sehr besorgt, dass ihr Unternehmen von einem Cyberangriff betroffen sein könnte und 44 % sind etwas besorgt, während 35 % berichten, dass sie bereits Opfer eines Cyberangriffs gewesen seien



36 % gaben an, dass Informationen fälschlicherweise von ihren Domains oder EMail-Adressen gesendet worden seien, 5 % gaben an, dass vertrauliche Informationen gestohlen worden seien, 4 % gaben an, dass auf Bankkonten zugegriffen worden sei, und 52 % gaben an, dass ein Angriff eine Serviceunterbrechung verursacht habe

Heutige webbasierte Bedrohungen können in zwei Hauptbereiche unterteilt werden: Malware und Phishing. Botnets sind eine wichtige Untergruppe von Malware, der besondere Aufmerksamkeit geschenkt werden muss.

Malware ist schädliche Software, die heimlich auf Geräten installiert wird. Manipulierte Websites können Softwarefehler auf einem Gerät ausnutzen, um Malware zu laden. Nutzer können auch dazu verleitet werden, zu einer schädlichen Website zu navigieren und dort eine schädliche Datei zu laden. So manche Malware kann sich auf einem Gerät aktivieren und dann selbstständig über ein Netzwerk verbreiten. Es gibt viele verschiedene Arten von Malware, die auf Unternehmen abzielen:

Kryptowährungs-Miner sind Programme, die Rechenleistung von unwissenden Opfern stehlen. KMU-Ressourcen werden kompromittiert, und diese Angriffe können schwer zu erkennen sein, weil Geräteinhaber – anders als bei Ransomware – nicht aufgefordert werden, Geld zu bezahlen.

Spezialisierte Malware, die auf POS-Geräte geladen wird, erfasst Kartendaten und leitet sie an den Angreifer weiter. Dadurch werden Unternehmer Sicherheitsbedrohungen ausgesetzt.

Advanced Persistent Threats (APTs) erlangen Zugriff auf Netzwerke und sammeln und extrahieren wertvolle Daten. APTs sind so konzipiert, dass sie extrem unauffällig sind, sodass sie über längere Zeit aktiv bleiben können. KMU können so wertvolle Daten verlieren – oder, noch schlimmer, das Vertrauen ihrer Kunden. Sie müssen auch mit behördlichen Maßnahmen rechnen, wenn personenbezogene Daten offengelegt werden.

Ransomware blockiert den Zugriff auf Dateien, indem sie alles auf einem Gerät oder Server verschlüsselt. Angreifer bieten den Entschlüsselungskey gegen einen erheblichen Geldbetrag an. In einigen Fällen händigen sie den Key sogar nach Erhalt des Geldes nicht aus. Im besten Fall verlieren KMU das Lösegeld. Im schlimmsten Fall verlieren sie das Geld *und* geschäftskritische Daten.

Es gibt mehrere Arten, auf die Malware wertvolle Daten sammelt. **Spyware** sucht nach Daten wie Anmelde- und Finanzdaten und sendet Berichte an Kriminelle. **Malware zur Datenexfiltration** wurde speziell dafür entwickelt, wertvolle Daten auf Computern zu finden, zu identifizieren und zu extrahieren. **Keylogger** zeichnen Tastenanschläge auf und können so trainiert werden, dass Kriminelle Zugriff auf Finanzkonten, Anmeldedaten für Social Media oder andere wertvolle Informationen erhalten. **Banking-Trojaner** überwachen das Nutzerverhalten, um Anmeldedaten abzugreifen und/oder Banking-Websites zu imitieren, um Geld zu stehlen.

Botnets sind Netzwerke von Geräten, die mit derselben Malware infiziert sind und über einen zentralen Kanal (Command and Control [C2]) von einem Verbrecher oder einer Gruppe gesteuert werden. Botnets stehen oft auch auf Auftragsbasis zur Verfügung – und die meisten können viele verschiedene Funktionen wie die oben beschriebenen ausführen, um Geld zu beschaffen.

Phishing nutzt Täuschung, insbesondere Social Engineering, um Opfer dazu zu verleiten, Informationen freizugeben, die ein Angreifer monetarisieren kann. In der Vergangenheit haben Phishing-Angriffe Nutzer dazu verleitet, in unaufgeforderten Spam-E-Mails auf Links zu klicken und vertrauliche Informationen offenzulegen. Entwickler von Phishing-Angriffen haben ihre Aktivitäten erheblich diversifiziert und integrieren inzwischen auch Phishing-URLs in Social-Media-Beiträge oder -Kommentare sowie Textnachrichten, SMS, Skype, Messenger oder andere Service.

Mobilgeräte sind die wichtigsten Phishing-Ziele – dank ihrer kleinen Bildschirmen und multitaskenden Nutzern, die subtile Hinweise auf einen schädlichen Link übersehen können. Um es noch schwieriger zu machen, imitieren Phisher legitime Domainnamen mit ähnlichen Zeichen aus verschiedenen Zeichensätzen.

Dies sind echte Beispiele für verwendete Zeichenketten:

7eleven.com

Adîdas.com

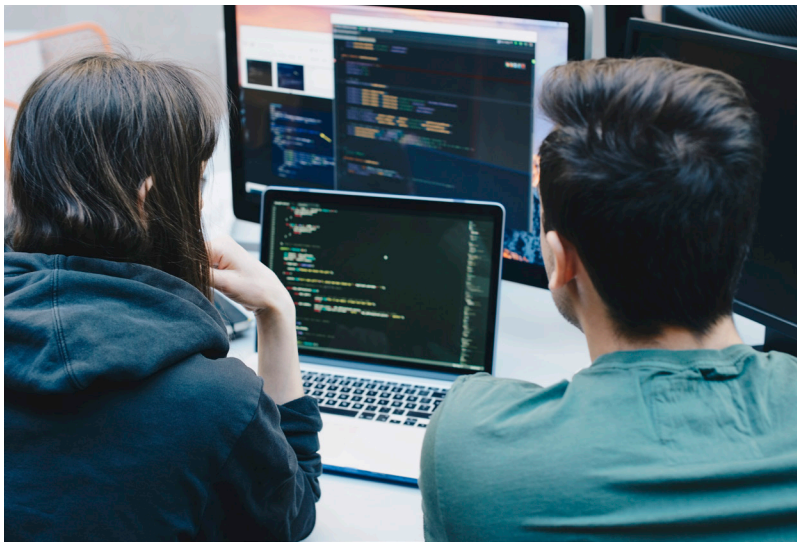
adidąs.com

philippineairlınes.com

rolex.com

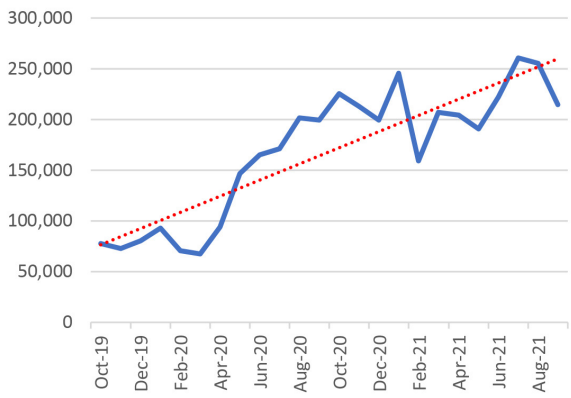
singaporeaır.com

thaiairways.com



In letzter Zeit ist beim Phishing ein Wachstumstrend zu beobachten. Der Phishing Activity Trends Report der Anti-Phishing Working Group für das 3. Quartal 2021 berichtet: „Phishing erreicht im 3. Quartal monatlichen Rekord; Angriffe seit Ende 2019 verdoppelt." Die nachfolgende Grafik aus dem Bericht veranschaulicht diesen Trend. Dies liegt daran, dass es einfacher sein kann, einen Nutzer zu einer unbeabsichtigten Aktion zu verleiten, als Softwarefehler auszunutzen.

Phishing-Angriffe, 4. Quartal 2019 bis 3. Quartal 2021



Die gesammelten Daten der Research-Teams für Betreiber- und Unternehmenssicherheit von Akamai zeigen außerdem, dass die Lebensdauer der für Phishing verwendeten Domainnamen zurückgeht, wobei der Mittelwert im März 2019 auf etwa 1,5 Stunden zurückging. Dies hat direkte Auswirkungen auf den Schutz: Die Abwehr muss ebenso agil sein wie die Angriffe.

Fazit

Dies ist keine erschöpfende Liste von Web-Bedrohungen. Angreifer prüfen ständig die Umsetzbarkeit ihrer Exploits und entwickeln sie weiter, um ihren Gewinn zu maximieren. Dabei verändern sie das Aussehen und die Funktion ihrer Arbeit ständig. Es gibt auch andere Arten von Malware, die in erster Linie eher ablenkend oder lästig sind und unerwünschte Werbung oder Inhalte zeigen.

KMU müssen vor webbasierten Bedrohungen durch Lösungen geschützt werden, die mit ihren individuellen Anforderungen und Einschränkungen kompatibel sind. Akamai bietet Secure Internet Access Services speziell für kleine und mittelständische Unternehmen an. Sie schützen kleine und mittelständische Unternehmen vor den in diesem Dokument beschriebenen Angriffen, ohne dabei einen Verwaltungsaufwand zu erzeugen. Jedes Gerät und jede Person am Arbeitsplatz, einschließlich der Gäste, ist automatisch geschützt. Unternehmensmanager erhalten ein einfaches grafisches Portal, über das sie sofort sehen können, was in ihrem Netzwerk passiert und welche Bedrohungen abgewehrt wurden.

Akamai Secure Internet Access Services wurden speziell entwickelt, um ISPs bei den folgenden Aufgaben zu unterstützen:

- Umsatzgenerierung mit Sicherheitsmaßnahmen der Enterprise-Klasse für KMU
- Zuverlässige und schnelle Bereitstellung sowie Differenzierung der Services für verschiedene Sicherheitsanforderungen
- Minimierung der Bereitstellungsbarrieren, Kostensenkung und Vereinfachung der Servicebereitstellung mit einer cloudbasierten Version der Secure Internet Access Services

Der Service kann komplett mit einem markenorientierten Erscheinungsbild individuell angepasst werden. Der Funktionsumfang und die Threat Intelligence können auch auf lokale Marktanforderungen zugeschnitten werden.

Jede Person. Jedes Gerät. Jederzeit. Akamai bietet die Lösung.

Wenden Sie sich jetzt an Akamai, um mehr zu erfahren.

Akamai

Akamai unterstützt und schützt das digitale Leben. Führende Unternehmen weltweit setzen bei der Erstellung, Bereitstellung und beim Schutz ihrer digitalen Erlebnisse auf Akamai. So unterstützen wir täglich Milliarden von Menschen in ihrem Alltag, bei der Arbeit und in ihrer Freizeit. Mithilfe der am meisten verteilten Computing-Plattform – von der Cloud bis zur Edge – ermöglichen wir es unseren Kunden, Anwendungen zu entwickeln und auszuführen. So bleiben die Erlebnisse nahe beim Nutzer und Bedrohungen werden ferngehalten. Möchten Sie mehr über die Sicherheits-, Computing- und Bereitstellungslösungen von Akamai erfahren? Dann besuchen Sie uns unter akamai.com und akamai.com/blog oder folgen Sie Akamai Technologies auf Twitter und LinkedIn. Veröffentlicht: 06/22.