Akamai

DOCUMENTO

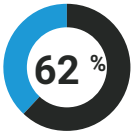
Las PYMES afrontan grandes amenazas

Introducción

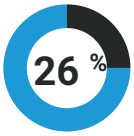
Los ciberataques a grandes empresas son noticia, pero cada vez es más frecuente que las pequeñas y medianas empresas (pymes) se enfrenten a los mismos riesgos de ciberseguridad que las grandes. Muchos de los ataques no discriminan, ya que a los atacantes únicamente les interesa la ganancia económica. No les importa lo grande que sea una empresa si pueden ganar dinero. Los criminales usan una variedad de métodos para atacar a los trabajadores y los dispositivos de los que dependen, incluso dispositivos conectados inteligentes cuyo uso está muy extendido. Los proveedores de servicios de Internet están bien posicionados para ayudar a las pymes a defenderse.

En este breve documento se describen algunas de las amenazas más comunes a las que están expuestas las pymes, así como el impacto que tienen.

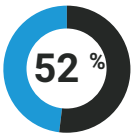
La encuesta Technology and Small Business Survey, publicada por la National Small Business Association, reveló un gran número de estadísticas interesantes:



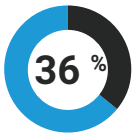
El 62 % de los propietarios de pequeñas empresas afirma que la ciberseguridad es un aspecto muy importante, un 33 % dice que es algo importante y solo el 5 % piensa que no es importante en absoluto.



Solo el 26 % de los propietarios de negocios afirma que sabe cómo lidiar con problemas de ciberseguridad



Al 52 % le preocupa mucho que su negocio pudiera verse afectado por un ciberataque. Al 44 % le preocupa un poco, mientras que el 35 % declara haber sido víctima de un ciberataque.



El 36 % afirma que se ha enviado información de manera falsa desde sus dominios o direcciones de correo electrónico. El 5 % denuncia el robo de información delicada, el 4 % el acceso no autorizado a cuentas bancarias y el 52 % haber sufrido un ataque que provocó la interrupción de los servicios.

Las amenazas actuales basadas en la web se pueden clasificar, a grandes rasgos, en dos áreas principales: malware y phishing. Las botnets son un importante subconjunto de malware que requieren una atención especial.

El malware es un software malicioso que se instala de manera secreta en los dispositivos. Los sitios web afectados pueden aprovechar las vulnerabilidades de software de un dispositivo para cargar malware. Los usuarios también pueden ser engañados para acceder a un sitio web malicioso y hacer clic para cargar un archivo infectado. Algunos programas de malware pueden activarse en un dispositivo y, a continuación, propagarse a través de una red por sí solos. Existen muchos tipos diferentes de malware dirigidos a las empresas:

Los mineros de criptomonedas son programas que utilizan la potencia de procesamiento de un dispositivo sin el consentimiento de la víctima. Los recursos de las pymes se ven afectados, y estos ataques pueden ser difíciles de detectar porque, a diferencia del ransomware, a los propietarios de los dispositivos no se les pide que paguen un rescate.

El malware especializado cargado en dispositivos de puntos de venta captura los datos de las tarjetas de pago y los envía a un sitio pirata, lo que expone a riesgo a los propietarios de negocios.

Las amenazas persistentes avanzadas (APT) obtienen acceso a las redes y recopilan y extraen datos valiosos. Estas APT están diseñadas para ser extremadamente sigilosas, de modo que pueden permanecer activas durante períodos prolongados. Las pymes pueden perder datos valiosos o, lo que es más importante, la confianza del cliente. También pueden estar sujetas a acciones reglamentarias si se exponen los datos personales.

El ransomware bloquea el acceso a los archivos mediante el cifrado de todo el contenido presente en un dispositivo o servidor. Los atacantes ofrecen la clave de descifrado a un coste elevado, aunque en algunos casos recogen el pago y no envían la clave. En el mejor de los casos, las pymes pierden el dinero del rescate. En el peor de los casos, *además* del dinero, pierden datos críticos para el negocio.

El malware recopila datos valiosos de distintas maneras. **El spyware** busca datos como credenciales de inicio de sesión y datos financieros, y envía informes a los delincuentes. El malware de

exfiltración de datos está diseñado específicamente para localizar, identificar y extraer datos valiosos de los ordenadores. **Los keyloggers** registran las teclas pulsadas y se pueden entrenar para permitir a los delincuentes acceder a cuentas financieras, credenciales de acceso de las redes sociales u otra información valiosa. **Los troyanos bancarios** monitorizan el comportamiento de los usuarios para descubrir las credenciales de inicio de sesión o suplantar sitios web bancarios para robar dinero.

Las botnets son redes de dispositivos infectados con el mismo malware que un delincuente o grupo común controla a través de un canal central (llamado comando y control [C2]). A menudo, las botnets están disponibles como "servicio de alquiler", y la mayoría puede realizar muchas funciones diferentes, como las descritas anteriormente, para generar dinero.

El phishing utiliza el engaño, especialmente la ingeniería social, para inducir a las víctimas a divulgar información que un atacante puede monetizar. En el pasado, los ataques de phishing tentaban a los usuarios a hacer clic en enlaces en correos electrónicos de spam no solicitados y a divulgar información confidencial. Los desarrolladores de ataques de phishing han diversificado sus esfuerzos de manera sustancial; ahora también incorporan URL de phishing en publicaciones o comentarios de redes sociales, así como mensajes de texto, SMS, Skype, Messenger u otros servicios.

Los dispositivos móviles son los principales objetivos del phishing, pues, al tener pantallas pequeñas y realizarse en ellos múltiples tareas, los usuarios podrían no darse cuenta de que un enlace es malicioso. Para que sea incluso más engañoso, los atacantes utilizan caracteres similares de diferentes conjuntos de caracteres para imitar nombres de dominio legítimos.

Estos son ejemplos reales de cadenas de caracteres que se han utilizado:

7eleven.com

Adîdas.com

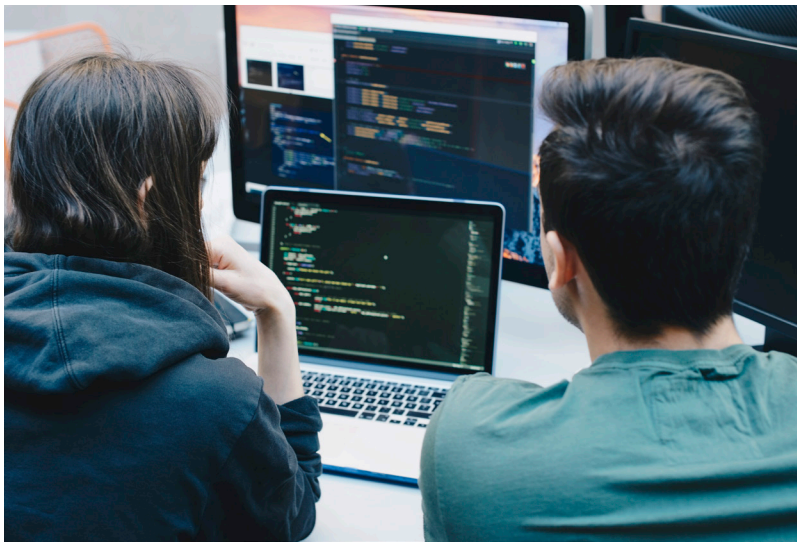
adidąs.com

philippineairlınes.com

rolex.com

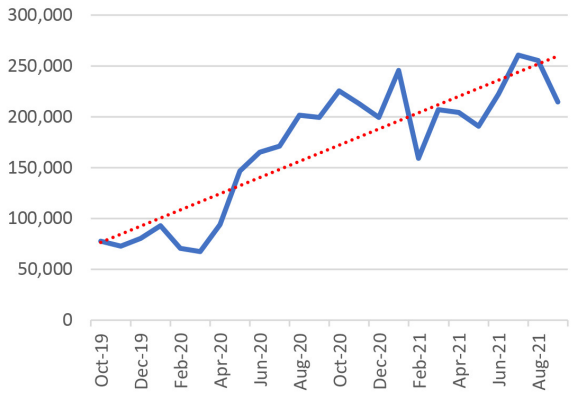
singaporeaır.com

thaiairways.com



Últimamente, los ataques de phishing tienen una tendencia al alza. En el informe sobre tendencias de phishing del tercer trimestre de 2021 Phishing Activity Trends Report, publicado por el Grupo de Trabajo Antiphishing, se recoge lo siguiente: "El phishing alcanza el récord mensual en el tercer trimestre; los ataques se han duplicado desde finales de 2019". La siguiente tabla, extraída del informe, ilustra la tendencia. Esto se debe a que engañar a un usuario para que realice una acción no intencionada es más fácil que aprovechar las vulnerabilidades del software.

Ataques de phishing, T4 2019 - T3 2021



Los datos recopilados por el operador de Akamai y los equipos de investigación de seguridad empresarial también muestran que la duración de los nombres de dominio utilizados para el phishing está disminuyendo. La media se ha reducido a, aproximadamente, 1 hora y media en marzo de 2019. Esto tiene consecuencias directas para la protección: Las defensas deben ser tan ágiles como los ataques.

Conclusión

Esta no es una lista exhaustiva de amenazas web. Los atacantes evalúan constantemente la viabilidad de sus ataques e innovan para maximizar sus beneficios, por lo que el aspecto y el mecanismo de funcionamiento de sus programas cambia continuamente. Además, existen otros tipos de malware que son principalmente una distracción o molestia, que muestran anuncios o contenido no deseados.

Las pymes deben protegerse de las amenazas basadas en la web con soluciones que se adapten a sus necesidades y condicionantes específicos. Akamai ofrece los servicios Secure Internet Access diseñados para pymes a fin de protegerlas de los tipos de ataques descritos en este documento sin imponer una carga de gestión. Todos los dispositivos y usuarios presentes en un lugar de trabajo, incluidos los invitados, se protegen automáticamente. Los responsables empresariales disponen de un portal gráfico simple donde pueden ver instantáneamente lo que está sucediendo en su red y qué amenazas se han disuadido.

Los servicios Secure Internet Access de Akamai están diseñados específicamente para ayudar a los ISP a:

- Generar ingresos con defensas de seguridad de nivel empresarial para pymes
- Ir más allá de la velocidad y la fiabilidad, haciendo que los servicios para las pymes se diferencien por la seguridad
- Minimizar los obstáculos a la implementación, reducir los costes y simplificar la entrega de servicios con una versión basada en la nube de los servicios Secure Internet Access

El servicio se puede personalizar completamente con un “aspecto y sensación” conformes a la propia marca, y el conjunto de funciones y la inteligencia ante las amenazas también se pueden adaptar a los requisitos del mercado local.

Cualquier persona. Cualquier dispositivo. En cualquier momento. Akamai puede ser de gran ayuda.

Póngase en contacto con Akamai para obtener más información.

Akamai potencia y protege la vida online. Las empresas líderes de todo el mundo eligen Akamai para crear, proteger y ofrecer sus experiencias digitales, ayudando así a millones de personas a vivir, trabajar y jugar cada día. Gracias a la plataforma informática más distribuida del mundo, de la nube al Edge, nuestros clientes pueden desarrollar y ejecutar las aplicaciones con facilidad, mientras acercamos las experiencias a los usuarios y mantenemos las amenazas a raya. Para obtener más información acerca de las soluciones de seguridad, informática y distribución de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en Twitter y LinkedIn. Publicado en junio de 2022.