SONICWALL

RESUMEN EJECUTIVO: POR QUÉ LAS AMENAZAS AVANZADAS REQUIEREN SEGURIDAD DE CORREO ELECTRÓNICO AVANZADA

El ransomware y las amenazas desconocidas hacen que la seguridad de correo electrónico sea más crucial que nunca

Resumen

En el mundo hiperconectado de hoy en día, las comunicaciones vía e-mail no solo son comunes, sino que además se han convertido en un elemento fundamental para hacer negocios de forma efectiva. Asimismo, se prevé que el volumen total de e-mails enviados al día en todo el mundo aumentará como mínimo en un 5% anualmente. Dada su naturaleza omnipresente, el correo electrónico constituye un vector crítico que las organizaciones deben proteger.

El uso del correo electrónico continúa en aumento

A pesar de la proliferación de los mensajes de texto y los medios sociales, la comunicación vía e-mail continúa creciendo con fuerza. Según un estudio realizado recientemente por The Radicati Group, el volumen total de e-mails enviados y recibidos al día en todo el mundo ha alcanzado los 205.000 millones, y se prevé que aumente como mínimo en un 5% anualmente.[1] Los hackers, conscientes de ello, buscan constantemente oportunidades para explotar los sistemas de las organizaciones.

1 The Radicati Group, Inc., Email Statistics Report, 2015-2019

Anatomía de un ataque por correo electrónico:

- Un CFO recibe un e-mail del CEO para autorizar una transferencia de fondos para una emergencia. Sin embargo, el e-mail en realidad ha sido enviado por un cibercriminal.
- Un empleado que cuenta con derechos administrativos para acceder a los sistemas clave recibe un e-mail urgente del departamento de TI para actualizar la contraseña de su red. Sin saberlo, facilita su contraseña a los cibercriminales.
- Un empleado recibe un e-mail con un archivo adjunto importante sobre su proveedor de beneficios. Al abrir el archivo adjunto para leerlo, activa un malware troyano oculto.

Las amenazas vía e-mail a las que se enfrentan las organizaciones en la actualidad

Los e-mails ofrecen a los hackers un vehículo para introducir diversas vulnerabilidades a las organizaciones. Estas son algunas de las amenazas basadas en correo electrónico más comunes:

- **Ransomware:** Una variante de malware especialmente perniciosa es el ransomware. Una vez que se activa el archivo adjunto al e-mail, el código se embebe en la red y el ransomware normalmente cifra o bloquea archivos y sistemas críticos. Entonces, los hackers coaccionan a la organización para que pague una extorsión a cambio del descifrado o desbloqueo de sus archivos o sistemas. El correo electrónico es el vehículo preferido para entregar ransomware, ya sea mediante archivos infectados o URLs maliciosas.
- **Spear Phishing / Whaling:** Esta variante de phishing va dirigida contra individuos clave, como responsables de TI o de la red, o ejecutivos de la empresa, y utiliza e-mails infectados con malware que aparentan proceder de una fuente fiable, con la intención de acceder a sistemas y datos internos. Más del 90% de los ciberataques empiezan con una campaña de phishing lanzada con éxito.[1]
- **Compromiso del correo electrónico de negocio / Fraude al CEO / E-mails de impostores:** Según las últimas cifras del FBI,[2] durante los últimos años, los ataques de Compromiso del correo electrónico de negocio (BEC) han provocado pérdidas por un valor total de como mínimo 5.300 millones de dólares, afectando a aproximadamente 22.000 empresas de todo el mundo. El FBI define el Compromiso del correo electrónico de negocio como un sofisticado ataque por correo electrónico dirigido contra empresas que trabajan con socios extranjeros y que realizan regularmente pagos vía transferencia por cable.
- **Phishing:** Esta táctica común consiste en enviar e-mails con enlaces embebidos a páginas de hackers. Cuando los usuarios, ajenos al peligro, visitan estas páginas, se les pide que introduzcan información personal, que los hackers utilizan para robar identidades, comprometer datos corporativos o acceder a otros sistemas críticos.
- **Malware:** El correo electrónico es uno de los principales mecanismos de entrega utilizados para distribuir malware tanto conocido como desconocido. Los hackers suelen embeber el malware en los archivos adjuntos del correo electrónico con la esperanza de que el destinatario abra o descargue el archivo adjunto en un ordenador o en una red, permitiéndoles acceder a los recursos, robar datos o colgar los sistemas.
- **Spam:** Los e-mails se utilizan para enviar mensajes spam o no solicitados, que pueden colapsar las bandejas de entrada y los recursos de red, reducir la productividad del negocio y aumentar los costes operativos.
- **Secuestro de e-mails salientes:** Las empresas también están sujetas a políticas corporativas y a normas gubernamentales, que les hacen responsables de sus e-mails salientes y de proteger los datos personales de sus clientes. Los ataques zombie y el secuestro de IP pueden difundir los datos personales de los clientes, arruinando la reputación de una empresa.

Conclusión

Actualmente, las comunicaciones vía e-mail son esenciales para las organizaciones, un hecho que los hackers saben aprovechar. Dada la naturaleza sofisticada y específica de los ataques actuales, es imprescindible para las empresas implementar una solución de seguridad multicapa que ofrezca una protección avanzada para el correo electrónico. Para combatir de forma efectiva las amenazas emergentes de hoy en día, las organizaciones deberían utilizar una solución de próxima generación de gestión de la seguridad de correo electrónico que les proporcione prestaciones de prevención de brechas en tiempo real.

Si desea obtener más información sobre cómo puede proteger el correo electrónico de su organización, lea nuestro resumen de la solución What your next-gen email security needs to stop advanced threats (Qué necesita su solución de seguridad de correo electrónico de próxima generación para detener las amenazas avanzadas).

1 www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
2 www.ic3.gov/media/2016/160614.aspx

Acerca de nosotros

SonicWall lleva más de 25 años combatiendo la industria del crimen cibernético, defendiendo a las empresas pequeñas, medianas y grandes de todo el mundo. Nuestra combinación de productos y partners nos ha permitido crear una solución de defensa cibernética en tiempo real adaptada a las necesidades específicas de más de 500.000 negocios en más de 150 países, para que usted pueda centrarse por completo en su negocio sin tener que preocuparse por las amenazas.

Si tiene alguna duda sobre el posible uso de este material, póngase en contacto con nosotros:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Para más información, consulte nuestra página Web.
www.sonicwall.com