Productos CrowdStrike

CROWDSTRIKE

REALIDADES RANSOMWARE PARA PEQUEÑAS Y MEDIANAS EMPRESAS

Todas las organizaciones pueden ser blanco de un ataque de ransomware que toma como rehenes las computadoras o archivos de los usuarios u obstaculiza el acceso al sistema hasta que se cumplan las exigencias del rescate. Y aunque el **Big Game Hunting** está en aumento - con operadores de ransomware atacando grandes organizaciones empresariales para obtener grandes pagos-, el ransomware suele dirigirse a organizaciones pequeñas y medianas, incluidos los gobiernos estatales y locales, los cuales suelen ser más vulnerables a los ataques. Las organizaciones de todas las formas y tamaños deben mantenerse alerta y al tanto de su seguridad. Este documento explica el impacto que tiene el ransomware en las organizaciones pequeñas y medianas, explora los factores que conducen a una mayor vulnerabilidad y ofrece asesoría sobre cómo proteger su organización.

ATAQUES DE RANSOMWARE: EL TAMAÑO NO GARANTIZA LA SEGURIDAD

Las pequeñas y medianas empresas (PYMEs) impulsan la economía, contribuyendo al crecimiento y la innovación. No obstante, a menudo éstas permanecen rezagadas en comparación con las grandes empresas en lo que concierne la ciberseguridad, haciéndolas vulnerables a ataques maliciosos. Un retraso en la ciberseguridad no les preocupaba a las PYMEs en el pasado, pues muchas creían que sus organizaciones estaban fuera del radar de ataques y ransomware. Si bien esta actitud continúa existiendo en algunas empresas, estudios recientes sugieren que los tiempos están cambiando.

Un estudio realizado por **Paychex** en el 2017 informó que el 68% de los propietarios de PYMEs no estaban preocupados por ser hackeados. Esta forma de pensar fue confirmada por un **estudio** más reciente del 2019, donde el 66% de los tomadores de decisiones de las PYMEs no creía ser un posible blanco de ataque. Pero otro **estudio** del 2019 mostró que la sensibilización y preocupación pueden estar cambiando. Un informe publicado a finales del 2019 por la Alianza Nacional para la Ciberseguridad (NCSA, por sus siglas en inglés) señaló que el 88% de las organizaciones de menor tamaño encuestadas creían ser al menos un objetivo “algo probable” para los cibercriminales, siendo que casi la mitad (46%) afirmó ser un objetivo "muy probable".

Si bien la percepción del riesgo puede variar, tal como sugerido por diferentes estudios, hay una buena razón para esta creciente preocupación: en su **Informe de Investigaciones sobre Brechas de Datos del 2019**, Verizon señaló que el 43% de las brechas tuvieron como víctimas a pequeñas empresas. Y, desafortunadamente, solo el **30%** de las pequeñas empresas cree que su postura de seguridad de TI es lo suficientemente fuerte frente a las amenazas.

Verizon reportó en su Informe de Investigaciones sobre Brechas de Datos del 2019 que el 43% de las brechas tuvieron como víctimas a pequeñas empresas. Y, desafortunadamente, solo el 30% de las pequeñas empresas cree que su postura de seguridad de TI es lo suficientemente fuerte frente a las amenazas.

LAS PYMEs TIENEN LO QUE LOS ADVERSARIOS QUIEREN

Las pequeñas empresas son objeto de ataques por una serie de razones, desde el dinero y la propiedad intelectual (PI) hasta por el acceso a los clientes y sus datos.

De hecho, el acceso puede ser el principal impulsor de un ataque porque una PYME puede ser utilizada como vector para atacar a una empresa matriz más grande o a la cadena de suministro de un objetivo mayor. Los propietarios de pequeñas empresas pueden no darse cuenta de su valor para los atacantes. Muchas noticias relativas al ransomware destacan los ataques a organizaciones más grandes con más frecuencia que los dirigidos a las más pequeñas, perpetuando una falsa sensación de seguridad de que los ataques ransomware están relacionados con el tamaño y la rentabilidad.

REALIDADES RANSOMWARE PARA PEQUEÑAS Y MEDIANAS EMPRESAS

Los ciberdelincuentes tienen mucho que ganar al atacar a las PYMES y, desafortunadamente, las PYMEs tienen mucho más que perder. Según **KnowBe4**, el rescate promedio solicitado a las PYMEs es de aproximadamente $ 4,300 dólares. Aunque esta cantidad puede parecer insignificante, el mismo informe señaló que el costo promedio del tiempo de inactividad relacionado con un incidente de ransomware es mucho mayor, siendo de aproximadamente $ 46,800 dólares.

Algunos ataques de ransomware encriptan archivos en los computadores y discos duros, bloqueando el acceso de los usuarios a sus dispositivos y datos. Otras variantes de ransomware pueden acceder a los datos del usuario y ponerlos a disposición o venderlos a terceros, conllevando brechas de datos y mayores pérdidas.

Aunque las organizaciones más grandes - como **FedEx**, que fue atacado por el ransomware NotPetya con pérdidas estimadas en $ 300 millones - están mejor equipadas para absorber grandes perjuicios y continuar prosperando, esta no es la realidad de muchas pequeñas empresas. Las organizaciones más pequeñas pueden perder algo más que dinero en un ataque de ransomware - el ataque puede dañar su reputación y disminuir sus posibilidades de supervivencia. Investigaciones indican que el **60%** de las PYMEs en Estados Unidos que sufren un ciberataque acaban cerrando en los seis meses siguientes.

Debido a su menor tamaño y recursos limitados, las PYMEs tienen más dificultades para absorber el costo adicional de un ataque de ransomware y de la tensión en las relaciones con los clientes. Y la percepción de que no son un blanco posible implica que las empresas más pequeñas a menudo no cuentan con el personal o el presupuesto de ciberseguridad para protegerse, lo que empeora la situación. El estudio del **Instituto Ponemon** señaló que el 77% de las pequeñas empresas afirmó no tener el personal necesario para mitigar las brechas y riesgos cibernéticos, el 55% no contaba con suficiente presupuesto y el 45% no sabía cómo protegerse contra los ataques.

La idea de que un ataque ransomware acabe con un negocio puede parecer poco realista, pero, desafortunadamente, es un riesgo real.

VULNERABILIDADES COMUNES

El éxito de los ataques de ransomware contra las pequeñas empresas puede atribuirse a los desafíos específicos asociados con el menor tamaño, así como también a los retos generales que enfrentan las organizaciones de cualquier talla: el elemento humano.

Aunque un computador de trabajo es algo usual, e inclusive esperado, en grandes organizaciones, las empresas pequeñas no siempre cuentan con éstos y, en cambio, dependen de que los empleados utilicen sus propios dispositivos. Estos dispositivos se utilizan tanto para fines relacionados con el trabajo, incluido el acceso y el almacenamiento de documentos e información confidencial, como para actividades personales como la búsqueda y navegación. Estos dispositivos de doble propósito contienen grandes volúmenes de información comercial y personal, incluyendo información de tarjetas de crédito, cuentas de correo electrónico, plataformas de redes sociales, fotos y contenido personal. La encuesta de AppRiver 2019 descubrió que el 48% de las PYMEs no almacena sus datos más importantes y confidenciales exclusivamente en una red segura, sino que los dispersa en múltiples ubicaciones inseguras o no sabe dónde están almacenados. Los puntos ciegos de acceso y almacenamiento de datos, unidos a una cobertura de seguridad inconstante o inadecuada, rápidamente acarrean vacíos en la protección cibernética, aumentando el riesgo.

TERROR EN LA SALUD

En abril de 2019, Brookside ENT and Hearing Services, un pequeño consultorio médico dirigido por dos médicos en Michigan, fue víctima de un **ataque de ransomware** que eliminó y sobrescribió cada cita médica, factura e historia clínica de los pacientes. Éste también borró las copias de seguridad y dejó un duplicado de los archivos eliminados, los cuales podían ser desbloqueados si se pagaba un rescate de $6,500 dólares. Los médicos se negaron a pagar el rescate y continuaron yendo al consultorio para atender los pacientes. Debido a que los archivos e historias médicas fueron eliminados, los doctores no tenían cómo contactar a los pacientes para cancelar o reprogramar las citas. Después de unas semanas agotadoras, el consultorio se vio obligado a cerrar y los médicos debieron conformarse con una jubilación anticipada.

Este fue el primer caso en el que un consultorio médico tuvo que cerrar debido a un ataque de ransomware. En este caso, como en muchos otros, tener copias de seguridad no fue suficiente para protegerse contra un ataque de ransomware. El pequeño consultorio se vio obligado a cerrar porque no tenía la capacidad para soportar las cargas en tiempo y en dinero necesarias para la remediación.

EL FACTOR HUMANO

Para las organizaciones de cualquier tamaño, el comportamiento de los empleados — desde compartir demasiadas cosas en las redes sociales hasta hacer clic en cualquier enlace que aparezca — es una preocupación y es un factor de riesgo determinante para las organizaciones más pequeñas. De hecho, el **77%** de las PYMEs percibe el uso de las redes sociales como un riesgo de ciberseguridad, destacando el Facebook como una preocupación principal en lo que respecta los empleados. Las plataformas de redes sociales son hubs para cuentas de spam. Aunque muchas pueden ser inofensivas, ciertas cuentas contienen pop-ups y enlaces web bien encubiertos que conducen a ransomware. Los empleados también pueden compartir demasiadas cosas en Facebook y atraer a posibles estafadores que pueden llevar a cabo investigaciones sobre el negocio y lanzar intentos de ingeniería social. La ingeniería social puede asumir varias formas, desde simples cuentas falsas que recopilan información, hasta ataques completos de spear phishing que se hacen pasar por un jefe o colega del funcionario. El spear-phishing a través de correos electrónicos comprometidos es el principal punto de entrada para muchos ataques de ransomware. Las víctimas a menudo caen en la trampa de estos correos electrónicos y hacen clic en los links que se encuentran allí dentro, pues el remitente parece ser una entidad conocida de una fuente de confianza, como un colega o gerente.

KnowBe4 publicó los resultados de sus servicios de prueba de correo electrónico de phishing y reveló que, del total de usuarios que hizo clic en los e-mails de prueba de phishing, el 56% tenía que ver con mensajes de LinkedIn. Por lo general, los usuarios confían en las plataformas de redes sociales, como LinkedIn y Facebook, convirtiendo estos canales en principales fuentes para recopilar información y fomentar campañas de phishing. LinkedIn e Facebook, geralmente têm a confiança de seus usuários, o que torna esses canais as principais fontes para coletar informações e alimentar campanhas de phishing.

De hecho, al 77% de las PYMEs les preocupa el uso de las redes sociales como un riesgo de ciberseguridad, señalando a Facebook como una de las principales preocupaciones en lo que concierne los empleados. Las plataformas de redes sociales son hubs para cuentas de spam. Aunque muchas pueden ser inofensivas, ciertas cuentas contienen pop-ups y enlaces web bien encubiertos que conducen a ransomware.

CÓMO PROTEGERSE DEL RANSOMWARE

En septiembre de 2019, el **Departamento de Seguridad Nacional de EE. UU.** publicó un artículo que describe las medidas adicionales que las organizaciones deben tomar para enfrentar las amenazas del ransomware. El artículo ofrece consejos sobre cómo protegerse contra el ransomware, prepararse para un posible incidente y recuperarse de un ataque, así como dónde encontrar ayuda. Éste incluye recomendaciones prácticas que van desde mantener los sistemas parcheados y actualizados, hasta capacitar a los usuarios finales y crear y ejecutar un plan de respuesta a incidentes.

Recuerde, las copias de seguridad son una buena defensa, pero también deben protegerse, pues a menudo son lo primero que los atacantes bloquean o intentan destruir en un entorno. Asegurarse de que las copias de seguridad estén seguras y se pueda acceder a ellas por separado, incluso en un entorno comprometido, es una medida de precaución estándar que permite, también, una remediación más rápida en el caso de que ocurra un ataque de ransomware.

Implementar capacitaciones adecuadas para los empleados también es una práctica esencial para ayudar a mantener su marca y su negocio seguros. Mantener a los empleados actualizados en prácticas de sensibilización es fundamental para reducir las tentativas de acceso de phishing. Esto incluye no hacer clic en enlaces o descargar archivos adjuntos de correos electrónicos sospechosos y verificar las direcciones de correo electrónico de los remitentes.

Adoptar una solución eficaz de protección de endpoints es otro método clave para defender a su organización. Afortunadamente, CrowdStrike ofrece una protección para endpoints de última generación, ayudándoles a las PYMEs a prosperar.

SOLUCIONES DE CROWDSTRIKE PARA PEQUEÑAS Y MEDIANAS ORGANIZACIONES

Los expertos en seguridad de CrowdStrike® entienden que las organizaciones más pequeñas enfrentan diferentes desafíos que las más grandes, y también saben que las organizaciones más pequeñas a menudo enfrentan las mismas amenazas y necesitan el mismo nivel de protección.

La plataforma de última generación de CrowdStrike Falcon® de protección de endpoints utiliza una variedad de métodos complementarios de prevención y detección para luchar contra las técnicas de ransomware que cambian constantemente. La plataforma Falcon incluye lo siguiente:

- **Machine learning** para la prevención de ransomware conocido y previamente desconocido o de "día cero", sin necesidad de actualizaciones
- **Bloqueo de exploits** para detener la ejecución y propagación de ransomware a través de vulnerabilidades sin parchear.
- **Indicadores de ataque (IOAs)** para identificar y bloquear comportamientos adicionales de ransomware y proteger contra las nuevas categorías de ransomware sin archivos
- **Análisis de amenazas automatizado** para obtener, de manera inmediata, todos los detalles sobre el ransomware encontrado, incluyendo su origen, atribución, familias similares e IOCs (indicadores de compromiso)

CrowdStrike ofrece varios paquetes de protección de endpoints para proveerle la solución más adecuada a sus necesidades en seguridad. Estas soluciones incluyen desde el Falcon Pro, con un antivirus de última generación, hasta el Falcon Complete ™, donde todas sus necesidades de seguridad de endpoints son manejadas por el equipo de especialistas de CrowdStrike.

Como los titulares de noticias continúan recordándonoslo, el ransomware sigue siendo una amenaza significativa. CrowdStrike está comprometido en defender contra el ransomware, evolucionando e innovando su tecnología de seguridad para mantenerse un paso adelante de los adversarios más determinados. Se requiere una combinación de elementos para proteger adecuadamente a su organización. Esto incluye tomar medidas prácticas para que su organización esté alineada con sólidas prácticas de seguridad, así como también implementar la innovadora tecnología de prevención y detección nativa de la nube provista por la plataforma de CrowdStrike Falcon.

Más información en **www.crowdstrike.com**

© 2020 CrowdStrike, Inc. Todos los derechos reservados.

SOBRE CROWDSTRIKE

CrowdStrike® Inc (Nasdaq: CRWD)., un líder mundial en ciberseguridad, está redefiniendo la seguridad en la era de la nube con una plataforma de protección de endpoints construida desde cero para detener las brechas. La arquitectura de un agente único y liviano de la plataforma CrowdStrike Falcon® aprovecha la inteligencia artificial (IA) a escala de nube y ofrece protección y visibilidad en tiempo real en toda la empresa, previniendo ataques en endpoints, dentro o fuera de la red. Con la tecnología patentada de la CrowdStrike Threat Graph®, CrowdStrike Falcon correlaciona más de dos billones de eventos por semana, y en tiempo real, relativos a endpoints de todo el mundo, alimentando una de las plataformas de datos más avanzadas del mundo en seguridad.

Con CrowdStrike, los clientes se benefician de una mayor protección, un mejor rendimiento y un valor-tiempo inmediato ofrecidos por la plataforma Falcon en la nube.

Solo hay una cosa que recordar sobre CrowdStrike: detenemos las brechas.

Hable con un representante para obtener más información sobre cómo CrowdStrike puede ayudarle a proteger su entorno:

Email: latam@crowdstrike.com
Web: www.crowdstrike.com