ZEBRA

Plataforma de seguridad de Zebra

Proteja su ventaja de rendimiento

La omnipresente conectividad que agiliza su negocio también puede exponerlo a potenciales riesgos de seguridad. Si bien la primera medida consiste en establecer *firewalls*, estos no son de ningún modo la panacea ante las sofisticadas amenazas que surgen continuamente. Descubra las prácticas idóneas y las soluciones empresariales que pueden mejorar la defensa de su organización y sus datos.

Cómo detener las amenazas a la seguridad antes de que estas detengan su negocio

La seguridad es imprescindible

Números de tarjetas de crédito. Historias médicas. Números de la Seguridad Social. Contraseñas. Si su actividad implica atender a clientes, pacientes o ciudadanos, se espera de usted —y muchas veces se le exige— que mantenga la privacidad de los datos personales.

El riesgo aumentará

Esto le resultará cada vez más difícil. Es cierto que Internet de las Cosas y la tecnología de nube permiten conectar a las personas y la información como nunca, lo que brinda a su organización un control y una visibilidad operativa sin precedentes. Aunque el futuro es prometedor, entraña diversos riesgos.

Los 50.000 millones[1] de dispositivos interconectados que se espera que existan en 2022 podrían abrir sus organizaciones y datos confidenciales a innumerables puntos de vulnerabilidad. Dados los elevados beneficios y la baja probabilidad de repercusiones (solo un cinco por ciento de los *hackers* ha sido procesado[2]), no parece que la ciberdelincuencia vaya a reducirse.

¿Qué hay en juego?

Una sola infracción de seguridad puede salir muy cara, con costes de productividad y pérdidas financieras muy elevados, además de poner en entredicho su reputación.

¿Qué puede hacer usted? Tomarse en serio la seguridad. Aunque su organización disponga de un programa de seguridad, lo más probable es que las percepciones poco realistas estén minando su integridad y provocando vulnerabilidades innecesarias.

3,9 millones de $:
coste medio de una infracción de seguridad de datos[3]

25.575 registros:
tamaño medio de una infracción de seguridad de datos[3]

12 horas:
tiempo medio que tarda el 88 % de los *hackers* en superar las defensas de ciberseguridad[4]

197 días:
tiempo medio que tarda una organización en darse cuenta de que se ha producido una infracción de seguridad.[3]

Objetivos:

***Retail*:**
el 80 % del tráfico de inicios de sesión que registran los comercios *online* se atribuye a *hackers* que utilizan datos robados[5]

Administración del Estado/Sector público:
es el principal objetivo de los *hackers*, cuyos ataques están motivados por el espionaje y la ganancia financiera[6]

Atención sanitaria:
segundo sector que más ciberataques recibe —un 15 % del total[6]

Manufactura:
ha sufrido más ataques relacionados con el espionaje que otros mercados verticales en los últimos años[6]

No permita que las percepciones falsas debiliten su seguridad

A pesar de la amplia cobertura que han recibido numerosos incidentes, muchas organizaciones siguen mostrándose complacientes en lo que a seguridad se refiere. No se deje llevar por una falsa sensación de seguridad. Si se sorprende a sí mismo diciendo cosas como estas, podría tener problemas.

«Mi organización no es lo suficientemente grande para ser el objetivo de un ataque.»

El 43 % de los ciberataques van dirigidos a pequeñas empresas.[6] Los *hackers* explotan la falta de recursos y conocimientos de las empresas pequeñas. Puede que incluso utilicen su organización para acceder a sus conexiones con entidades mayores.

«Estamos protegidos por nuestra red.»

Una iniciativa de seguridad seria debe contar con múltiples capas y evolucionar constantemente. Cerrar la puerta de casa con llave no impedirá que los ladrones entren por la ventana si la deja abierta. De hecho, un estudio revela que las medidas correctoras tradicionales, como los *firewalls* y antivirus, casi nunca ralentizan la actividad de los *hackers*, sino que son las tecnologías de seguridad de extremos las que resultan más eficaces para detener los ataques.[4]

«No hemos sufrido ninguna infracción de seguridad, por lo que nuestra seguridad funciona bien.»

Es posible que se haya producido una infracción de seguridad y que usted no lo sepa. El estudio indica que una empresa puede tardar hasta 197 días en detectarla.[3]

«Ya contamos con un programa de seguridad formal.»

Estupendo. ¿Evoluciona constantemente para hacer frente a las nuevas amenazas que surgen continuamente? ¿Cubre toda su tecnología? Adoptar una solución y olvidarse para siempre no sirve para combatir a los sofisticados ciberdelincuentes de hoy en día.

«La seguridad es demasiado complicada.»

Una seguridad bien diseñada resulta intuitiva y fácil de implementar. Puede tener la certeza de que sus trabajadores tendrán una experiencia armonizada de su funcionamiento y que su gestión resultará sencilla para su departamento de sistemas informáticos.

«La seguridad afecta negativamente a la productividad.»

Las quejas de que los sistemas de seguridad son demasiado complicados, demasiado difíciles de integrar o que detienen las operaciones son, por desgracia, bastante habituales. Sin embargo, una infracción de seguridad puede parar por completo su actividad. La solución consiste en elegir una tecnología en cuyo diseño esté integrada la seguridad. De este modo, la seguridad propicia la productividad en lugar de dificultarla.

Proteja su organización con múltiples capas de defensa

No todas las medidas de seguridad están a la altura de sus necesidades. Al elegir una tecnología, tenga en cuenta estos atributos críticos de seguridad intrínsecos a Zebra Technologies e imprescindibles para lograr la tranquilidad.

Protección y rendimiento integrados:
Elija la marca que integra seguridad y productividad en una misma tecnología desde el principio. Comprobará que nuestras soluciones se han diseñado intencionadamente para aumentar su rendimiento, al tiempo que incorporan de forma armonizada una serie de protocolos y funciones de seguridad muy efectivas.

Prestaciones de seguridad automatizadas:
La certificación de Wi-Fi®, una tarea en la que su departamento de sistemas informáticos solía invertir semanas, ahora puede hacerse de forma automática, lo que permite acelerar la creación de un entorno conectado seguro para usted y su equipo.

Adaptable a sus necesidades:
¿Prefiere establecer su propia tolerancia de seguridad? Zebra se lo facilita con soluciones configurables que ajustan los niveles de seguridad a las necesidades de su empresa o departamento.

Mantenimiento y servicio más simples:
Puede tener la seguridad de que nuestras funciones de seguridad, así como nuestro software y hardware, han sido desarrollados y comprobados para que funcionen con un mantenimiento mínimo y una disponibilidad máxima. Además, nuestro equipo de servicio está a su disposición las 24 horas.

Integración sin esfuerzo:
Zebra le ofrece una integración sencilla y rápida. Gracias a nuestro profundo conocimiento de su sector y sus aplicaciones, nuestras soluciones están diseñadas para anticiparse y atender sus necesidades de integración.

Vigilancia y asistencia continuas:
Combinamos años de actualizaciones de seguridad del sistema operativo y mejoras del *firmware* con solución de problemas, evaluaciones de vulnerabilidad y colaboración de seguridad interna.

Sigue prácticas idóneas reconocidas globalmente:
Puede tener la tranquilidad de que Zebra adopta un conjunto de prácticas idóneas y directrices establecidas por los expertos en seguridad de todo el mundo, incluidos ISO, NIST (National Institute of Standards and Technology) y los controles de referencia del Center for Internet Security. Nuestros productos y soluciones se utilizan en aplicaciones que ayudan a las organizaciones a cumplir la normativa HIPAA, PCI-DSS y el RGPD.

Líder en tecnología empresarial segura:
Trabaje con la empresa que fortaleció el sistema operativo Google Android™ para uso empresarial y que ofrece hasta diez años de asistencia de seguridad para el sistema operativo. Ya sean nuestros ordenadores móviles fortalecidos para uso empresarial, nuestras impresoras seguras o nuestra tecnología visionaria, observará que la productividad y la seguridad están en el propio núcleo de todo lo que hacemos.

Productos, soluciones y servicios Zebra Asistencia para todo el marco de ciberseguridad (Cybersecurity Framework) de NIST

IDENTIFICAR	Supervisión de la gestión de riesgos Printer Security Assessment Wizard Servicios profesionales	Gestión de riesgos de la cadena de suministro Comité de seguridad
PROTEGER	LifeGuard™ for Android Modo protegido de impresora Control de dispositivos	Actualizaciones de PrintSecure Gestión automática de certificados de Wi-Fi Marco de gestión de riesgos
DETECTAR	Printer Profile Manager Enterprise Supervisión de la seguridad	Detección en tiempo real
RESPONDER	Gestión de dispositivos Detección de amenazas y medidas para contrarrestarlas	Respuesta a incidentes Alertas a clientes
RECUPERAR	Servicios profesionales Mejoras	Restauración de un estado conocido

Protección de su ventaja de rendimiento

La seguridad es crucial para su empresa y sus flujos de trabajo. Por eso Zebra protege proactivamente contra las vulnerabilidades de seguridad integrando en sus soluciones varias capas de protección. En el diseño de los dispositivos, la tecnología y los servicios Zebra se ha tenido en cuenta la seguridad sin que esta impida la productividad. Comprobará que nuestra seguridad es fácil de implementar y que sus trabajadores de primera línea la perciben con un funcionamiento armonizado. Gracias a nuestra tecnología inteligente y configurable, puede equilibrar los objetivos operativos con la seguridad en tiempo real en el mundo real. Puede tener la seguridad de que Zebra le proporcionará la tranquilidad que necesita para implementar sus estrategias empresariales y tecnológicas de primera linea.

ZEBRA

Conozca cómo nuestros estándares de seguridad mejoran los suyos

Visite www.zebra.com/product-security

Fuentes:

1. Juniper Research, 2018 **2.** Carbon Black Incident Response Threat Report, Nov. 2018 **3.** Ponemon Institute, 2018 / 2019 Cost of Data Breach **4.** Black Report, Nuix 2017 **5.** Shape Credential Spill Report 2018 **6.** Verizon 2019 Data Breach Investigations Report