Si tiene una empresa, la seguridad es un aspecto central a su negocio

Por qué la seguridad es fundamental para la productividad

A medida que el mundo se vuelve cada vez más interconectado, la red y los datos confidenciales de su organización se vuelven más vulnerables al acceso ilegal. Las violaciones de datos pueden ser devastadoras. Todo ataque exitoso es una fuente potencial de pérdidas financieras, infracciones legales o normativas y daños a la reputación de su empresa.

Sin embargo, a pesar del aumento que ha habido en los ciberataques, muchas organizaciones se escudan detrás de una capa de protección delgada y estática. Si su cultura de seguridad es como la de muchos, podría estar guiándose por percepciones peligrosas y medidas de seguridad inadecuadas que exponen sus operaciones a riesgos.

Descubra mejores prácticas que son esenciales para proteger su tecnología y mantener un óptimo nivel de productividad.

Las amenazas de seguridad son reales y constantes

Debe proteger el pilar de los negocios

Desde las transacciones financieras y las credenciales hasta la documentación y los registros, son incontables las tareas empresariales diarias que dependen de la confidencialidad, la integridad y la disponibilidad de su tecnología y sus datos. Ya sea que deba satisfacer a consumidores, pacientes o ciudadanos, se espera —y muchas veces se exige— que usted proteja la información confidencial y las soluciones que la almacenan.

El impacto de las violaciones es destructivo

Cuando sus datos y su tecnología se ven amenazados o comprometidos, la productividad cae en picada, la confianza de los clientes disminuye y los gastos se disparan. En 2018, el costo promedio global de un evento único de violación de datos alcanzó los US$ 3,86 millones. Es probable que, ante consecuencias tan graves, su organización haya implementado protocolos de seguridad. Pero a menos que esas iniciativas evolucionen e incluyan múltiples capas de defensa, puede ser que no sean suficientes para mitigar los ataques, especialmente a medida que continúan creciendo.

El delito cibernético crece en tamaño y en fuerza

Hasta la fecha, solo el 5% de los hackers ha sido sometido a juicio.[3] Esta falta de consecuencias por sus acciones combinada con las jugosas ganancias de esta actividad actúan como un incentivo para los criminales que buscan constantemente puntos débiles en su defensa. A medida que la tecnología avanza, sus amenazas no solo se vuelven más sofisticadas, sino también más difíciles de detectar. Tomemos, por ejemplo, la inteligencia artificial. Las pruebas de ZeroFOX han demostrado que los hackers artificiales son considerablemente más hábiles para componer y distribuir mensajes de suplantación de identidad que sus contrapartes humanas. A eso se le agrega el auge del Internet de las cosas (IoT), que se prevé que llegue a 50 mil millones de dispositivos para 2022.[4] Para los hackers, la proliferación de estos dispositivos inteligentes conectados representa un punto de ingreso expansivo a su red y a las redes de otros.

Los conceptos erróneos pueden generar problemas de seguridad

Aunque los ciberataques están en el centro de la atención pública, muchas organizaciones funcionan con una falsa sensación de seguridad, dejándose llevar por percepciones equivocadas y medidas inadecuadas. Este artículo se propone descubrir esos puntos débiles y ofrecerle estrategias para reforzar su seguridad, sin perjudicar su productividad.

US$ 3,86 millones
fue el costo promedio global de una violación de datos en 2018.[1]

88% de los hackers
puede derribar las barreras de ciberseguridad en 12 horas.[2]

41% de las empresas de seguridad
halló que sus protecciones de red habían sido burladas.[3]

54% de las empresas
respondió a incidentes que involucraron dispositivos para consumidores.[3]

38% de las empresas
denunció ataques que involucraron dispositivos empresariales.[3]

Los supuestos predominantes debilitan las medidas de protección

¿Alguna vez oyó estos mitos en su empresa?

Nuestras actitudes influyen en las medidas y prácticas de ciberseguridad que aplicamos. Algunos empleados sienten que el tamaño de su empresa es barrera suficiente para los hackers, mientras que otros consideran que el firewall de su red es un escudo aceptable. Asimismo, están los que toman el camino más corto porque consideran que la seguridad es una molestia que perjudica la productividad. Sea cual sea su opinión, algo es seguro: los cibercriminales buscan constantemente formas de sortear sus sistemas de seguridad. Si no cuenta con medidas y prácticas de seguridad sólidas, exhaustivas y en constante evolución, su tecnología y sus datos no están bien protegidos. Es importante poner a prueba esos conceptos equivocados con la realidad para reforzar posibles debilidades en la seguridad de su organización.

Mito: **Mi organización no es tan grande como para ser un objetivo.**

Realidad: **Las pequeñas empresas sufren el 58% de los ataques de malware.[6]**

Si tiene una pequeña o mediana empresa, esté atento. Los cibercriminales explotan su falta de recursos e incluso pueden utilizar su organización como puerta de acceso a entidades más grandes

---

Mito: **Nuestra red nos protege.**

Realidad: **Las contramedidas tradicionales, como firewalls y programas antivirus, casi nunca detienen a los hackers, pero las tecnologías de seguridad para dispositivos finales han sido más efectivas a la hora de combatir los ciberataques.[2]**

¿Qué tan seguro estaría su hogar si cerrara con llave la puerta principal, pero dejara abiertas las ventanas o el portón del jardín? Un plan de seguridad sólido es multicapay continuo.

Mito: **No hemos sufrido violaciones, así que nuestro sistema de seguridad funciona bien.**

Realidad: **Ya puede haberse producido una violación.**

Algunas investigaciones han hallado que una empresa puede tardar hasta 197 días en detectar una brecha de seguridad.[1]

Mito: **Contamos con un programa de seguridad formal.**

Realidad: **Una solución inicial y aislada no es suficiente para defenderlo contra amenazas emergentes y cambiantes.**

Pregúntese si su programa actualmente cubre toda su tecnología conectada a sus redes y datos, incluso sus soluciones, sensores, sistemas y dispositivos empresariales. Con demasiada frecuencia, esas capas se pasan por alto. Analice qué tan proactiva es su organización a la hora de actualizar y desarrollar su programa de seguridad. Debe ser tan incansable como sus enemigos.

Mito: **La seguridad es demasiado complicada.**

Realidad: **Un sistema de seguridad bien diseñado es intuitivo y fácil de implementar.**

Busque dispositivos y soluciones empresariales con múltiples capas de seguridad, que cuenten con el respaldo de actualizaciones proactivas y que cumplan con rigurosos estándares de seguridad. Estos ofrecen un muro metafórico que protege a su empresa. Sus controles centralizados y automatizados simplifican las tareas de TI, mientras su seguridad inherente trabaja detrás de escena para los usuarios finales.

Mito: **La seguridad perjudica la productividad.**

Realidad: Una encuesta realizada por el Instituto Ponemon reveló exactamente cuánto puede sufrir la productividad en manos de los hackers: [7]

El **30%** de las empresas encuestadas perdió productividad a nivel de TI y de usuarios finales[7]

El **25%** sufrió tiempo de inactividad del sistema[7]

El **23%** sufrió robos de recursos informativos[7]

Refuerce la seguridad con mejores prácticas sensatas

¿Qué puede hacer para proteger mejor su tecnología y sus datos? Implemente un conjunto de mejores prácticas para defender sus dispositivos y soluciones empresariales. Los dispositivos móviles son inherentemente vulnerables cuando se utilizan por fuera de sus firewalls, de sus mecanismos de gestión de amenazas, de los filtros de contenido y correo basura, y de otras herramientas destinadas a mantener a raya las interacciones malintencionadas. Entonces, es esencial que minimice su exposición al riesgo a través de estos métodos efectivos.

Por último, no desestime la importancia de su personal. Puede ser su punto más débil o más fuerte, dependiendo de su voluntad para seguir las instrucciones. Genere conciencia, aliente la participación comunicando la importancia de la seguridad y fortalezca su programa premiando a quienes lo adoptan y haciendo respetar las políticas.

1. Inicie un plan con mucha anticipación:

La tecnología moderna ofrece emocionantes posibilidades, así como también riesgos de seguridad. Tómese el tiempo para definir los protocolos de seguridad mucho antes de implementar sus soluciones y dispositivos nuevos.

2. Proteja los datos:

Utilice conexiones encriptadas y autenticadas donde sea posible y encripte los datos almacenados en sus dispositivos. Si bien es habitual implementar contraseñas y mecanismos de encriptación en sus dispositivos con conexión inalámbrica, su tecnología cableada o conectada mediante Ethernet también puede necesitarlo (según la información que maneje). Recuerde que debe tener cuidado con todo lo que esté conectado a su red.

3. Controle los servicios:

Muchos dispositivos ofrecen múltiples métodos de comunicación. Por ejemplo, los servicios de red pueden incluir FTP, SNMP y SMTP. Si bien estos servicios hacen que sea más fácil acceder a los dispositivos y administrarlos, considere apagarlos cuando no estén en uso.

4. Cambie las contraseñas:

Las contraseñas predeterminadas representan métodos documentados de acceso a un dispositivo. Active las contraseñas de interfaz de usuario. Deben ser sólidas y únicas: en otras palabras, fáciles de recordar, pero difíciles de adivinar. Prohíba que el personal comparta credenciales y exija una política de cambio regular de contraseñas. Es importante que rote sus contraseñas, claves de acceso y credenciales de autenticación.

5. Utilice un sistema de administración remota:

Esto le permitirá actualizar rápidamente la configuración. Los dispositivos, soluciones y sistemas se vuelven blancos cada vez más fáciles cuanto más tiempo pasan con configuraciones obsoletas. Los sistemas de administración remota también mejoran la productividad de las tareas de TI, pero su acceso y sus permisos deben controlarse cuidadosamente.

6. No anuncie las actualizaciones:

Asegúrese de que los cronogramas y planes de actualización solo lleguen a manos de quienes los necesitan. Saber cuándo se planifican las actualizaciones puede alentar involuntariamente conductas indebidas.

7. Monitoree la tecnología fuera de contacto:

Planifique un método para monitorear de forma continua su sistema y detectar dispositivos “fuera de contacto”. Cuando sospeche que se ha retirado un dispositivo, retenga sus credenciales hasta que pueda confirmar su ubicación.

8. Elija dispositivos que puedan actualizarse y planifique actualizaciones periódicas:

Invierta en dispositivos que puedan actualizarse constantemente a lo largo de su ciclo de vida para asegurarse de mantenerlos al día con los nuevos estándares. También es importante que sus sistemas de actualización cuenten con los medios para verificar que los archivos de actualización no hayan sido manipulados.

9. Dé seguimiento a su tecnología:

Implemente un plan de retiro para sus dispositivos y soluciones. De este modo, podrá asegurarse de eliminar las configuraciones del sistema empresarial, borrar cuentas de usuario y credenciales de los dispositivos y comprobar que los sistemas existentes no estén codificados de forma rígida para buscar unidades retiradas.

10. Considere aplicar el modelo CIA:

Durante todas las etapas del ciclo de vida de un dispositivo o solución, se recomienda aplicar el modelo de confidencialidad, integridad y disponibilidad, también conocido como el modelo “CIA” (por sus siglas en inglés).

a. **Confidencialidad:**
Asegúrese de que solo el personal autorizado obtenga acceso a su tecnología e información.

b. **Integridad:**
Mantenga la uniformidad, la precisión y la fiabilidad de los datos a lo largo de todo su ciclo de vida.

c. **Disponibilidad:**
Finalmente, asegúrese de que el dispositivo y los datos estén disponibles cuando el usuario los necesita.

La introducción de nueva tecnología no debería introducir riesgos de seguridad

Usted invierte en tecnología para optimizar la productividad y aumentar la eficiencia. Pero la seguridad de una tecnología debería estar en el mismo nivel de prioridad, ya que es esencial para el bienestar de su organización. Pregúntese si la solución y su desarrollador facilitan o dificultan la aparición de riesgos de seguridad. Utilice estas preguntas como referencia para medir la solidez de su tecnología empresarial.

1 ¿El fabricante cumple con mejores prácticas de seguridad reconocidas globalmente?

No todos los fabricantes lo hacen. Averigüe qué tan estrictos son los estándares de su proveedor de tecnología. Debería ayudarlo a monitorear y responder ante amenazas mediante herramientas, actualización y soporte.

Es importante que pueda poner en práctica cada uno de estos pasos de seguridad, tal como los establece el estándar de una organización de seguridad universalmente aceptada, como el marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología de EE. UU.:

- **Identificación:** evalúe y lleve a cabo un análisis de riesgos exhaustivo para descubrir potenciales preocupaciones.
- **Protección:** establezca mecanismos de protección, políticas y procedimientos; implemente controles de acceso y auditoría adecuados.
- **Detección:** monitoree y audite continuamente su tecnología, las 24 horas, los 7 días de la semana, los 365 días del año.
- **Respuesta:** establezca un sólido plan para analizar, seleccionar y responder ante eventos detectados.
- **Recuperación:** organice un plan de acción de recuperación; implemente mejoras para solucionar las vulnerabilidades sobre la marcha y prevenir ataques futuros.

2 ¿La seguridad se incorpora desde el inicio hasta la finalización?

Contar con seguridad empresarial integrada mitiga los riesgos. Esto se debe a que está diseñada para brindarle el control total centralizado de sus dispositivos y soluciones. Pregunte si puede bloquear la pantalla de inicio, las funciones y las interfaces periféricas de la tecnología, como la tecnología USB, Bluetooth®, GPS y comunicaciones de campo próximo (NFC). Además, busque tecnología que ofrezca encriptación de datos granular y con especificaciones de nivel gubernamental.

3 ¿Verifica la seguridad de su cadena de suministros?

Sin examinar a los proveedores, no es posible comprobar que la tecnología esté diseñada como se había previsto. En un caso, un comprador descubrió un minúsculo microchip no autorizado que podría haber creado una puerta discreta hacia sus redes. Es mejor investigar las prácticas de la cadena de suministros de su proveedor de alta tecnología.

4 ¿Su plataforma de seguridad es lo suficientemente flexible para satisfacer sus necesidades operativas?

Cada empresa es diferente. Lo mismo sucede con las tolerancias de seguridad. Es importante que establezca sus propios niveles y configuraciones de seguridad de acuerdo con las necesidades de sus departamentos y de su empresa en general. Tenga eso en mente cuando busque adquirir nuevas tecnologías. Averigüe hasta qué punto la solución le ofrece flexibilidad y control.

5 ¿Hay actualizaciones constantes y soporte de seguridad disponibles a lo largo de todo el ciclo de vida de la solución?

Sus necesidades de seguridad no desaparecen cuando adquiere tecnología, y tampoco debería desaparecer el soporte de su fabricante. Las amenazas son impredecibles, cambian constantemente. Entonces, ¿cómo puede estar siempre un paso adelante? Elija un proveedor que cubra las actualizaciones de seguridad durante toda la vida útil de su tecnología.

6 ¿Será proactivo al evaluar potenciales vulnerabilidades de seguridad?

Idealmente, debe encontrar un socio de seguridad, y no simplemente un proveedor de tecnología. Un fabricante que se jacte de serlo le informará de amenazas emergentes, le ofrecerá consejo sobre cómo defenderse de ellas, evaluará sus vulnerabilidades y solucionará problemas en los ámbitos específicos de su empresa donde se necesite.

7 ¿Puede garantizar una respuesta rápida y efectiva?

Si se identifica una vulnerabilidad, necesita soporte inmediato y efectivo. Busque un proveedor que cuente con un procedimiento documentado para notificar vulnerabilidades y responder a ellas rápidamente. Debería haber recursos adecuados disponibles para investigar y remediar de inmediato las vulnerabilidades detectadas en el producto.

Zebra protege su ventaja competitiva

Confíe en los productos, servicios y soluciones de Zebra para garantizar su seguridad, sin comprometer su desempeño. Tomamos muy en serio nuestra responsabilidad de cuidar su empresa, porque para protegerla de las vulnerabilidades es necesario un enfoque proactivo y múltiples capas de protección.

Explore Zebra, y podrá ver nuestro compromiso con la seguridad en acción. Nuestro compromiso se puede ver claramente en nuestro equipo de profesionales de seguridad, diseño y desarrollo; en nuestro marco de seguridad; en las prácticas seguras de nuestra cadena de suministros; y en nuestra garantía de actualizaciones preventivas continuas y alertas para clientes.

Nuestra tecnología es fácil de implementar y fácil de usar para sus empleados de primera línea. Nuestra flexibilidad y nuestras funciones pueden configurarse para asegurar tanto la seguridad como la productividad de su empresa. Nuestro compromiso es diseñar dispositivos, soluciones y servicios inteligentes y configurables que le permitan encontrar el equilibrio entre objetivos operativos y de seguridad, en tiempo real, en el mundo real.

Confíe en Zebra para obtener soluciones seguras que no perjudicarán su desempeño, ni la productividad de sus empleados de primera línea. Gane más tranquilidad que lo ayude a implementar sus estrategias tecnológicas y empresariales en sus operaciones en campo.

Fuentes:
1. Informe Cost of Data Breach, 2018, Instituto Ponemon **2.** Black Report, Nuix, 2017 **3.** Informe Incident Response Threat, Carbon Black **4.** Juniper Research, 2018 **5.** Informe Cost of Data Breach, 2019, Instituto Ponemon **6.** Informe Data Breach Investigations, Verizon **7.** Ponemon, State of Endpoint Security Risk, 2018

ZEBRA

Descubra cómo puede sentirse y estar más seguro

Visite www.zebra.com/product-security