Microsoft

Seis pasos para crear una estrategia de seguridad integral

Esta información es para ti

si eres director de seguridad de la información o director de seguridad TI que:

- Necesita una guía rápida y seria sobre la estrategia de seguridad general.
- Quiere estar informado sobre las últimas prácticas de seguridad.

Tiempo estimado de lectura: menos de 9 minutos

Índice

Afrontar el desafío

Una de las principales prioridades para las organizaciones es proteger sus datos y sistemas. Pero como los ataques son cada vez más sofisticados, afrontar este desafío resulta cada día más difícil. Los empleados utilizan un conjunto más amplio de dispositivos y aplicaciones y los datos entran y salen de las empresas de más maneras. Con el cambio masivo al teletrabajo, la seguridad se ve aún más comprometida.

Los responsables deben lograr un equilibrio entre estos desafíos y la necesidad empresarial de colaboración, innovación y crecimiento. Es necesario un enfoque de seguridad polifacético que proteja constantemente todos los puntos de conexión, detecte los signos tempranos de una infracción y responda antes de que se produzcan daños. Y no importa lo sólidas que sean tus defensas; las medidas preventivas ya no son suficientes, también es necesario adoptar una postura que implique "asumir una infracción" y que incluya medidas de detección y respuesta.

Los directores de seguridad de la información (CISO) de hoy en día necesitan marcos de seguridad ágiles que permitan la transformación digital y estén respaldados por estrategias integrales incorporadas en tecnologías, procesos y programas de formación. Si bien todo esto está disponible para las soluciones on-premises, la verdad es que una migración al cloud mejora inmediatamente las capacidades de seguridad en toda la organización.

En este e-book se explican los seis procedimientos recomendados de los CISO que han hecho de la seguridad la piedra angular del éxito empresarial. Estos procedimientos recomendados se aplican a un escenario on-premises, pero son infinitamente más fáciles de lograr en un escenario de cloud.

1. Utilizar productos de seguridad integrados para permitir una respuesta rápida

75

Número de productos de seguridad que utiliza una gran empresa de media.[1]

Los perpetradores de ataques han pasado de usar métodos de "ataques exprés" a poner en peligro sistemas con la esperanza de mantener una presencia persistente de larga duración. Ahora los atacantes emplean diversos vectores de ataque y emplean una cada vez más avanzada variedad de técnicas y herramientas: robo de credenciales, instalación de malware que se borra a sí mismo para evitar su detección, modificación de los procesos internos y reenrutamiento de los datos de red, estafas de ingeniería social y ataques incluso a los teléfonos móviles y dispositivos domésticos de los empleados.

Las organizaciones están implementando cada vez más herramientas de seguridad contra estas amenazas. Si bien están destinadas a abordar problemas específicos, estas soluciones rara vez funcionan juntas. Muchas utilizan paneles, consolas y registros patentados. La dificultad de la integración dificulta tener una visión general y priorizar las amenazas rápidamente. Es un desafío aún mayor cuando se trata de recursos on-premises y en el cloud. Como resultado, los ataques pueden pasar desapercibidos durante más de 140 días.[2]

[1] "Symantec presenta la nueva era de la protección contra amenazas avanzada", Businesswire, octubre de 2015.

[2] "Panorama de amenazas con cifras". Mandiant, A FireEye Company, 2016.

Prueba esto

Como la detección y la respuesta rápidas cada vez resultan más importantes, han surgido estos procedimientos recomendados:

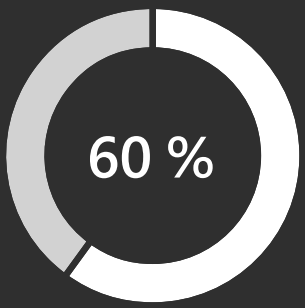
- Obtén una visión integral de la seguridad de toda tu red, incluidos los entornos híbridos y en el cloud.
- Crea un ecosistema de productos y plataformas de seguridad que se integren entre sí y proporcionen conocimientos.
- Asóciate con proveedores de tecnología que colaboren y compartan información en el sector de la seguridad.

Conclusiones principales

La falta de integración entre los productos de seguridad dificulta que los equipos de seguridad puedan ver y combatir las amenazas de forma global y rápida.

Busca productos diseñados para integrarse con otros.

2. Administrar el acceso a través de la identidad, no de los puntos de conexión



de las vulneraciones deriva de un punto de conexión que ha dejado de ser seguro.[3]

Una vulneración de datos puede tener enormes costes. El establecimiento de suficientes controles de seguridad para obtener visibilidad de las amenazas y los ataques es una forma de combatir el alto coste. Pero los equipos de seguridad también tienen que ofrecer soporte a un equipo de TI orientado al consumidor, en el que los empleados ya no trabajan exclusivamente en dispositivos estrictamente controlados y emitidos por la empresa, y esperan trabajar en cualquier lugar, en cualquier dispositivo o plataforma, independientemente de si el equipo de TI corporativo ha autorizado o no su uso.

En este mundo, las estrategias de seguridad basadas en la identidad vinculan el acceso a la identidad, no a los dispositivos. Los controles se aplican basándose en el rol y la necesidad, sin importar cómo se conecte el usuario. Esta atención a la adecuada autenticación y administración de los usuarios según acceden a recursos corporativos permite a las organizaciones proteger sus datos independientemente de dónde se almacenan, cómo se accede a ellos o con quién se comparten.

[3] "Las cinco principales amenazas de seguridad a las que se enfrenta tu empresa y cómo responder ante ellas", blog de Microsoft Secure, octubre de 2016.

Prueba esto

El cambio desde una estrategia de seguridad que solo se basa en los puntos de conexión te da un enfoque más sólido. Estas herramientas pueden ayudarte:

- **Las soluciones de administración de identidades y de acceso (IAM)** y la **administración de aplicaciones móviles con soluciones de prevención de pérdida de datos (DLP)**. Ambas ayudan a reducir el riesgo protegiendo el acceso a aplicaciones y datos en recursos corporativos y en el cloud. La IAM puede eliminar la necesidad de tener varias credenciales al conceder a los empleados una única identidad para acceder a recursos on-premises y en el cloud. Los sistemas de IAM basados en el cloud también pueden usar el análisis y la inteligencia sobre amenazas del proveedor de tecnología para detectar mejor los intentos de acceso anómalos y responder automáticamente de forma adecuada.
- La **autenticación multifactor (MFA)** ofrece otra capa de protección, y exige que un usuario presente algo que conoce (su contraseña) y algo que tiene (autenticación secundaria mediante un dispositivo, huella digital o reconocimiento facial). Entre otras tácticas sólidas se incluye basar el acceso en el riesgo del usuario, el riesgo del dispositivo, el riesgo de la aplicación e incluso el riesgo de ubicación. Estas capacidades pueden permitir, bloquear o requerir automáticamente MFA de un usuario en tiempo real en función de las políticas que establezca, lo que permite esencialmente a las organizaciones aumentar la protección en su propia puerta principal.

Conclusiones principales

Una estrategia de seguridad basada en la identidad cambia el foco de atención de hacer un seguimiento de puntos de conexión (dispositivos) a administrar a los usuarios que acceden a los datos corporativos.

Una protección de puntos de conexión más sólida ofrece conocimientos posteriores a las infracciones sobre las técnicas de los adversarios.

3. Adoptar un modelo de confianza cero para derrotar las amenazas

17 000

alertas de malware

De media, una gran empresa tiene que analizar este volumen a la semana.[4]

Los hackers saben que las organizaciones tienen múltiples puntos de entrada. Utilizan estafas de phishing, ataques de malware y spyware, aprovechan vulnerabilidades de navegadores y software, acceden a través de dispositivos perdidos y robados, emplean ingeniería social y otras tácticas para violar su seguridad. La vigilancia debe ser constante para mantener la visibilidad de las amenazas ya conocidas y ser conscientes de las nuevas vulnerabilidades.

Algunas herramientas pueden ayudar a mantener un enfoque de seguridad siempre alerta, pero tiene más sentido adoptar un enfoque más amplio. Las herramientas tradicionales se centran en la prevención, pero eso ya no es suficiente. Las organizaciones deben asumir o que ya se ha producido una vulneración o que se producirá pronto. Esto se conoce como confianza cero. Después, deben encontrar la manera de reducir considerablemente el tiempo necesario para detectar la vulneración y recuperarse de ella.

[4] "El coste de la contención del malware". Ponemon Institute, enero de 2015.

Prueba esto

Conviértete en experto en seguridad avanzada. Adelantarse a las amenazas puede significar mirar hacia atrás para aprender de los incidentes, las actividades y los pasos anteriores que han dado los hackers.

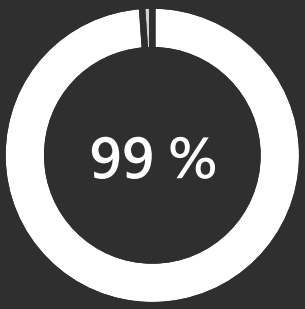
- Muchas aplicaciones de seguridad utilizan capacidades de análisis y de machine learning integradas para analizar cómo ha obtenido acceso un hacker. Las soluciones de análisis y seguridad más avanzadas usarán esos conocimientos para actuar automáticamente con el fin de prevenir infracciones similares y responder ante ellas, lo que contribuye a reducir considerablemente el tiempo necesario para la mitigación.
- Detrás de estas soluciones hay una enorme amplitud y profundidad de señales e inteligencia; cuando se combinan con la experiencia y el conocimiento de expertos humanos, estas soluciones pueden ser herramientas muy poderosas contra los perpetradores de ataques, que son extremadamente rápidos.

Conclusiones principales

Las aplicaciones nativas del cloud admiten un modelo de confianza cero más fácilmente que las aplicaciones heredadas.

Hay que modernizar las aplicaciones heredadas para que admitan el acceso condicional basado en identidad.

4. Migrar al cloud de forma segura



de errores de seguridad en el cloud será culpa del cliente hasta 2025.[5]

Todas las organizaciones están en una fase diferente de su recorrido hacia el cloud. Los requisitos de conformidad, las normativas locales y otros retos de migración implican que no todas las organizaciones están listas para traspasar cargas de trabajo críticas al cloud. Las estrategias de cloud híbrido son una forma en que las organizaciones pueden introducirse fácilmente en el cloud, manteniendo algunas cargas de trabajo on-premises y trasladando otras.

Los modelos de servicio en el cloud afectan a cómo comparten responsabilidades los proveedores de servicios y los clientes. Esto genera problemas para los CISO mientras sortean los retos que supone renunciar a algunos de los controles de las soluciones on-premises en favor de la mayor seguridad que los proveedores del cloud pueden proporcionar.

La regla general para la seguridad en el cloud es que es una responsabilidad compartida. Los proveedores de servicios en el cloud tienen que proporcionar la seguridad y el cifrado más avanzados, pero los clientes deben asegurarse de que los servicios que compran son realmente seguros, y de que extienden las políticas de seguridad necesarias a sus nuevos recursos en el cloud.

[5] "¿El cloud es seguro?", Gartner, octubre de 2019.

Prueba esto

Hazte las preguntas adecuadas. Evaluar a los proveedores del cloud no es solo cuestión de elegir un servicio, sino de elegir a quién confiar tus datos. Entre las preguntas fundamentales sobre seguridad y control de acceso que debes plantearte se incluyen:

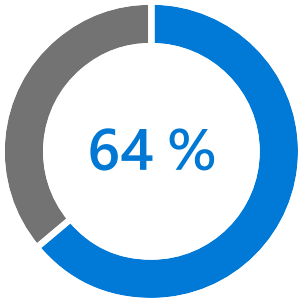
- ¿Están nuestros datos protegidos con fuertes medidas de seguridad y tecnología de vanguardia?
- ¿Está incorporada la privacidad por diseño y podemos controlar nuestros datos en nuestro cloud empresarial?
- ¿Qué tipos de inversiones se han hecho en procesos de cumplimiento sólidos e innovadores que nos ayuden a satisfacer nuestras necesidades de cumplimiento?
- ¿Dónde se almacenarán nuestros datos, quién tiene acceso a ellos y por qué?
- ¿Se realizan evaluaciones anuales de terceros para garantizar que se cumplan las normas de seguridad y cumplimiento?
- ¿Se rechazará cualquier petición para la divulgación de datos personales de los clientes que no sean jurídicamente vinculantes?
- ¿Se cumplen a los estándares de conformidad y regulación de los diferentes países y ubicaciones? En caso afirmativo, ¿cuáles son?

Conclusiones principales

Al evaluar los proveedores de servicios en el cloud, asegúrate de que cumplan con normas internacionales.

Busca proveedores que publiquen información detallada sobre cómo operan sus servicios y manejan los datos.

5. Echar un vistazo a la TI en la sombra



de los empleados han creado al menos una cuenta (registrándose en un sitio web o una aplicación relacionados con el trabajo) sin intervención del departamento de TI.[6]

El hecho de que un empleado cree una cuenta en el cloud sin la autorización o el conocimiento de la empresa se conoce como TI en la sombra. Las cuentas parecen bastante inofensivas: una herramienta para corregir los errores gramaticales, por ejemplo. Sin embargo, estas cuentas crean vulnerabilidades incluso en las configuraciones de seguridad más estrictas.

Los usuarios suelen aceptar los términos y condiciones sin leerlos y sin conocer totalmente a lo que están concediendo acceso. Las soluciones de seguridad de red tradicionales no se han diseñado para proteger los datos de las aplicaciones SaaS y no pueden ofrecer visibilidad al departamento de TI sobre cómo los empleados usan el cloud.

En última instancia, no queremos suprimir las motivaciones que subyacen a la TI de la sombra. Permitir que los usuarios y los equipos utilicen las aplicaciones en el cloud más adecuadas para su tipo de trabajo ayuda a impulsar la innovación y la productividad. Obtener visibilidad, control y protección frente a las amenazas de las aplicaciones SaaS en la sombra es el primer paso para administrar los riesgos y facilitar la transformación digital que ya se ha iniciado en tu empresa.

[6] "Un nuevo estudio revela los riesgos de la TI en la sombra", 1password, febrero de 2020.

Prueba esto

Obtén la información que necesitas. Los agentes de acceso de seguridad al cloud (CASB) ofrecen a las organizaciones una imagen detallada de cómo sus empleados usan el cloud:

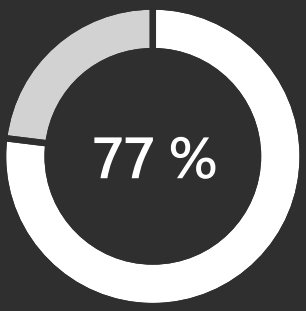
- ¿Qué aplicaciones en el cloud utilizan los empleados?
- ¿Qué riesgo suponen estas aplicaciones para la organización?
- ¿Cómo se accede a estas aplicaciones?
- ¿Qué tipo de datos se están enviando y compartiendo desde estas aplicaciones?
- ¿Cómo es el tráfico de carga y descarga?
- ¿Existen anomalías en el comportamiento de los usuarios como viajes imposibles, intentos fallidos de inicio de sesión o IP sospechosas?

Conclusiones principales

Los agentes de seguridad para el acceso al cloud (CASB) pueden ofrecerte una imagen detallada de cómo los empleados usan el cloud.

Con una mayor visibilidad, puedes definir políticas que hagan un seguimiento y controlen cómo los empleados utilizan estas aplicaciones.

6. Hacer que la protección y la productividad sean perfectas



de los CISO afirman sentirse atrapados entre dejar a los usuarios trabajar libremente y mantener la empresa segura.[7]

Los datos escapan a tu control ahora más que nunca, ya que tus empleados, socios y clientes los comparten. Si bien esto ayuda a impulsar la productividad y la innovación, puede tener consecuencias importantes si datos muy confidenciales acaban en manos equivocadas. Los responsables de seguridad deben administrar y proteger los datos almacenados en varias ubicaciones y compartidos a través de fronteras internacionales para cumplir las normativas.

Los empleados tolerarán tan solo cierto grado de molestias antes de encontrar soluciones alternativas a los requisitos de seguridad. La clasificación y el cifrado son las mejores maneras de mantener los datos seguros y al mismo tiempo permitir el uso productivo y el intercambio de información. Se pueden eludir los errores humanos automatizando la clasificación de datos. Las herramientas pueden entender el contexto de los datos, como números de tarjeta de crédito dentro de un archivo, o el carácter confidencial de los datos según su origen. Una vez etiquetados, se pueden aplicar automáticamente marcas visuales (encabezados, pies de página y marcas de agua) y también protección (como cifrado, autenticación y derechos de uso) a los datos confidenciales.

[7] "La seguridad de la TI obstaculiza la productividad y la innovación, según un estudio", ComputerWeekly.com, octubre de 2017.

Prueba esto

Familiarízate con los detalles. Los equipos de seguridad deberían poder hacer un seguimiento de las actividades en los archivos compartidos altamente confidenciales o que tienen gran repercusión para la empresa y revocar el acceso si es necesario.

- Esta protección persistente viaja con los datos y los protege en todo momento, independientemente de dónde se almacenen o con quién se hayan compartido.
- Un sistema de administración de identidades y acceso alivia la carga de realizar el seguimiento de los archivos con un alto nivel de confidencialidad.

Conclusiones principales

La seguridad en el nivel de los datos es responsabilidad de todos.

La clasificación y el etiquetado de los datos deben realizarse en el momento de la creación, y los equipos de seguridad deben poder supervisar las actividades en los archivos y tomar medidas rápidas.

Microsoft

Conclusión

Dada la naturaleza polifacética de las ciberamenazas, ya no basta con resolver tan solo algunos de los desafíos de seguridad a los que uno se enfrenta. Las necesidades de seguridad de cada empresa son únicas, pero las empresas se enfrentan a los mismos desafíos y comparten la misma responsabilidad de proteger sus datos, personas y sistemas, al tiempo que fomentan la innovación y el crecimiento. Necesitas marcos de seguridad ágiles que promuevan y apoyen la transformación digital, respaldados por estrategias integrales de seguridad incorporadas en tecnologías, procesos y programas de formación.

Si no te has planteado una migración al cloud, ahora es un momento excelente para explorar las mayores capacidades de seguridad que se ofrecen en ese entorno. Microsoft 365 ofrece una solución completa e inteligente para empresas de cualquier tamaño que admite su transformación digital con funcionalidad de seguridad y cumplimiento integrada en todos los niveles.

Obtén más información en esta serie de seminarios web gratuitos y exhaustivos.

Ver la serie >