Microsoft

Seis pasos para crear una estrategia holística de seguridad

Esta información es para usted

Si usted es un director de seguridad de la información o líder de seguridad de TI que:

- Necesita una guía rápida y que tenga sentido para la estrategia general de seguridad.
- Desea mantenerse informado con relación a los procedimientos de seguridad más recientes.

Tiempo de lectura estimado: <9 minutos

Contenido

Cumplir con el desafío

Proteger los datos y los sistemas es una prioridad para las organizaciones. Pero cumplir con este desafío se vuelve más difícil cada día a medida que los ataques se tornan más sofisticados, los empleados utilizan una variedad más amplia de dispositivos y aplicaciones, y los flujos de datos entran y salen de su negocio de más maneras. Con la migración masiva al trabajo remoto, la seguridad se ve aún más comprometida.

Los líderes tienen que equilibrar estos desafíos con la necesidad de colaborar, innovar y expandir un negocio. Necesita un enfoque de seguridad multifacético 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 fuertes que sean sus defensas, las medidas preventivas ya no bastan, también necesita adoptar una postura de "suponer una infracción" 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 sean respaldados por estrategias holísticas integradas en tecnologías, procesos y programas de capacitación. Si bien todo esto está disponible para las soluciones locales, lo cierto es que una migración a la nube mejora inmediatamente las capacidades de seguridad en toda su organización.

> **En este eBook se comparten los seis procedimientos recomendados de los CISO que han concentrado todos sus esfuerzos en la seguridad para poder prosperar. Estos procedimientos recomendados se aplican a un escenario local, pero son infinitamente más fáciles de lograr en un escenario de nube.**

1. Use los productos de seguridad integrados para permitir una respuesta rápida

75

Cantidad de productos de seguridad que usa una organización grande promedio.[1]

Los atacantes han evolucionado de los ataques "relámpago" que vulneran los sistemas con la esperanza de mantener una presencia continua, a largo plazo. Ahora usan una variedad de vectores y una gama cada vez mayor de técnicas y herramientas avanzadas: roban credenciales, instalan malware que se borra a sí mismo para evitar la detección, modifican los procesos internos y desvían datos de las redes, usan engaños de ingeniería social e incluso atacan los teléfonos móviles y los 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 pocas veces funcionan juntas. Muchos utilizan paneles, consolas y registros propietarios. La dificultad de la integración complica tener una visión general y prioriza las amenazas rápidamente. Esto se vuelve un desafío aún mayor cuando se trata de recursos locales y en la nube. Como resultado, los ataques pueden pasar inadvertidos durante más de 140 días.[2]

[1] "Symantec Introduces New Era of Advanced Threat Protection", Businesswire, octubre de 2015.

[2] "Threat Landscape: By the Numbers". Mandiant, A FireEye Company, 2016.

Intente hacer esto

A medida que la detección y la respuesta rápidas se vuelven más importantes, han surgido estos procedimientos recomendados:

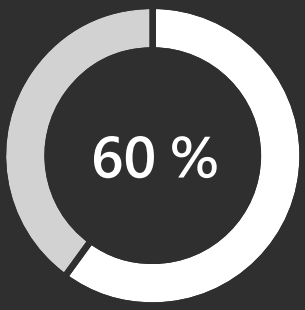
- Obtenga una visión holística de la seguridad de toda su red, incluidos los entornos híbridos y en la nube.
- Cree un ecosistema de productos y plataformas de seguridad que se integren entre sí y proporcionen información.
- Asóciese con los proveedores de tecnología que colaboren y compartan información con toda la industria de seguridad.

Aspectos claves

La falta de integración entre los productos de seguridad hace que sea difícil para los equipos de seguridad ver y combatir rápidamente las amenazas de forma holística.

Busque productos diseñados para integrarse con otros.

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



de las vulneraciones se originan en un punto de conexión comprometido.[3]

Una filtración de datos puede tener enormes costos. El establecimiento de controles de seguridad adecuados para tener visibilidad de las amenazas y los ataques es una forma de combatir este costo elevado. Sin embargo, los equipos de seguridad también tienen que apoyar a TI de consumo, donde los empleados ya no trabajan de forma exclusiva en dispositivos estrictamente controlados y entregados por la empresa, y esperan trabajar en cualquier lugar, en cualquier dispositivo o plataforma, independiente de si ha sido sancionada por TI corporativa.

En este mundo, las estrategias de seguridad basadas en la identidad vinculan el acceso a la identidad, no a los dispositivos. Aplique controles basados en el rol y la necesidad, independientemente de cómo se conecte el usuario. Este enfoque en autenticar y administrar a los usuarios a medida que acceden a los recursos corporativos también les permite a las organizaciones proteger sus datos sin importar dónde se almacenan, cómo se accede a ellos o con quiénes se comparten.

[3] "Top Five Security Threats Facing Your Business and How To Respond", Microsoft Secure Blog, octubre de 2016.

Intente hacer esto

Cambiar de una estrategia de seguridad que se trata exclusivamente de puntos de conexión le ofrece un enfoque más sólido. Estas herramientas pueden ser útiles:

- **Soluciones de administración de identidades y acceso (IAM)** y soluciones de **administración de aplicaciones móviles con soluciones de prevención de pérdida de datos (DLP)**. Ambos ayudan a reducir el riesgo protegiendo el acceso a aplicaciones y datos en recursos corporativos y en la nube. La IAM puede eliminar la necesidad de usar múltiples credenciales al entregar a los empleados una identidad única para acceder a los recursos locales y en la nube. Los sistemas de IAM basados en la nube también pueden usar las funciones de análisis e inteligencia de amenazas del proveedor de tecnología para detectar mejor los intentos de acceso anómalos y responder automáticamente cuando sea necesario.
- La **autenticación multifactor (MFA)** ofrece otra capa de protección que exige que el usuario presente algo que sabe (contraseña) y algo que tiene (autenticación secundaria a través de un dispositivo, de una huella digital o de reconocimiento facial). Otras tácticas sólidas incluyen 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 la MFA de un usuario en tiempo real en función de las directivas que establezca, lo que, en esencia, permite a las organizaciones aumentar la protección en su propia puerta principal.

Aspectos claves

Una estrategia de seguridad basada en la identidad pasa del control de puntos de conexión (dispositivos) a la administración de los usuarios que acceden a los datos corporativos.

Una protección de puntos de conexión más sólida ofrece información posterior a la infracción de las técnicas del adversario.

3. Adopte un modelo de Confianza cero para derrotar las amenazas

17.000

alertas de malware

La cantidad que las organizaciones grandes promedio deben analizar cada semana.[4]

Los hackers saben que cada organización tiene varios puntos de entrada. Utilizan estafas de phishing, ataques de malware y spyware, vulneraciones de navegador y software, acceso a través de dispositivos perdidos y robados, ingeniería social y otras tácticas para infringir su seguridad. Es necesaria una vigilancia constante para mantener la visibilidad de todas las amenazas que ya conoce y para tomar conciencia de las vulnerabilidades emergentes.

Algunas herramientas pueden ayudar a mantener un enfoque de seguridad permanente, pero un enfoque más amplio tiene más sentido. Las herramientas tradicionales se centran en la prevención, pero eso ya no es suficiente. Las organizaciones deben suponer que ya se ha producido una vulneración o que se producirá pronto. Esto se conoce como Confianza cero. A continuación, deben encontrar formas de reducir significativamente el tiempo necesario para detectarlas y recuperarse de ellas.

[4] "The Cost of Malware Containment". Ponemon Institute, enero de 2015.

Intente hacer esto

Sea experto en seguridad avanzada. Anticiparse a las amenazas puede darle una mirada retrospectiva para aprender de los incidentes, las actividades y los pasos que realizaron los hackers anteriormente.

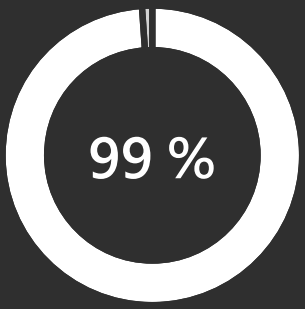
- Muchas aplicaciones de seguridad usan capacidades de análisis y machine learning integradas para analizar la forma en que un hacker obtuvo acceso. Las soluciones de seguridad y análisis más avanzadas usarán esa información para tomar automáticamente las medidas de prevención y respuesta adecuadas a vulneraciones similares, lo que ayuda a reducir el tiempo para la mitigación.
- Hay una amplitud y profundidad enormes de la señal y la inteligencia detrás de estas soluciones, y cuando se combinan con la experiencia y el conocimiento de los expertos humanos, pueden ser herramientas poderosas contra los atacantes dinámicos.

Aspectos claves

Las aplicaciones nativas de la nube admiten con más facilidad un modelo de Confianza cero que las aplicaciones heredadas.

Las aplicaciones heredadas requieren modernización para admitir el acceso condicional basado en la identidad.

4. Migre de forma segura a la nube



de las fallas de seguridad en la nube serán responsabilidad del cliente para el año 2025.[5]

Cada organización se encuentra en una etapa diferente de su viaje a la nube. Los requisitos, las normativas locales y otros desafíos de la migración significan que no todas las organizaciones están preparadas para migrar las cargas de trabajo críticas a la nube. Las estrategias de nube híbrida son una forma en que las organizaciones pueden irse acostumbrando a la nube, al mantener algunas cargas de trabajo locales y migrar otras.

Los modelos de servicios en la nube afectan la forma en que los proveedores de servicios y los clientes comparten responsabilidades. Esto plantea problemas para los CISO cuando afrontan los desafíos de tener que renunciar a algunas de las soluciones locales por la seguridad mayor que les pueden brindar los proveedores de nube.

La regla general para la seguridad en la nube es que se trata de una responsabilidad compartida. Los proveedores de nube tienen que contar con seguridad y cifrado de vanguardia, pero los clientes deben asegurarse de que los servicios que adquieren son realmente seguros y de que extienden las directivas de seguridad necesarias hacia los nuevos recursos en la nube.

[5] "Is the Cloud Secure", Gartner, octubre de 2019.

Intente hacer esto

Haga las preguntas correctas. Evaluar a los proveedores de nube no es solo elegir un servicio, sino elegir a quién confiar sus datos. Las preguntas críticas sobre seguridad y control de acceso que debe hacer incluyen:

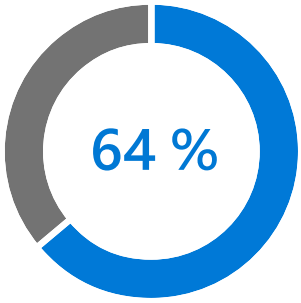
- ¿Están protegidos nuestros datos con una seguridad eficaz y tecnología de punta?
- ¿Incorpora la privacidad por diseño y permite el control de nuestros datos en la nube empresarial?
- ¿Qué tipo de inversiones ha realizado en los procesos de cumplimiento sólidos e innovadores para ayudarnos a satisfacer nuestras necesidades de cumplimiento?
- ¿Dónde se almacenarán nuestros datos, quién tiene acceso a estos y por qué?
- ¿Realiza revisiones anuales a través de terceros para garantizar que se cumplan las normativas de seguridad y cumplimiento?
- ¿Rechazará las solicitudes de divulgación de información personal de los clientes cuando no sean legalmente vinculantes?
- ¿Se atiene a las normativas de cumplimiento y reglamentarias de los diferentes países y localidades? Si es así, ¿a cuáles?

Aspectos claves

Al evaluar a los proveedores de servicios de nube, asegúrese de que cumplan con las normativas internacionales.

Busque a los proveedores que publiquen información detallada sobre la forma en que administran los servicios y datos.

5. Dele un vistazo a shadow IT



de los empleados han creado al menos una cuenta (se han registrado en un sitio web o una aplicación relacionada con el trabajo) sin involucrar al departamento de TI.[6]

Cuando un empleado crea una cuenta basada en la nube sin la autorización o el conocimiento de un negocio, esto se conoce como shadow IT. Las cuentas parecen bastante inofensivas: una herramienta para corregir la gramática escrita, por ejemplo. Sin embargo, estas cuentas crean vulnerabilidades incluso en las configuraciones de seguridad más estrictas.

Las personas frecuentemente aceptan los términos y condiciones sin leerlos ni entender cabalmente a qué otorgan acceso. Las soluciones de seguridad de red tradicionales no se diseñaron para proteger los datos en las aplicaciones de SaaS y no pueden entregar visibilidad de TI sobre la forma en que los empleados usan la nube.

En última instancia, no queremos reprimir las motivaciones detrás de shadow IT. Permitir a las personas y los equipos que utilicen las aplicaciones en la nube más adecuadas para su tipo de trabajo ayuda a fomentar la productividad y la innovación. Lograr visualizar, controlar y proteger las aplicaciones de SaaS en shadow IT son los primeros pasos para controlar los riesgos y facilitar la transformación digital que ya empezó en su empresa.

[6] "New research reveals risks of shadow IT", 1password, febrero de 2020.

Intente hacer esto

Obtenga la información que necesita. Los agentes de seguridad de acceso a la nube (CASB) entregan una imagen detallada de la forma en que los empleados usan la nube:

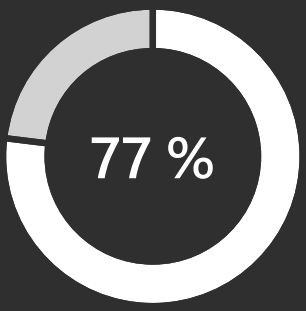
- ¿Qué aplicaciones están usando los empleados?
- ¿Qué riesgo representan estas aplicaciones para la organización?
- ¿Cómo se accede a estas aplicaciones?
- ¿Qué tipos de datos se envían y comparten en estas aplicaciones?
- ¿Cómo se ve el tráfico de carga y descarga?
- ¿Se detectan anomalías en el comportamiento de los usuarios, como viajes imposibles, intentos fallidos de inicio de sesión o direcciones IP sospechosas?

Aspectos claves

Los agentes de seguridad de acceso a la nube (CASB) pueden entregarle una imagen detallada de la forma en que los empleados usan la nube.

Con una mejor visibilidad, puede establecer directivas que registren y controlen la forma en que los empleados utilizan esas aplicaciones.

6. Haga que la protección y la productividad sean perfectas



de los CISO señalan sentirse atrapados entre permitir que las personas trabajen libremente y mantener la seguridad de la empresa.[7]

Los datos escapan de su control ahora más que nunca, ya que sus empleados, socios y clientes los comparten. Esto impulsa la productividad y la innovación, pero puede tener consecuencias significativas si los datos altamente confidenciales caen en las manos equivocadas. Los líderes de seguridad deben administrar y proteger los datos almacenados en varias ubicaciones y compartidos en distintos países, en cumplimiento con la normativa.

Los empleados tolerarán solo cierta cantidad de contratiempos antes de buscar soluciones alternativas a los requisitos de seguridad. La clasificación y el cifrado de los datos son las mejores maneras de mantener los datos seguros y, al mismo tiempo, permitir el uso productivo y el intercambio de información. Puede eludir el error humano al automatizar la clasificación de datos. Las herramientas son capaces de entender el contexto de los datos (por ejemplo los números de tarjeta de crédito dentro de un archivo o la confidencialidad de los datos) en función del origen de estos. Una vez que la información confidencial está debidamente etiquetada, se pueden aplicar automáticamente marcas visuales (como encabezados, pies de página y marcas de agua) y protección (como cifrado, autenticación y derechos de uso).

[7] "IT security hindering productivity and innovation, survey shows", ComputerWeekly.com, octubre de 2017.

Intente hacer esto

Siéntase cómodo con los detalles. Los equipos de seguridad deberían poder registrar la actividad en los archivos compartidos que son altamente confidenciales o que tienen un alto impacto comercial, y revocar el acceso si fuera necesario.

- Esta protección continua se desplaza junto a los datos y los protege en todo momento, independientemente de dónde se almacenan o con quién se comparten.
- Un sistema de administración de identidades y acceso alivia la carga de realizar seguimiento a archivos altamente confidenciales.

Aspectos claves

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

La clasificación y el etiquetado de datos deben producirse en el momento de la creación, y los equipos de seguridad deben ser capaces de supervisar las actividades en los archivos y tomar medidas rápidamente.

Microsoft

Conclusión

La naturaleza multifacética de las ciberamenazas significa que ya no basta con solo resolver algunos de sus desafíos de seguridad. 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, a la vez que fomentan la innovación y el crecimiento. Usted requiere marcos de seguridad ágiles que promuevan y apoyen la transformación digital, respaldados por estrategias holísticas de seguridad integradas en tecnologías, procesos y programas de capacitación.

Si no ha considerado realizar la migración a la nube, este es un buen momento para explorar las capacidades de mayor seguridad que encontrará allí. Microsoft 365 ofrece una solución completa e inteligente para empresas de todos los tamaños, que admite su transformación digital con funcionalidad de seguridad y cumplimiento integrada en todos los niveles.

Obtenga más información en esta serie de completos webinars gratuitos.

Vea la serie >