MONOGRÁFICO

11 controles de seguridad para reducir el ciberriesgo

Formas prácticas de reforzar sus defensas, mejorar la resiliencia cibernética y reducir el riesgo para la organización.

SOPHOS

Resumen ejecutivo

Es esencial que el equipo directivo de toda organización sea consciente de que optimizar los controles de seguridad no solo supone proteger los datos y los sistemas, sino también reducir el riesgo para la empresa en lo que respecta a la reputación de la marca, la confianza de los clientes y la continuidad de la actividad. Los ciberataques, como el ransomware y las estafas por correo electrónico corporativo comprometido (BEC), pueden tener graves consecuencias operativas y financieras. Según la revista Cyber Defense Magazine, se prevé que la ciberdelincuencia le cueste al mundo 1,2 billones USD en 2025[1]. Aunque los ataques se mitiguen, pueden causar graves interrupciones si es necesario desconectar los sistemas para restablecerlos y reinstalarlos. Algunas organizaciones pueden capear este tipo de temporal. Otras se plantean cuestiones existenciales que nunca habían previsto.

1,2 billones USD

Se prevé que en 2025 la ciberdelincuencia le cueste al mundo 1,2 billones USD.[1]

El papel de los controles de seguridad a la hora de maximizar las ciberdefensas

Los controles de seguridad son las herramientas que los equipos de seguridad pueden utilizar para reducir el riesgo y proteger a la organización frente a las amenazas. Existen muchos tipos de controles, pero todos ellos comparten el objetivo de prevenir incidentes y filtraciones de seguridad o minimizar los daños cuando se producen incidentes de seguridad. Algunos se centran en la prevención, mientras que otros ofrecen diferentes niveles de mitigación en materia de prevención, detección y respuesta ante amenazas. Es fundamental contar con la combinación perfecta de controles de seguridad sólidos en todas las áreas para lograr una defensa exhaustiva.

Unos controles de seguridad eficaces también son un componente fundamental para gestionar el riesgo a través de los ciberseguros. Las aseguradoras tienen en cuenta los controles de la organización a la hora de fijar las primas y los límites de la cobertura.

Por lo general, estos cubren:

Las **responsabilidades propias** incluyen los daños directos que su organización puede sufrir como consecuencia de un ciberataque o una filtración de seguridad. Estos daños pueden incluir la interrupción de la actividad comercial, los costes de restauración de datos, el robo de datos o el pago de un rescate debido al ransomware.

Las **responsabilidades frente a terceros** se derivan de clientes, Partners, reguladores u otros y pueden incluir demandas, reclamaciones de indemnización o multas impuestas por organismos gubernamentales o asociaciones comerciales.

Por qué es importante

Unos controles más eficaces no solo protegen sus operaciones, sino que también pueden reducir las primas del seguro y mejorar la tramitación de las reclamaciones de indemnización.

Reduzca el ciberriesgo con estos 11 controles de seguridad

Invertir en controles sólidos ayuda a reducir el ciberriesgo y puede contribuir a mejorar la asegurabilidad y las posibles condiciones de las pólizas. A continuación presentamos 11 controles básicos que refuerzan las defensas en diversas categorías de prevención y reducción del impacto.

Si se aplican correctamente, estos controles de seguridad refuerzan la postura de ciberseguridad y la preparan para hacer frente tanto a las amenazas de hoy como a las del futuro.

1. Gestión de identidades y accesos
2. Seguridad para endpoints
3. Autenticación multifactor
4. Gestión de vulnerabilidades
5. Protección del correo electrónico
6. Gestión de sesiones con privilegios
7. Gestión de activos
8. Segmentación y arquitectura
9. Detección y respuesta ampliadas (XDR)
10. Copias de seguridad y continuidad de la actividad
11. Seguridad de la red y control del tráfico

1. Gestión de identidades y accesos

La gestión de identidades y accesos (IAM) garantiza que solo las personas autorizadas puedan acceder a los sistemas y datos. La gestión del acceso con privilegios (PAM) limita aún más el acceso a lo estrictamente necesario para los usuarios. Puede parecer sencillo, pero esto puede convertirse rápidamente en un aprieto, especialmente en las organizaciones más grandes. Todas las empresas deben mantener procesos estrictos de incorporación y salida de empleados, aplicar una higiene de contraseñas segura y auditar periódicamente los accesos.

Independientemente del tamaño, todas las organizaciones deben contar con normas claras para eliminar identidades obsoletas; de lo contrario, los atacantes pueden explotar las cuentas olvidadas para aumentar privilegios y moverse lateralmente por su entorno sin ser detectados.

2. Seguridad para endpoints

Cada uno de los dispositivos conectados a su entorno es un posible blanco de ataque. El trabajo híbrido ha supuesto una mayor exposición, por lo que la protección de endpoints es más importante que nunca. Muchos ataques comienzan con amenazas "genéricas" poco complejas que una herramienta para endpoints potente puede detectar y neutralizar. Sin embargo, los endpoints descuidados o que ya no reciben soporte suelen convertirse en puntos débiles y son un punto de entrada habitual para los ataques de ransomware remoto. Asegúrese de que todos los dispositivos estén protegidos.

3. Autenticación multifactor

La autenticación multifactor (MFA) valida la identidad de un usuario con múltiples factores: algo que sabe (p. ej., una contraseña), algo que tiene (p. ej., un token) o algo que es (p. ej., una huella digital). Dado que el compromiso de credenciales sigue siendo una de las principales causas de los ataques,[2] la MFA es un control vital para las organizaciones modernas. Plantéese formas más avanzadas, como la geolocalización y la coincidencia de números, para mejorar la resiliencia frente a las tácticas de elusión de los atacantes, al tiempo que consigue el equilibrio entre la experiencia del usuario y la privacidad.

Conclusiones

Las cuentas inactivas y los privilegios no utilizados son vías de acceso fáciles para los atacantes. Una vez dentro, pueden usarse para elevar el acceso y ampliar discretamente el alcance de un ataque.

El punto de entrada más común suele ser el menos visible. No deje que los endpoints no actualizados se conviertan en una puerta trasera.

Implemente la autenticación MFA adaptativa para aumentar la verificación en situaciones de alto riesgo sin generar fricción innecesaria.

4. Gestión de vulnerabilidades

La gestión de vulnerabilidades es el proceso continuo de identificar, evaluar y remediar las deficiencias de seguridad en todo su entorno. Incluye prácticas comunes como la aplicación de parches de software y sistemas, actualizaciones de configuración y supervisión de vulnerabilidades recién descubiertas. Una sólida información sobre amenazas es fundamental para poder adelantarse a los riesgos emergentes.

Saber dónde se encuentran todos los recursos de la red es esencial para que los escaneados puedan realizarse de forma exhaustiva. Con tal visibilidad, las organizaciones pueden adoptar un enfoque basado en el riesgo para priorizar las vulnerabilidades que deben abordarse primero, en función de la exposición, la probabilidad de explotación y el impacto en el negocio.

5. Protección del correo electrónico

A pesar de ser una tecnología antigua, el correo electrónico sigue siendo uno de los principales puntos de entrada para los atacantes. En concreto, el phishing es un vector habitual para el ransomware y el robo de credenciales. Las estafas por correo electrónico corporativo comprometido (BEC) también se encuentran entre las reclamaciones de indemnización más frecuentes a las ciberaseguradoras.[3] Una seguridad del correo electrónico sólida puede evitar que el contenido malicioso llegue a la bandeja de entrada, lo que lo convierte en una primera línea de defensa fundamental. A medida que la IA generativa perfecciona las tácticas de phishing con una gramática y mensajes más elaborados, las protecciones deben evolucionar para reducir el índice de éxito de estos ataques antes de que lleguen a los usuarios.

Pero la protección no debe limitarse a la fase de entrega. Las URL y los archivos adjuntos que parecen seguros en un primer momento pueden convertirse en elementos maliciosos una vez que el mensaje llega a la bandeja de entrada. Ahora, las soluciones avanzadas de protección del correo electrónico ofrecen detección y remediación posentrega, lo que permite volver a analizar automáticamente el contenido, recuperar los mensajes maliciosos y neutralizar los enlaces si cambia su perfil de riesgo. Estos controles ayudan a detectar las amenazas que logran burlar las defensas iniciales y minimizan el tiempo que los mensajes dañinos permanecen en las bandejas de entrada de los usuarios.

Conclusiones

Busque vulnerabilidades en sus aplicaciones y servicios en la nube de terceros, no solo en sus sistemas centrales.

Solo hace falta un clic. La mejor manera de detener el phishing es asegurarse de que los usuarios nunca vean el cebo, ni siquiera después de entregarlo.

6. Gestión de sesiones con privilegios

Las cuentas de administrador ofrecen a los ciberdelincuentes el máximo poder, especialmente cuando esos privilegios incluyen el acceso a sistemas de identidad, controles de configuración y herramientas de seguridad. Si un atacante consigue acceso a nivel de administrador, puede desactivar las defensas y desplegar ransomware a escala.

Para reducir ese riesgo, las organizaciones deben implementar un modelo por niveles para el acceso con privilegios y supervisar de forma activa cómo se utilizan esas cuentas. La gestión de sesiones con privilegios (PSM) permite supervisar, registrar y, en algunos casos, controlar las sesiones de administrador en tiempo real, lo que ayuda a detectar actividades sospechosas, evitar el uso indebido y garantizar el cumplimiento normativo.

7. Gestión de activos

No podemos proteger lo que no sabemos que tenemos. Las organizaciones deben mantener al día inventarios tanto de activos físicos como de datos. Durante un incidente, saber dónde se almacenan los datos confidenciales es fundamental para llevar a cabo una investigación pronta y eficaz, elaborar informes detallados y contener rápidamente la situación. Una gestión adecuada de los activos favorece una investigación exhaustiva, ayuda a delimitar responsabilidades y reduce el impacto de una filtración.

8. Segmentación y arquitectura

Si un ciberdelincuente logra acceder a su entorno, su siguiente paso suele ser el movimiento lateral, es decir, intentar aumentar sus privilegios, acceder a sistemas confidenciales o desplegar ransomware. Una segmentación sólida de la red y una arquitectura bien diseñada pueden dificultar mucho esa maniobra. Al generar fricción y obligar a los adversarios a hacer más ruido, la segmentación aumenta las posibilidades de detectarlos antes en la cadena de ataque.

La arquitectura de un sistema debe regirse por los principios de confidencialidad, integridad, disponibilidad y resiliencia. Esto incluye limitar el acceso entre sistemas y entre usuarios y sistemas mediante un modelo Zero Trust, en el que cada transacción se verifica en función de la identidad, el dispositivo y los permisos del usuario.

Conclusiones

¿Puede ver quién accedió como administrador al sistema el martes pasado y qué hizo exactamente? Si la respuesta es no, es hora de reforzar la supervisión.

Conservar registros innecesarios puede aumentar los costes del seguro y multiplicar el daño a la reputación en caso de filtración.

Segmente la red para aislar los sistemas críticos de los puntos de acceso rutinarios.

9. Detección y respuesta ampliadas (XDR)

Compaginar decenas de herramientas distintas puede fragmentar las alertas, ralentizar la clasificación y ocultar la actividad de las amenazas. La detección y respuesta ampliadas (XDR) soluciona esto al ofrecer una visión unificada de la actividad en los sistemas de protección de endpoints, firewalls, redes, correo electrónico, identidad, copias de seguridad y la nube, lo que reduce el número de alertas generado y permite una toma de decisiones más rápida y segura. Así, los analistas no tienen que alternar entre herramientas aisladas para investigar y responder a las amenazas.

Los sistemas XDR más robustos también aplican análisis avanzados, detección priorizada por IA, búsqueda exhaustiva de datos y correlación y derivación automatizadas de alertas. Esta convergencia de funcionalidades mejora la precisión de la detección, acelera las investigaciones y ayuda a los equipos de seguridad a centrarse en las amenazas de mayor riesgo sin atascarse en la fricción de las herramientas.

10. Copias de seguridad y continuidad de la actividad

Cuando un ciberincidente interrumpe las operaciones o daña los sistemas, unas copias de seguridad bien preparadas y un plan de continuidad de las actividades sólido pueden suponer la diferencia entre una recuperación rápida y un periodo de inactividad largo. Pero no todas las copias de seguridad son iguales. Para que sean eficaces, las copias de seguridad deben validarse, probarse periódicamente y han de poder restaurar los sistemas y los datos con integridad.

Un error habitual es la configuración: muchas organizaciones se percatan demasiado tarde de que sus copias de seguridad solo restauran parcialmente los sistemas o pierden datos críticos, lo que convierte una interrupción a corto plazo en un caos que dura semanas.

Es igualmente importante que las copias de seguridad estén protegidas mediante autenticación fuera de banda. Sin ella, un ciberdelincuente con acceso generalizado podría intentar desactivar o eliminar los datos de las copias de seguridad como parte de su ataque.

Conclusiones

La XDR transforma las alertas aisladas en acciones decisivas, lo que acelera las investigaciones y mejora los resultados de la respuesta.

Mantenga las copias de seguridad segmentadas y fuera de línea siempre que sea posible. Su recuperación nunca debe depender de un solo canal.

11. Seguridad de la red y control del tráfico

La red es más que una capa de conexión: es un punto de control estratégico para inspeccionar, filtrar y gestionar el tráfico en todo su entorno. Los firewalls, los sistemas de prevención de intrusiones (IPS), el filtrado de DNS y las puertas de enlace web seguras constituyen la columna vertebral de la implementación por capas.

Pero no todos los firewalls son iguales. Las soluciones heredadas, mal configuradas o infrautilizadas pueden presentar lagunas que pueden ser explotadas. Para mantener la resiliencia, es crucial evaluar periódicamente las defensas, mantenerlas actualizadas y alinearlas con el panorama actual de amenazas.

Los controles modernos, como Zero Trust Network Access (ZTNA), permiten aplicar medidas de acceso más granulares y sensibles al contexto. Junto con las protecciones tradicionales, ayudan a reducir la superficie de ataque, evitar el movimiento lateral y detener la exfiltración en entornos híbridos y en la nube.

Conclusiones

Integre la telemetría de red en su pila de detección para mejorar la visibilidad, agilizar las investigaciones e identificar actividades anómalas, sobre todo el movimiento lateral y el tráfico de comando y control.

De una visión integral a un enfoque integral

La ciberseguridad no consiste solo en desplegar las herramientas adecuadas, sino en contar con una estrategia que aúne a las personas, los procesos y la tecnología. Si se aplican de forma meditada y coherente, estos 11 controles pueden reducir considerablemente la exposición al riesgo de su organización.

La resiliencia a largo plazo pasa por crear un programa de ciberseguridad sólido, repetible, adaptable y fundamentado en una responsabilidad clara. La tecnología es poderosa, pero se necesitan equipos cualificados y procesos estructurados para garantizar que se utiliza de forma eficaz.

Evolucionarán las amenazas, cambiarán las tecnologías y su negocio también se transformará. Para mantenerse por delante hay que pensar de forma integral, adaptarse continuamente y crear una cultura en la que la seguridad no sea solo una casilla que marcar, sino un factor clave para el negocio.

[1] Cyber Defense Magazine: The True Cost of Cybercrime: Why Global Damages Could Reach $1.2-$1.5 Trillion by End of Year 2025
[2] Sophos, Informe anual sobre amenazas 2025
[3] Dark Reading, “Email-Based Attacks Top Cyber-Insurance Claims”, 8 de mayo de 2025

¿Listo para evaluar su programa de ciberseguridad?

Hable con un experto de Sophos hoy mismo.

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com