Aspectos destacados en seguridad: el costo de los errores humanos y las ventajas de la automatización

Descubra los motivos que llevan a los organismos gubernamentales a replantearse el uso de los enfoques manuales para gestionar la seguridad y la contribución de la automatización inteligente para evitar las posibles amenazas de las fallas de seguridad costosas.

Siguiente

Lea en este ebook:

01 Introducción: la creciente amenaza de los delitos cibernéticos

Los delitos cibernéticos siguen aumentando. Durante el último ejercicio económico, el Centro Australiano de Ciberseguridad (ACSC) recibió más de 67 500 denuncias de delitos cibernéticos (un aumento del 13 % anual)% con pérdidas informadas internamente que superaron los USD 33 000 millones[3]. Aproximadamente un cuarto de estos incidentes afectó a las entidades asociadas con la infraestructura esencial de Australia.

A medida que los organismos gubernamentales adoptan tecnologías nuevas y se adaptan a los modelos híbridos de trabajo, los atacantes cibernéticos también transforman sus habilidades. El personal y los recursos informáticos cada vez están más distribuidos, y el entorno de la infraestructura de TI que evoluciona rápidamente brinda a los malhechores formas nuevas de aprovecharse de las fallas y los puntos vulnerables de seguridad. Esto termina provocando un aumento en los costos por filtraciones de datos para las empresas; incluso aquellas que desarrollan estrategias sólidas de seguridad enfrentan más riesgos.

Medidas de seguridad para anticiparse a los delitos cibernéticos

Mientras los criminales cibernéticos idean formas nuevas de infringir los sistemas y los datos protegidos, las empresas padecen la presión interna y externa de desarrollar medidas más estratégicas y preventivas contra los ataques cibernéticos. De hecho, sus iniciativas que abordan la privacidad y la seguridad de los datos deben cumplir con más normas y reglas exhaustivas.

Por ejemplo, la política sobre la ciberseguridad de Nueva Gales del Sur (NSW) ahora exige la implementación y la ejecución de una evaluación de consolidación según el modelo Essential Eight del ACSC para revisar las estrategias de reducción de riesgos[1]. Además, con el proyecto de enmienda de la legislación sobre la seguridad de Australia (específicamente sobre la infraestructura esencial), posiblemente aumente la carga normativa en los organismos gubernamentales que gestionan u operan las infraestructuras más importantes[2] .

Refuerce sus medidas de protección

Las empresas que buscan mejorar la ciberseguridad primero necesitan identificar los puntos vulnerables actuales. Con bastante frecuencia, los errores humanos y una capacitación inadecuada pueden comprometer la seguridad, incluso cuando ya se pusieron en marcha las estrategias integrales. Los pequeños errores que se pasan pueden poner en riesgo a los sistemas, y así agravar un problema que ya de por sí era complejo. Como resultado, las empresas adoptan la automatización para mejorar la confiabilidad y reducir los riesgos en la estrategia de seguridad.

En este ebook, analizaremos los riesgos que se generan por los errores humanos y de qué manera esto perjudica la lucha contra los delitos cibernéticos. También abordaremos la automatización de las estrategias clave para la reducción de riesgos de ciberseguridad que puede fortalecer la seguridad y, a la vez, reducir el volumen de tareas que requieren mucho tiempo y representan una carga para los equipos de TI.

El costo de los delitos cibernéticos en Australia:

67 500

ataques cibernéticos denunciados[3]

USD 33 000 millones

en pérdidas informadas internamente[3]

13 %

anual de aumento en los ataques[3]

1. Gobierno de Nueva Gales del Sur. "DCS-2021-02 NSW Cyber Security Policy", febrero de 2021.
2. Parlamento de Australia. "Security Legislation Amendment (Critical Infrastructure) Bill 2021", 2021.
3. "ACSC Annual Cyber Threat Report 2020-21", Centro Australiano de Ciberseguridad, septiembre de 2021.

02 Todos deberían participar para que las estrategias de seguridad sean eficaces

Los seres humanos cometemos errores

Incluso dentro de los equipos de TI, las personas suelen subestimar o malinterpretar los puntos vulnerables de su sistema y los riesgos de seguridad consecuentes. Esta falta de capacidad para evaluarlos con precisión puede provocar costos considerables en las empresas.

Por ejemplo, imagínese que un técnico actualiza un firewall de forma manual y comete un pequeño error y, como no percibe que sea un problema, no lo resuelve. Lo que no se da cuenta es que este mínimo descuido genera un punto vulnerable importante en el sistema de TI de la empresa, el cual los criminales cibernéticos aprovecharán rápidamente.

En esta situación, el simple error del técnico podría provocar diferentes resultados negativos, entre ellos, datos comprometidos, infracción a las normas sobre seguridad de los datos del sector y del gobierno, interrupciones en los servicios y tiempo de inactividad de los sistemas, y todo eso en detrimento de la empresa.

Hay muchos elementos del sistema de seguridad que pueden presentar errores si se gestionan de forma manual: desde la ejecución de parches en las aplicaciones y la actualización de los firewalls hasta la configuración y la aplicación de los privilegios de administrador. A medida que los criminales cibernéticos mejoran sus habilidades para identificar los puntos vulnerables, usted puede sufrir consecuencias perjudiciales e irrecuperables si solo confía en los equipos de operaciones para llevar a cabo esas tareas.

La escasez de personal especializado agrava las fallas de seguridad

Las probabilidades de cometer errores humanos en las tareas manuales aumentan debido a que cuesta encontrar personas especializadas en ciberseguridad. En pocas palabras, no hay suficiente personal con las habilidades y la capacitación necesarias para evaluar y abordar los riesgos de seguridad. Según el estudio Cybersecurity Workforce Study de (ISC)[2], Australia necesita 25 000 trabajadores más en protección de la TI para resolver su falta de ciberseguridad[4].

La escasez crónica de estos especialistas dificulta la tarea de los organismos gubernamentales de gestionar los riesgos adecuadamente. Los equipos de TI ya tienen bastante presión y no tienen tiempo para aplicar los procesos de seguridad en toda la empresa, y mucho menos para definirlos.

Los equipos de seguridad deben usar la automatización

En esta lucha contra los delitos cibernéticos, se ha vuelto esencial analizar de qué forma los procesos manuales y la falta de habilidades en materia de seguridad aumentan los riesgos en las empresas. Por suerte, la automatización ofrece una solución prometedora. Como explicaremos con mayor detalle, la automatización de los procesos de seguridad proporciona la uniformidad, la precisión y la adaptación que tanto se necesitan en toda la empresa.

Las medidas de seguridad manuales son un riesgo

"Las empresas que no tienen la seguridad automatizada experimentaron un costo promedio de USD 6,71 millones por fallas en 2021, mientras que aquellas con una seguridad totalmente automatizada tuvieron un promedio de USD 2,90 millones"[5] .

4. "A Resilient Cybersecurity Profession Charts the Path Forward", Cybersecurity Workforce Study de (ISC)[2], 2021.
5. "Cost of a Data Breach Report 2021", IBM, 2021.

03 Desafíos comunes en la gestión de los riesgos

Los organismos gubernamentales necesitan una mejor gestión de los riesgos

Los organismos gubernamentales deben poder identificar y gestionar los riesgos de manera precisa y eficiente para poder garantizar la confidencialidad, la integridad y la disponibilidad de la información oficial. Las amenazas de seguridad están en permanente evolución, lo cual significa que las estrategias de protección y los perfiles de riesgo de las empresas deben ser adaptables. La automatización de las operaciones es esencial para responder a estos cambios con rapidez.

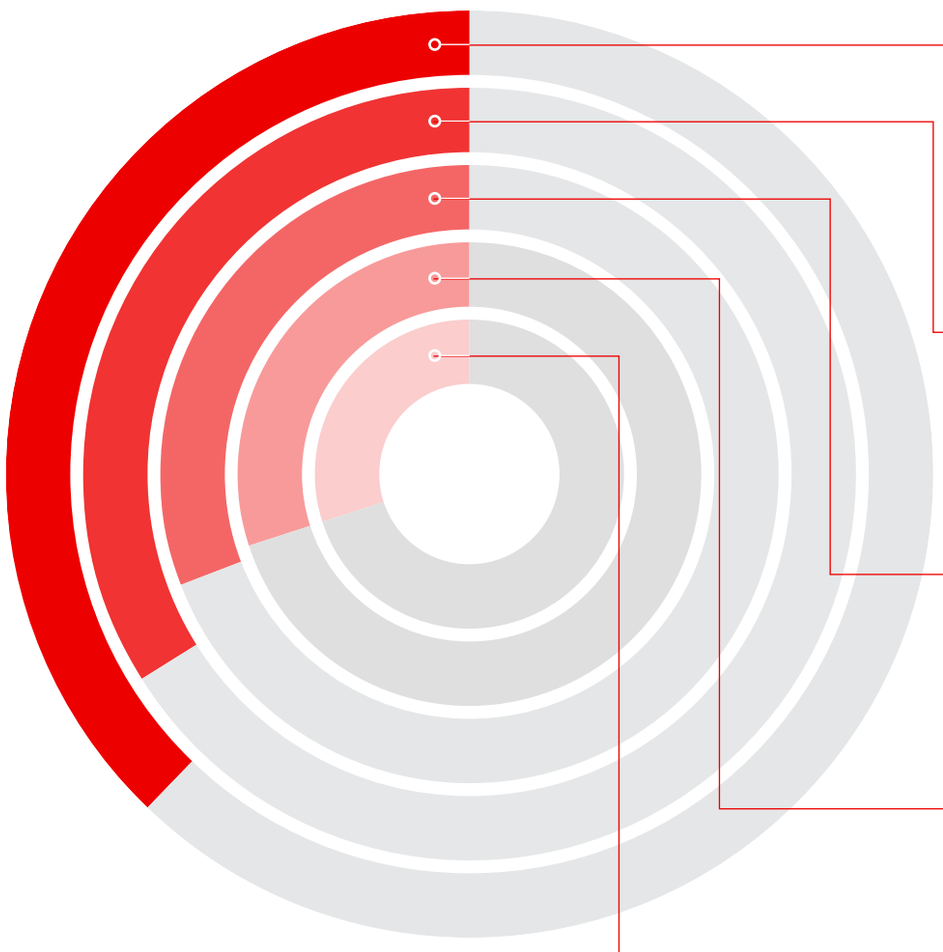
Los obstáculos a la hora de cambiar las prácticas de seguridad

Los organismos gubernamentales enfrentan varios desafíos, especialmente en relación con la gestión de los cambios, en cuanto a sus iniciativas para mejorar la seguridad. Estas son algunas de sus inquietudes más comunes:

- ¿Cómo adaptamos nuestro equipo para implementar una iniciativa nueva de ciberseguridad?
- ¿Cómo brindamos respaldo a las distintas partes de la empresa para garantizar que los protocolos de seguridad nuevos se cumplan?
- ¿Qué podemos hacer para proteger mejor nuestros sistemas actuales (que prestan servicios esenciales) mientras adoptamos las estrategias de seguridad modernas que necesita la empresa?
- ¿Podemos implementar estrategias como la confianza cero en las arquitecturas establecidas?

Sin embargo, en lugar de ver estos aspectos como una carga, las empresas pueden usar el panorama cambiante de la seguridad como una oportunidad para revaluar las prácticas en esta materia e implementar protocolos más estrictos.

Desafíos comunes de la ciberseguridad



38 %

Mantenerse al día con las amenazas que cambian rápidamente[6]

34 %

Concientizar sobre los riesgos y comportamientos[6]

31 %

Reforzar la estrategia interna de ciberseguridad[6]

30 %

Requerir capacitación sobre la ciberseguridad[6]

30 %

Considerar las implicaciones legales y financieras de las filtraciones de datos[6]

6. "State of the Channel 2021", CompTIA, agosto de 2021.

04 Fortalecimiento de las medidas de seguridad con la automatización

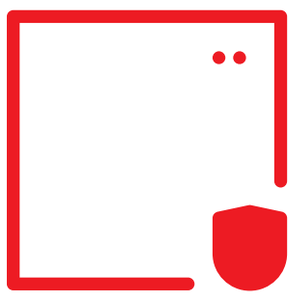
Automatice los elementos clave de su estrategia de ciberseguridad

Hoy en día, los organismos gubernamentales adoptan la automatización de la ciberseguridad para reducir los riesgos y hacer frente a esta clase de delitos. Cuando se automatiza el trabajo que se repite habitualmente, los equipos de ciberseguridad pueden enfocarse en las tareas más estratégicas y esenciales. Además, esta función evita sobrecargar a los equipos de TI con muchas tareas y trabajos, dado que esto aumentaría las probabilidades de que se cometan errores humanos y se produzcan riesgos de seguridad.

En el modelo Essential Eight del ACSC, se explica cómo puede utilizar la automatización para reforzar su estrategia de ciberseguridad. Ocurre en muchas empresas que, cuando lo implementan, se encuentran con que no hay forma de reducir o eliminar los errores humanos de manera uniforme, en especial debido a las limitaciones actuales en los recursos y la escasez de habilidades técnicas.

Los líderes de la TI comenzaron a notar que algunos elementos del marco de seguridad pueden y deberían automatizarse, para contrarrestar este problema. Vea estos ejemplos que ayudan a explicar de qué modo y en qué partes conviene adoptar la automatización en su empresa:

Automatización según el modelo Essential Eight del ACSC

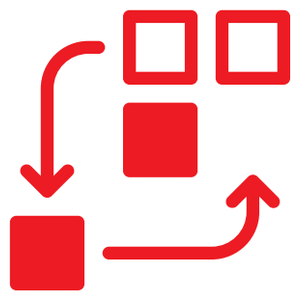


Control de las aplicaciones

Automatización de los cambios en el control de las aplicaciones en toda la nube híbrida

Ejecución de parches en las aplicaciones y en el sistema operativo

Automatización de las comprobaciones previas, la promoción de contenido y la verificación y las pruebas posteriores a las actualizaciones



Copias de seguridad y restauración

Automatización de los procesos de copia de seguridad, de las restauraciones y de las pruebas de verificación

Perfeccione la aplicación de parches

En el modelo Essential Eight, se recomienda que las empresas ejecuten los parches en las aplicaciones y las actualizaciones con frecuencia para no comprometer la seguridad y evitar ataques. La aplicación de parches en las aplicaciones no es solo una práctica recomendada sino también un requisito normativo. Dicho esto, llevar a cabo el proceso de forma manual siempre está sujeto a errores humanos y puede demandar bastante tiempo en las empresas grandes.

La aplicación de parches es un caso práctico estupendo para los flujos de trabajo automatizados. En lugar de depender de un especialista en TI para realizar las pruebas, configurar las comprobaciones previas y ejecutar los parches, las empresas pueden automatizar los procesos de verificación y prueba. De esta forma, se garantiza que todos estos pasos se realicen sin problemas y con eficiencia y que la seguridad interna establecida sea la adecuada.

Gestione los privilegios de administrador

En el modelo Essential Eight, se recomienda que las empresas restrinjan los privilegios de administrador para limitar el alcance de los ataques. El control del acceso con privilegios ayuda a proteger la infraestructura y las aplicaciones, ejecutar los procesos empresariales con eficiencia y mantener la confidencialidad de los datos que así lo requieran y la infraestructura esencial.

Solo un pequeño grupo de personas dentro de la empresa debería tener el control global, pero no es sencillo determinar quién debería tener esos privilegios. Tampoco lo es calcular la gravedad de un incidente de seguridad y evaluar el impacto total de ese posible evento, pero esta práctica le permite saber de forma anticipada qué sucedería si alguien usara mal las credenciales. Así el equipo de TI puede implementar medidas de seguridad para garantizar que el incidente no afecte a toda la empresa.

Cuando se automatizan los flujos de trabajo para la gestión de los accesos con privilegios y se almacenan las credenciales de manera centralizada (sin tener que insertarlas en las aplicaciones y que posiblemente se filtren), todo el proceso se vuelve más confiable y fácil de controlar.

05 La función de Red Hat en el enfoque para la ciberseguridad

Diseñe una práctica de ciberseguridad preparada para el futuro

Las soluciones de Red Hat® lo ayudan a automatizar los procesos manuales actuales y, de esa forma, disminuye los riesgos de que se produzcan descuidos debido a la sobrecarga de los equipos de TI de su empresa o al poco personal que los integra. Nuestros productos open source ofrecen flexibilidad y capacidad de ajuste en todas las arquitecturas y los entornos de nube, lo cual respalda a las empresas mientras realizan las implementaciones en sus entornos actuales y futuros.

El uso de la automatización como base de un modelo de consolidación de la ciberseguridad, les permite seguir pasos prácticos para agregar capas de automatización de manera rápida y constante, y reemplazar los procesos manuales. Las soluciones de Red Hat pueden ayudarlo con la eliminación de los riesgos y la respuesta frente a ellos.

Red Hat Ansible Automation Platform

La plataforma Red Hat Ansible® Automation Platform está diseñada con Ansible, un lenguaje de automatización comprensible para las personas que convierte los procesos manuales complejos en flujos de trabajo automatizados. Permite que sus equipos de TI automaticen e integren distintos protocolos de seguridad en toda la empresa. Además, puede utilizarla para investigar las amenazas y responder ante ellas de forma coordinada y unificada, usando un conjunto adaptado de módulos, funciones y playbooks.

Red Hat Ansible Automation Platform permite que las empresas automaticen ciertas tareas:

- La aplicación de parches en los puntos vulnerables y las exposiciones comunes (CVE).
- La implementación del control de aplicaciones.
- Los procesos de copia de seguridad y restauración o verificación.

Ansible Automation Platform presenta un marco empresarial estable y enfocado en la seguridad para diseñar y ejecutar la automatización de la TI según sea necesario, desde los entornos de la nube híbrida hasta los del extremo de la red. Con esta solución, los usuarios de toda la empresa pueden crear, compartir y gestionar los playbooks de Ansible, desde los equipos de desarrollo y operaciones hasta los de seguridad y redes. Los gerentes de TI pueden proporcionar a los equipos individuales los lineamientos para que apliquen esta herramienta, y sus creadores pueden redactar tareas para las que se necesiten los conocimientos actuales.

Además, Ansible Automation Platform puede servir como punto de integración para las soluciones de seguridad, ya que incluye contenido de partners certificados, como CyberArk, IBM y Splunk, que puede utilizarse para automatizar la gestión y la integración de las tecnologías de seguridad.

Obtenga más información sobre Ansible Automation Platform ›

Red Hat Enterprise Linux

Red Hat Enterprise Linux® ofrece una base desde la cual se pueden ajustar las aplicaciones actuales e implementar las tecnologías nuevas con una seguridad uniforme en todos los entornos virtuales, de nube, con servidores dedicados (bare metal) y en el extremo de la red.

Red Hat Enterprise Linux se enfoca de manera práctica en tres puntos clave para abordar los desafíos de seguridad:

- Reducir los riesgos: gestione la seguridad y disminuya el riesgo de que se produzcan filtraciones de información para evitar que sus datos, sus sistemas y su reputación se vean comprometidos.
- Brindar mayor protección: automatice y mantenga los controles de seguridad según sea necesario y con un tiempo de inactividad mínimo.
- Cumplir con los requisitos normativos: optimice las normas de cumplimiento en las empresas con entornos estrictamente regulados.

Red Hat Enterprise Linux también incluye políticas de seguridad integradas que se ajustan a la orientación del ACSC, como el manual Information Security Manual (ISM) y las estrategias del modelo Essential Eight. Gracias a ellas, los organismos gubernamentales gestionan mejor los riesgos automatizando la implementación de controles de seguridad en los servicios digitales nuevos, de manera simple y uniforme.

Obtenga más información sobre Red Hat Enterprise Linux ›

Anterior

Fortalezca la seguridad con Red Hat

Red Hat es la opción indicada para mejorar la seguridad de sus servicios digitales

Red Hat permite automatizar la orientación que ofrece el ACSC y mejorar la gestión de los riesgos con las integraciones de seguridad automatizadas.

Comuníquese con nosotros para obtener más información >