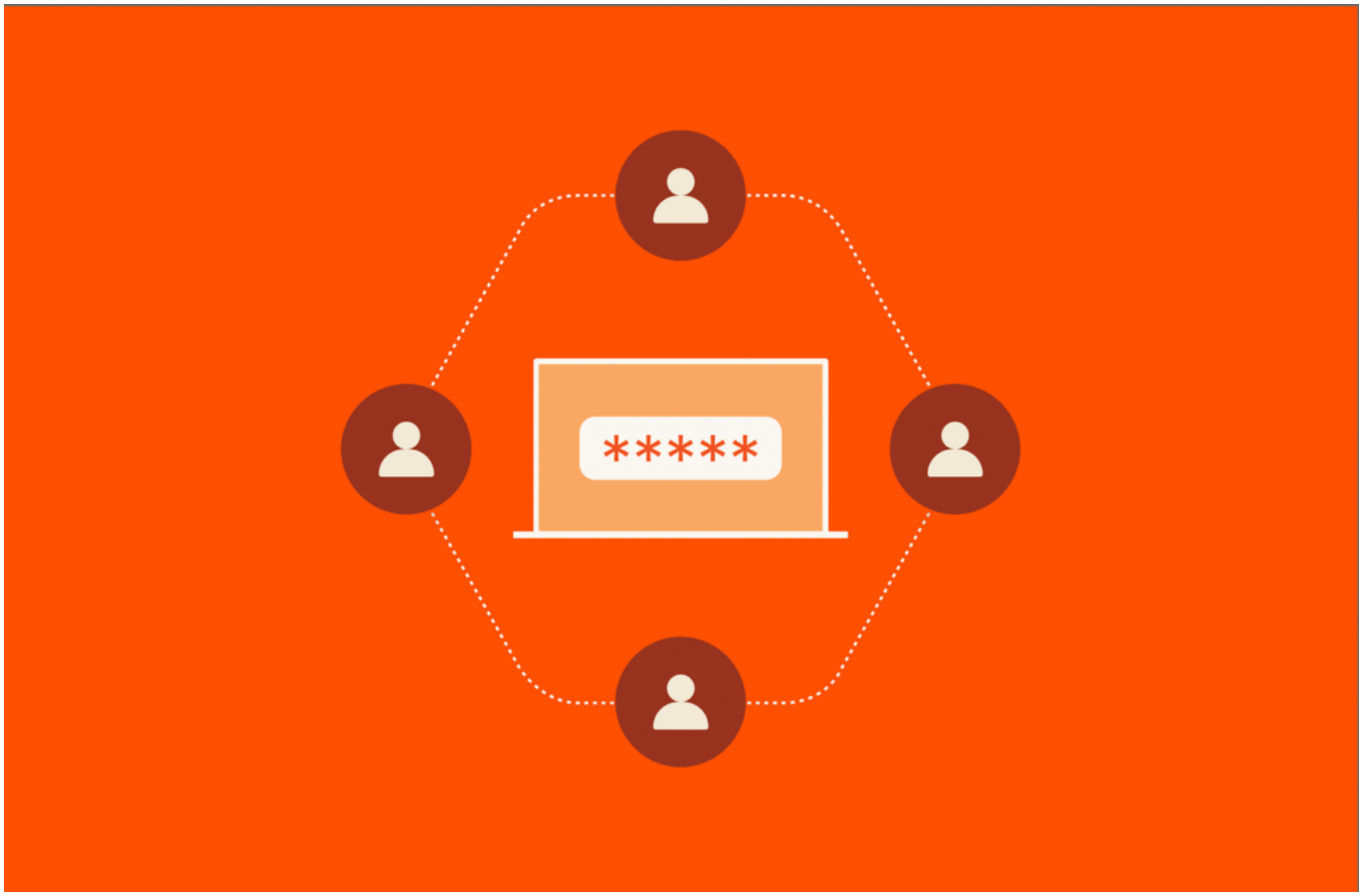
Si la resiliencia cibernética es un deporte en equipo, esto es lo que necesita en su banco



“Todos tienen un plan hasta que se golpean en la cara”, dijo el boxeador Mike Tyson.

Ese podría ser el mantra para los CISO y sus equipos de seguridad que pueden hacer toda la preparación posible antes de posibles incidentes de seguridad, solo para lanzar el libro de estrategias cuando la realidad llegue al fanático. Independientemente de cuánta preparación se haya hecho, un incidente de seguridad tiene una forma de poner al límite los procedimientos, las tecnologías y las personas de una organización.

No estamos argumentando que un manual de estrategias no sea importante para

la recuperación (mucho lo es), pero tener una base resiliente es la verdadera clave. Eso incluye tener un equipo bien educado y bien preparado armado con las herramientas adecuadas para entrar en acción en el calor del momento. Cuando tiene órdenes de marcha claras, un plan de recuperación completamente priorizado y una línea de visión para el equipo de recuperación y datos resilientes, es menos probable que esté luchando.

Lea el informe: Lograr la resiliencia cibernética requiere trabajo en equipo

Necesita un equipo dinámico

La seguridad cibernética es un deporte de equipo que requiere conocimiento, coordinación y preparación multidisciplinaria. El comodín más grande para cualquier organización que responda a un incidente son las personas. ¿Conocen sus funciones? ¿Están listos para intervenir y desempeñarse?

“En el calor de la batalla, surgen diferentes personalidades y las cosas que ensayó tienden a ser probadas”, dijo uno de los CISO en el reciente panel de discusión de Pure Storage. Es por eso que es esencial contar con un equipo de respuesta a emergencias bien preparado y listo para actuar cuando el tiempo sea esencial. Eso podría incluir:

- **Expertos forenses digitales.** Este grupo recopilará y analizará evidencia de las máquinas afectadas, así como registros de seguridad y otras herramientas, siguiendo procedimientos detallados para mantener la integridad de sus hallazgos y garantizar su idoneidad como evidencia. Esto incluye reconstruir los eventos que llevaron a un evento utilizando datos de registro de seguridad, recuperar datos perdidos de dispositivos físicos y virtuales, recopilar y analizar evidencia de incidentes, garantizar una cadena de custodia comprobable de evidencia digital, colaborar y colaborar con las fuerzas del orden público, y proporcionar testimonio en procedimientos legales.
- **Asesor legal.** Las águilas legales lo ayudan a comprender las obligaciones, los posibles conflictos y las responsabilidades asociadas con

un evento. Pueden asesorar sobre cómo comunicarse con las fuerzas de seguridad, las agencias de investigación y las partes interesadas. También pueden proporcionar información valiosa al redactar políticas y procedimientos.

- **Seguridad de la información (InfoSec).** InfoSec es un subconjunto de ciberseguridad específicamente relacionado con la seguridad de datos. El equipo de InfoSec coordina la investigación, la evaluación, el seguimiento, la resolución y el informe de incidentes de seguridad críticos. También serán las personas que promulguen el protocolo de violación de seguridad y determinen si es necesario informar un incidente de seguridad.
- **Tecnología de la información.** No es sorprendente que el equipo de TI participe activamente en todas las fases de la respuesta ante emergencias. Esto incluye el mapeo de todos los activos y puntos finales de TI y red, la identificación y evaluación de incidentes, las medidas de contención para minimizar el daño, la erradicación o la eliminación de la amenaza, la restauración de los sistemas a su estado anterior y el análisis posterior al evento para mejorar la seguridad futura y los esfuerzos de respuesta a incidentes.
- **Relaciones con los medios y comunicaciones corporativas.** Una organización debe poder comunicar una cuenta consistente y precisa durante y después del evento de seguridad. Un punto de contacto predeterminado puede controlar y coordinar la comunicación, incluidas las comunicaciones internas, y administrar la comunicación con medios de comunicación, entidades comerciales afiliadas y partes interesadas externas.
- **Relaciones con los inversores.** Designar a una sola persona o equipo para que se comunique con socios e inversores valiosos en caso de un incidente de seguridad ayuda a garantizar que reciban comunicaciones ordenadas y puedan evaluar los impactos financieros del incidente.
- **Gerente de incidentes.** El gerente de incidentes ocupa un puesto en la parte superior de la jerarquía de ERT. Su trabajo es coordinar todas las acciones del ERT, garantizar que cada miembro del equipo lleve a cabo sus

acciones, resumir los hallazgos, escalar los problemas a la gerencia superior y, cuando sea necesario, asignar roles ad hoc.

- **Otros miembros importantes del equipo.** Según sea necesario, el equipo puede incluir proveedores de seguros cibernéticos y organizaciones de cumplimiento de la ley locales o nacionales.

La tecnología que necesita

Después de una violación o ataque de seguridad, los recursos informáticos podrían cerrarse y los recursos comprometidos podrían confiscarse, ponerse en cuarentena o ser necesarios para que los investigadores los usen. Un entorno de recuperación por etapas, configurado y probado con anticipación, proporciona un entorno de TI seguro y limpio para ayudar a que los sistemas críticos vuelvan a estar en línea lo antes posible.

- **Instantáneas inmutables.** Apodadas “bolsas de aire para el almacenamiento de datos”, las snapshots inmutables protegen los datos de la modificación y eliminación no autorizadas en función de las políticas de retención de datos existentes. Después de la intrusión y el reconocimiento iniciales, el ransomware intentará ejecutar, encriptar y/o exfiltrar datos. Sin las snapshots, y si un ataque de ransomware encripta los datos de copia de seguridad o los metadatos de copia de seguridad, sus posibilidades de recuperación de datos son reducidas, lo que lo deja vulnerable a las demandas de rescate.
- **Un SLA de recuperación cibernética que envía matrices limpias para su recuperación.**
- **Arquitectura de resiliencia por niveles con “bunkers” de datos.** Las arquitecturas de copia de seguridad por niveles se basan en la adaptación. Garantizan que los datos estén en la mejor ubicación para la recuperación en todo momento, lo que lo acerca a lograr cero objetivos de tiempo de recuperación (RTO). Las snapshots por niveles las aíslan, lo que garantiza

aún más su disponibilidad en caso de desastre.

Manténgase resiliente ante eventos con la plataforma Pure Storage

¿Qué sucedería si su plataforma de almacenamiento de datos pudiera hacer que los “eventos importantes” se parezcan más a los “eventos tolerables”? Si bien una matriz de Pure Storage no puede evitar un ataque, puede darle la capacidad de sobrevivir a uno y recuperarse rápidamente. Así es como.

Las snapshots de Pure Storage® SafeMode™ son las únicas snapshots en la industria con esta ventaja. Las snapshots SafeMode son lo que llamo “superinmutable+”. Al igual que las snapshots tradicionales e inmutables, una vez almacenadas, los datos contenidos en el interior no se pueden cambiar, editar ni sobrescribir. Sin embargo, existe una gran ventaja para las snapshots SafeMode de Pure Storage: Tampoco se pueden eliminar, ni siquiera por un usuario o proceso con privilegios administrativos en la matriz de Pure Storage.

Para los suscriptores de Evergreen//One™, nuestra suscripción de almacenamiento como servicio de nivel empresarial, el SLA de recuperación cibernética y adaptación ofrece un servicio complementario único para mitigar el riesgo, lo que garantiza:

- Envío al siguiente día hábil de arreglo(s) de recuperación limpia*
- 48 horas para finalizar un plan de recuperación
- Tasa de transferencia de datos de 8 TiB/hora
- Servicios combinados, incluido un equipo de ingeniería de servicios técnicos para finalizar el plan de recuperación y un ingeniero de servicios profesionales en el lugar desde el momento de la llegada de la matriz hasta el reemplazo de la infraestructura de servicio afectada.
- Informes trimestrales de resiliencia cibernética, preparados por Pure

Storage y revisados con usted directamente

- Servicios de corrección proporcionados por los arquitectos de seguridad de Pure Storage si desea abordar las vulnerabilidades identificadas en el informe.

La resiliencia cibernética comienza con una sólida seguridad de datos y colaboración entre equipos. Descargue el nuevo informe de Pure Storage y 451 Research sobre cómo mejorar las relaciones entre las operaciones de TI y las cohortes de seguridad.

Cronograma de envío: Envío de arreglos al siguiente día hábil a América del Norte y EMEA. Tres días hábiles a Asia y Australia/Nueva Zelanda. El envío acelerado puede estar disponible según la región.