Defensa Contra Ransomware

Una guía de recursos del PCI Security Standards Council

EL RANSOMWARE ES LA AMENAZA DE MALWARE QUE ESTÁ CRECIENDO MÁS RÁPIDAMENTE.

El ransomware es un tipo de malware que roba o impide el acceso a los archivos, sistemas o redes de las computadoras de un negocio y exigen una recompensa por devolverlos. Los ataques que provienen de ransomware pueden ocasionar interrupciones costosas a las operaciones y la pérdida o exposición de información crítica y datos.[1]

1 Fuente: FBI

ENTENDIENDO EL RIESGO

Se espera que los costos totales del ransomware alcancen **20 mil millones de dólares** en 2021, de acuerdo con el último reporte de Cybersecurity Ventures.[2]

El costo total promedio de la recuperación de un ataque de ransomware se a duplicado y más, pasando de $761.106 en 2020 a **1,85 millones de dólares** en 2021.[3]

Toma en promedio **287 días** para que una compañía se recupere totalmente de un ataque de ransomware, de acuerdo con más de 60 expertos de la industria, gobierno, organizaciones sin fines de lucro y académicos conocidos como Equipo de trabajo de Ransomware.[4]

2: Fuente: Cybersecurity Ventures Report (Informe de Ciberseguridad Empresarial) 3: Fuente: Sophos State of Ransomware Report 2021 (Informe del estado del Ransomware de Sophos 2021) 4: Fuente: Ransomware Task Force (Equipo de trabajo del Ransomware)

EL ATAQUE

Phishing es la "acción" más relevante vista en las brechas de seguridad el año pasado y **43%** de las brechas de seguridad involucraban el phishing y / o el pretexto.[5]

CORREOS DE PHISHING

El phishing en los correos electrónicos constituye un medio común para transportar programas maliciosos. Estos correos parecen legítimos, como una factura o un fax electrónico, pero incluyen enlaces maliciosos y / o adjuntos que pueden infectar el sistema de su computadora.[5]

50% de las vulnerabilidades de aplicación se consideran de riesgo alto o crítico.[6]

VULNERABILIDADES DEL SITIO WEB Y DEL SOFTWARE

Los delincuentes implantan ransomware en sitios web y se aprovechan de las vulnerabilidades del software para atacar a los visitantes usando software obsoleto (navegador, plugin del navegador).

5: Fuente: Informe de Deloitte Cyber Intelligence Centre (Centro de Ciberinteligencia Deloitte) 6: Fuente: Vulnerability Statistics Report 2021 (Informe Estadístico de Vulnerabilidades 2021)

PCI Security Standards Council

PROTEJA SU NEGOCIO

ESTÉ PENDIENTE

Entrene a sus empleados. PCI DSS 12.6

- Desarrolle un plan que eduque a sus empleados en las mejores formas de evitar estos tipos de ataques y cómo reconocer y responder ante ellos si ocurren.
- Asegúrese de que ellos saben de los riesgos y que entienden que está bien borrar un correo electrónico si parece sospechoso.
- Piense antes de hacer clic. Los correos pueden parecer que vienen de cualquier persona de la empresa. Si tiene dudas, siempre contacte a esa persona para confirmar antes de hacer clic en un enlace o abrir un archivo.

MANTÉNGASE VIGILANDO

Pruebe sus sistemas. PCI DSS 11.3

- ¿Ha probado sus sistemas últimamente para ver si es fácil para alguien entrar en él? Los delincuentes son persistentes, usted también debería serlo.
- Una vulnerabilidad les proporciona una puerta "abierta" a los delincuentes para que puedan simplemente entrar. Es importante que cualquier vulnerabilidad encontrada durante la prueba sea reparada y que usted tenga otros controles establecidos para prevenir que un individuo malicioso entre en sus sistemas.

Aplicar parches a las actualizaciones. PCI DSS 6.2

- Sus vendedores le envían "actualizaciones" para arreglar los problemas en sus sistemas de pago o otros sistemas.
- ¿Cuándo fue la última vez que usted chequeó las nuevas actualizaciones de seguridad de sus vendedores del sistema de pagos y software?
- Las actualizaciones cierran las puertas que los delincuentes usan para entrar en sus sistemas. Siga las instrucciones de sus vendedores e instale actualizaciones tan pronto como sea posible.

Monitore actividad sospechosa. PCI DSS 11.5

- ¿Está monitoreando sus sistemas para ver si ha habido algún cambio? ¿Se han investigado los cambios sospechosos o no autorizados?
- Monitorear los cambios de sus sistemas le ayuda a ver cuándo alguien hace un cambio que usted no autorizó o aprobó. Investigar los cambios tan pronto como pasen le ayuda a encontrar los problemas más rápidamente y mejora sus posibilidades de acabar con el ataque.
- Un proceso de manejo de cambio le ayudará a determinar si los cambios han sido aprobados. Si el cambio no ha sido aprobado o es desconocido, usted debería investigar inmediatamente para determinar si su sistema se ha visto comprometido.

Tenga un respaldo de sus sistemas. PCI DSS 9.5.1, 12.10.1

- Cuide que su respaldo no sobrescriba los respaldos anteriores que sean buenos. Esto puede ayudar a prevenir el guardar la información encriptada por un ransomware y sobrepasar un buen respaldo. Las buenas prácticas, aun cuando tenga un método de respaldo, se trata de mantener respaldos de discos completos y respaldos incrementales (que tan solo respaldan la información que es nueva desde el último respaldo).
- Para reducir su riesgo, evite mantener información de respaldo en línea (conectado a los sistemas que están siendo respaldados). En vez de guardar su información de respaldo fuera de la sede y fuera de línea (guardar sus respaldos «en la nube» es un método común de almacenamiento fuera de línea; sin embargo, vea la última viñeta). Esto hace que sea más fácil recuperar su respaldo más reciente si sus archivos de información están siendo víctimas de cobro de recompensa.
- Mantenga múltiples generaciones de respaldo y tenga un periodo de retención consistentes con la habilidad de su organización de detectar el ransomware y su habilidad de reconstruirlo usando registros más viejos.
- ¿Usted ha probado la integridad de sus respaldos recientemente? ¿Usted ha probado sus procesos de recuperación y respaldo recientemente? Asegurarse de que usted pueda recuperar la información de su respaldo es crucial en el evento de que sus sistemas los bloquee el ransomware.
- Cuando use respaldos en la nube, asegúrese de que su proveedor del servicio de la nube está siendo diligente y que lo está protegiendo contra cualquier tipo de malware. El almacenamiento en la nube también puede bloquearlo el atacante si está conectado a los sistemas de respaldo haciendo una sincronización persistente.

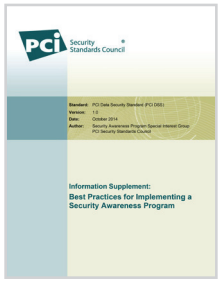
HAGA UN PLAN

Esté preparado. PCI DSS 12.10

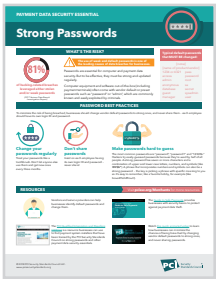
- Usted y sus empleados deberían saber cómo responder a un ataque y qué hacer cuando esto ocurre, incluyendo a quien contactar.
- Asegúrese de tener un plan establecido y comunicárselo a sus empleados.
- Repase este plan regularmente y haga un compromiso continuo de educar a su personal.

MATERIALES DE APOIO DETALLADO DE PCI

pdf PCI Data Security Standard Versión 3.2.1

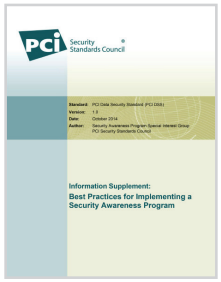


pdf Suplemento de Información: Monitoreo de registros diario efectivo



pdf La seguridad de los datos de pago es esencial: Contraseñas Seguras

pdf La seguridad de los datos de pago es esencial: Parcheado



pdf Las mejores prácticas para implementar un programa de conciencia de seguridad

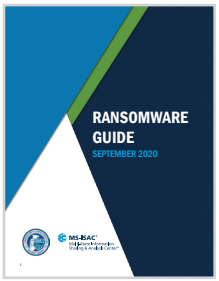
pdf Recursos de protección de pagos para los pequeños comerciantes: Guía de pagos seguros

RECURSOS RELACIONADOS DE LA INDUSTRIA

pdf No sea la próxima victima del ransomware. Ayude a proteger a su organización con estas mejores prácticas

pdf Ransomware: Qué es y qué hacer al respecto

www Proyecto No More Ransom



pdf Guía del Ransomware CISA MS-ISAC

Para obtener un comentario de un experto o hacer preguntas, por favor, contacte: press@pcisecuritystandards.org
Para obtener más información de los estándares PCI y de los recursos, por favor, visite: www.pcisecuritystandards.org.