Guía para líderes de TI sobre protección de datos ante el nuevo panorama de amenazas

Estrategias para establecer una última línea de defensa para mejorar la resiliencia del negocio y resistir a los impactos del ransomware

Insight

El auge de la ciberdelincuencia

A medida que el mundo continúa recuperándose tras muchos meses de acontecimientos que alteraron nuestras vidas, la ciberdelincuencia se ha vuelto más lucrativa que nunca.

¿Cuál es la táctica más utilizada? El ransomware. La actividad semanal media del ransomware se ha multiplicado por diez en el último año. Más de un tercio de las organizaciones sufrieron ataques de ransomware en 2020.[1]

El ransomware, no solo es más frecuente, sino que se está volviendo cada vez más sofisticado y preciso. la mayoría de las organizaciones afectadas por el ransomware el año pasado (un 54 %) declaró que los ciberdelincuentes lograron cifrar sus datos. Sin embargo, de media, solo el 65 % de los datos cifrados lograron restablecerse después de pagar el rescate. [1]

Este escenario de pérdida es particularmente preocupante, dado que el montante medio del rescate pagado por las organizaciones de tamaño mediano fue de 170.404$. Es más, el coste medio de rectificar un ataque de ransomware, teniendo en cuenta factores como el tiempo de inactividad y la dotación de personal, el rescate pagado y los costes en dispositivos, redes y oportunidades, fue de 1,85 millones.[1]

En 2020, se pagaron **350 millones de USD** en ataques de ransomware.[2]

Las empresas pequeñas representan aproximadamente **la mitad o las tres cuartas partes de las víctimas del ransomware**.[2]

El Departamento de Justicia de los Estados Unidos ha **elevado la prioridad de las investigaciones sobre los ataques de ransomware a una nivel similar al del terrorismo**.[3]

En busca de la seguridad

Para mitigar el riesgo, existen actualmente múltiples marcos de seguridad - algunos voluntarios, otros obligatorios por ley - con los que las organizaciones pueden alinearse. Existen estándares de cumplimiento normativo, como la Ley de responsabilidad y transferibilidad de seguros médicos (HIPAA) y el Reglamento general de protección de datos (RGPD), para ayudar a las organizaciones a determinar la mejor manera de proteger sus datos, gestionar el riesgo y cuidar los datos confidenciales.

Como parte de la estrategia de ciberseguridad de la UE, la Comisión Europea propuso la Directiva de la UE sobre seguridad de la información y redes (Directiva NIS). Adoptada en 2016, es la primera parte de la legislación sobre ciberseguridad en toda la UE, y los estados miembro de la UE han empezado a adoptar legislaciones nacionales que siguen o "incorporan" la directiva.

Las empresas pueden acabar adoptando múltiples marcos de seguridad, por elección o por necesidad, para crear un programa de seguridad capaz de hacer frente a la actividad de los ciberdelincuentes actuales. Pero, en conclusión, no existen garantías. Que su organización experimente o no un ciberataque, ya no es una cuestión de "si sucede", sino de "cuándo sucederá".

Por lo tanto, es esencial contar con una infraestructura sólida de protección de datos. Un entorno sólido de protección de datos ofrece un plan alternativo y mayor tranquilidad, incluso si los delincuentes se toman, cifran, eliminan o ponen en peligro sus datos.

En caso de que se convierta en víctima de un ciberataque, una protección de datos eficaz le garantiza que:

- Tiene un acceso seguro a sus datos.
- El tiempo de inactividad es mínimo.
- No tendrá que pagar por un rescate si se solicita uno.
- Las pérdidas (financieras, productividad, reputación, etc.) se minimizan.

Las organizaciones con infraestructura de protección de datos heredada deben tener en cuenta lo siguiente:
Los delincuentes se centran cada vez más en los entornos de protección de datos como estrategia ante los ciberataques, encontrando un punto de entrada y permaneciendo dentro de la organización durante varios meses para aprender sobre esos entornos, luego eliminarlos y/o comprometerlos. La modernización de su infraestructura y procesos de protección de datos puede ayudarle en gran medida a defenderse contra este tipo de ataques.

Ningún negocio está a salvo

Las organizaciones de todos los sectores han sufrido ataques devastadores de ransomware.

Instalaciones petroleras europeas

Los sistemas de TI sufrieron interrupciones en Oiltanking (Alemania) el 28 de enero de 2022, tras sufrir un ciberataque que también afectó a su cadena de suministro. La inversión en el SEA en Bélgica y Evos en los Países Bajos también se vio afectada por ataques similares.

Oiltanking es uno de los mayores partners independientes de terminales de tanques para aceites y biocombustibles en Alemania. Posee y opera una cartera de terminales con una capacidad total de almacenamiento de 2.375 millones de cbm. El rendimiento total de todas sus terminales en 2020 fue de aproximadamente 18,2 millones de toneladas.

- La empresa se vio obligada a operar a una capacidad limitada mientras investigaba el incidente.
- Un total de 13 terminales de distribución en toda Alemania fueron afectadas. Shell desvió sus operaciones a proveedores alternativos para minimizar el impacto en sus propios suministros.
- Se cree que todas las empresas se vieron afectadas porque utilizan el mismo software para las operaciones que pueden haberse visto comprometidas por los hackers.[4]

Salud pública y asistencia social

El 14 de mayo de 2021, el Departamento de Salud y Servicios Sanitarios de Irlanda se vio afectado por un ataque de ransomware "Conti" operado por humanos.

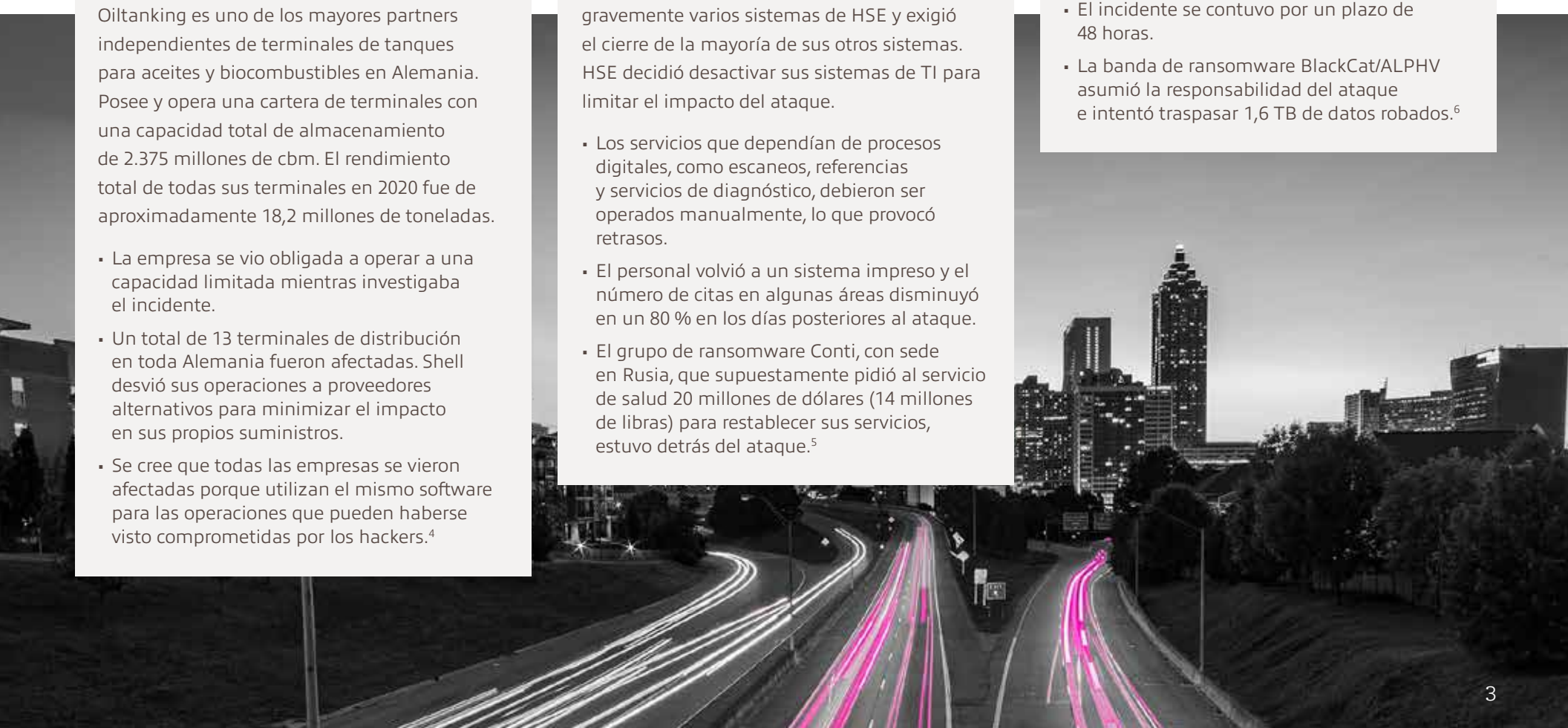
Se detectó actividad cibernética maliciosa en la red del Departamento de Salud que desactivó gravemente varios sistemas de HSE y exigió el cierre de la mayoría de sus otros sistemas. HSE decidió desactivar sus sistemas de TI para limitar el impacto del ataque.

- Los servicios que dependían de procesos digitales, como escaneos, referencias y servicios de diagnóstico, debieron ser operados manualmente, lo que provocó retrasos.
- El personal volvió a un sistema impreso y el número de citas en algunas áreas disminuyó en un 80 % en los días posteriores al ataque.
- El grupo de ransomware Conti, con sede en Rusia, que supuestamente pidió al servicio de salud 20 millones de dólares (14 millones de libras) para restablecer sus servicios, estuvo detrás del ataque.[5]

Empresa suiza de servicios de aviación

La empresa de servicios de aviación, Swissport, fue víctima de un ataque de ransomware el 4 de febrero de 2022, con algunos vuelos forzados a retrasos y otras operaciones interrumpidas.

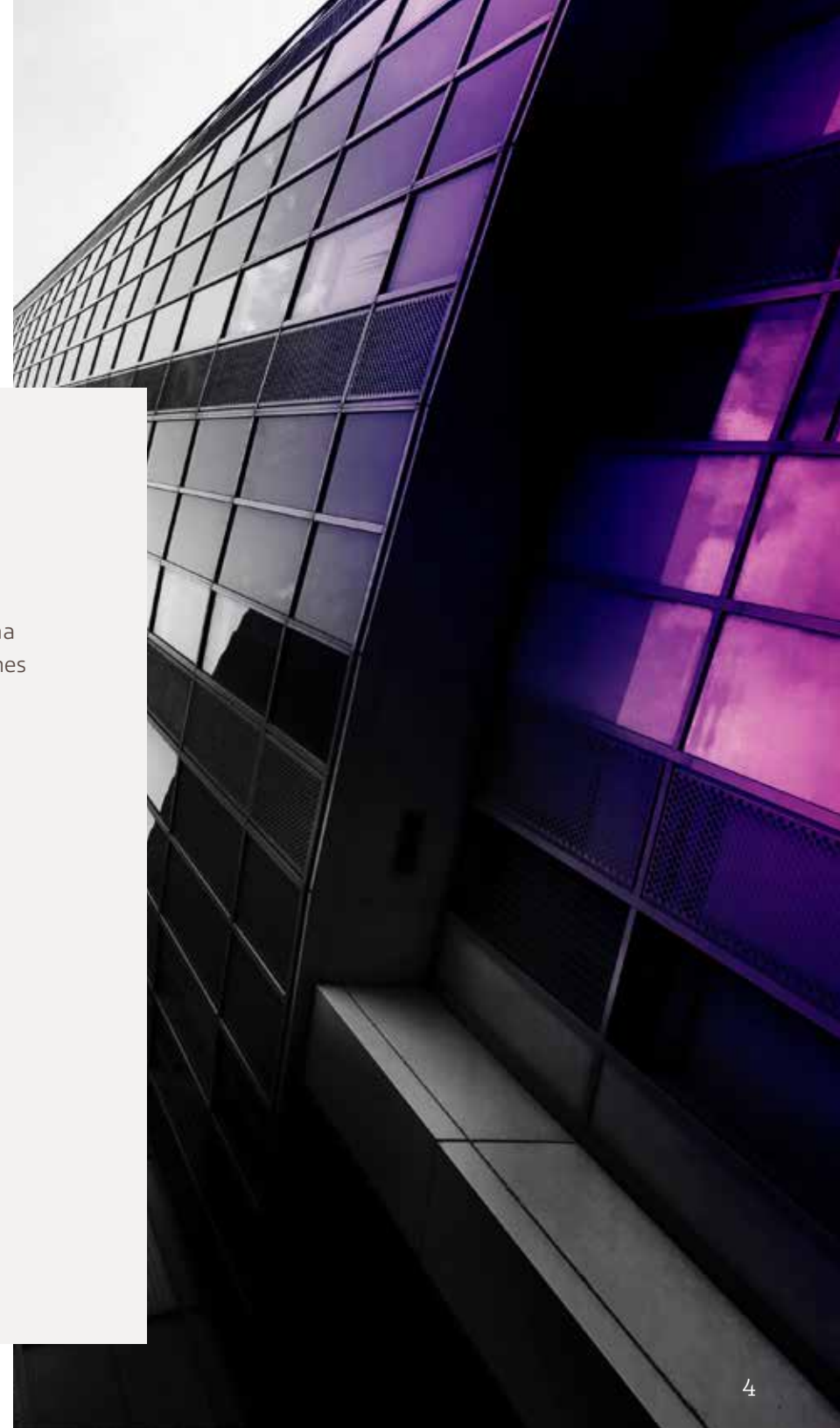
- Un pequeño número de vuelos se retrasó de 3 a 20 minutos.
- El incidente se contuvo por un plazo de 48 horas.
- La banda de ransomware BlackCat/ALPHV asumió la responsabilidad del ataque e intentó traspasar 1,6 TB de datos robados.[6]



Pasos erróneos y oportunidades perdidas

El problema del ransomware tiene muchas facetas, y parte del problema es la integridad de la infraestructura de protección de datos.

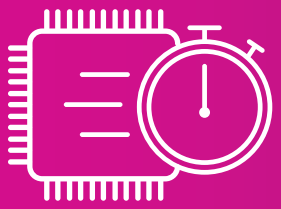
Las organizaciones deben reevaluar cómo se almacenan, protegen y realizan copias de seguridad de los datos en todos los entornos. Hay un puñado de trampas comunes que los líderes de TI pueden conocer y contra las que pueden trabajar para evitarlas.



1 Falta de pruebas exhaustivas

Cuando un delincuente se infiltra en un sistema y se produce un evento de ransomware, el tiempo lo es todo: ¿cuánto tardará la organización en volver a estar operativa?

Sin un compromiso con las pruebas, no se puede saber cuánto tiempo tardará una empresa en recuperarse, porque ese escenario no se ha validado. Las restauraciones de prueba se suelen realizar en partes más pequeñas de un entorno, como la restauración de un archivo, aplicación o parte de una red. Lo que no se ve mucho hoy en día es probar planes completos de respuesta al ransomware.



De vuelta en un instante

Si pregunta a cualquier experto informático en el ámbito de la seguridad y la protección de datos, le dirá que vale la pena tener en cuenta el almacenamiento flash. Flash proporciona tiempos de SLA (Nivel de servicios acordado) muy bajos, lo que le ayuda a volver a poner los sistemas en marcha rápidamente.

2 Falta de comprensión de los parques de datos

Los entornos de TI actuales son un panorama cada vez más amplio de plataformas y sistemas. La infraestructura heredada se combina con nuevas arquitecturas y formas de funcionamiento. Las nuevas tecnologías y la Inteligencia Artificial (IA), el aprendizaje automático y las cargas de trabajo de informática perimetral producen actualmente cantidades masivas de datos. Los datos están por todas partes, los silos son cada vez más numerosos y la complejidad es casi inevitable.

Los desafortunados resultados de esta situación, entre otros, son una visibilidad mínima y una seguridad deficiente, y las organizaciones que no saben qué datos tienen, dónde residen y cómo protegerlos y gestionarlos de manera eficaz.

Los retos principales de la gestión de datos:

- Crecimiento de datos (67 %)
- Falta de visibilidad (60 %)
- Complejidad de la cloud híbrida (60 %)

Retos de los datos:

- Protección de datos (53 %)
- Requisitos de cumplimiento normativo, de soberanía y privacidad de datos (47 %)
- Integridad de datos (46 %)[7]

3 Un enfoque aislado de las herramientas

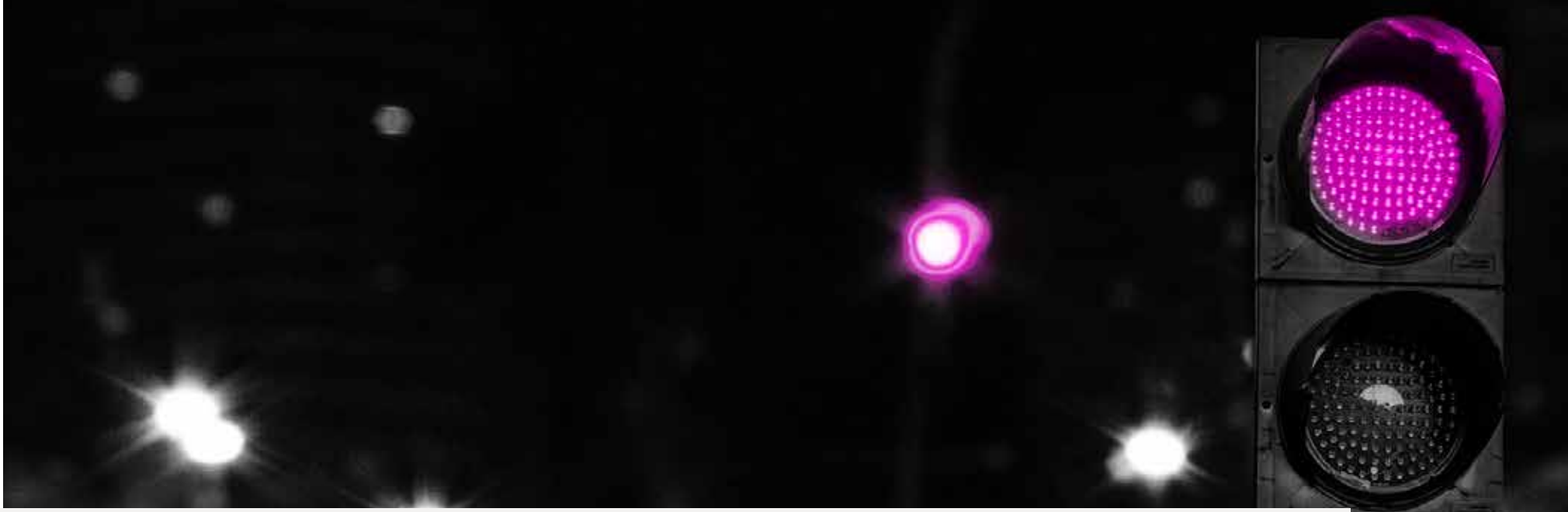
Muchos productos afirman poder detener el ransomware por sí solos. Esto no es posible. No hay una solución puntual que aborde todos los aspectos de la prevención y respuesta al ransomware.

La única forma de garantizar la preparación ante un ataque es desarrollar y ejecutar una estrategia que abarque la prevención de riesgos (controles de seguridad, firewalls, educación del usuario final, etc.) y minimización de riesgos (una infraestructura moderna de protección de datos).

4 Mentalidad de restauración única

Es relativamente fácil probar y habilitar restauraciones de un solo archivo o de una sola aplicación, pero hoy en día esto no es suficiente. Los ataques de ransomware no se dirigen a equipos individuales, sino que afectan a entornos informáticos completos y a las empresas a las que pertenecen.

Las organizaciones deben estar preparadas y ser capaces de restaurar entornos completos en un plazo razonable. No pensar en la recuperación segura a escala pone a la empresa en riesgo de sufrir daños adicionales significativos cuando se produce un ataque.



Protección de datos: Panorama general

La prevalencia de ciberataques como el ransomware ha dado lugar a un enfoque renovado en la prevención del ransomware, copia de seguridad y recuperación. Tenga en cuenta que: La mejor estrategia de protección de datos es una estrategia multicapa. Asegúrese siempre de seguir las mejores prácticas en las siguientes áreas:

- Gestión del ciclo de vida del software
- Gestión de datos
- Gestión de almacenamiento de datos
- Cumplimiento normativo y de estándares
- Seguridad de datos
- Control de gestión del acceso a los datos
- Pruebas, ejecución e informes
- Mejora continua

Factores de éxito

Los ataques de ransomware generalmente no tienen finales felices, pero hay varios aspectos clave en las organizaciones modernas que están mejorando con éxito sus posibilidades de minimizar los daños y el impacto de un ataque.

01. Un cambio en la mentalidad de los equipos de seguridad

Los equipos de seguridad desempeñan un papel fundamental en la defensa de una organización contra los ciberataques, pero los enfoques programáticos se han vuelto críticos. Es probable que las organizaciones que son capaces de romper los silos e impulsar esfuerzos interdisciplinarios entre los equipos de seguridad e infraestructura/operaciones desarrollen estrategias de protección de datos más sólidas, mejoren la posición general en materia de seguridad y obtengan mejores resultados de negocio.

02. Cinta para copias de seguridad aisladas

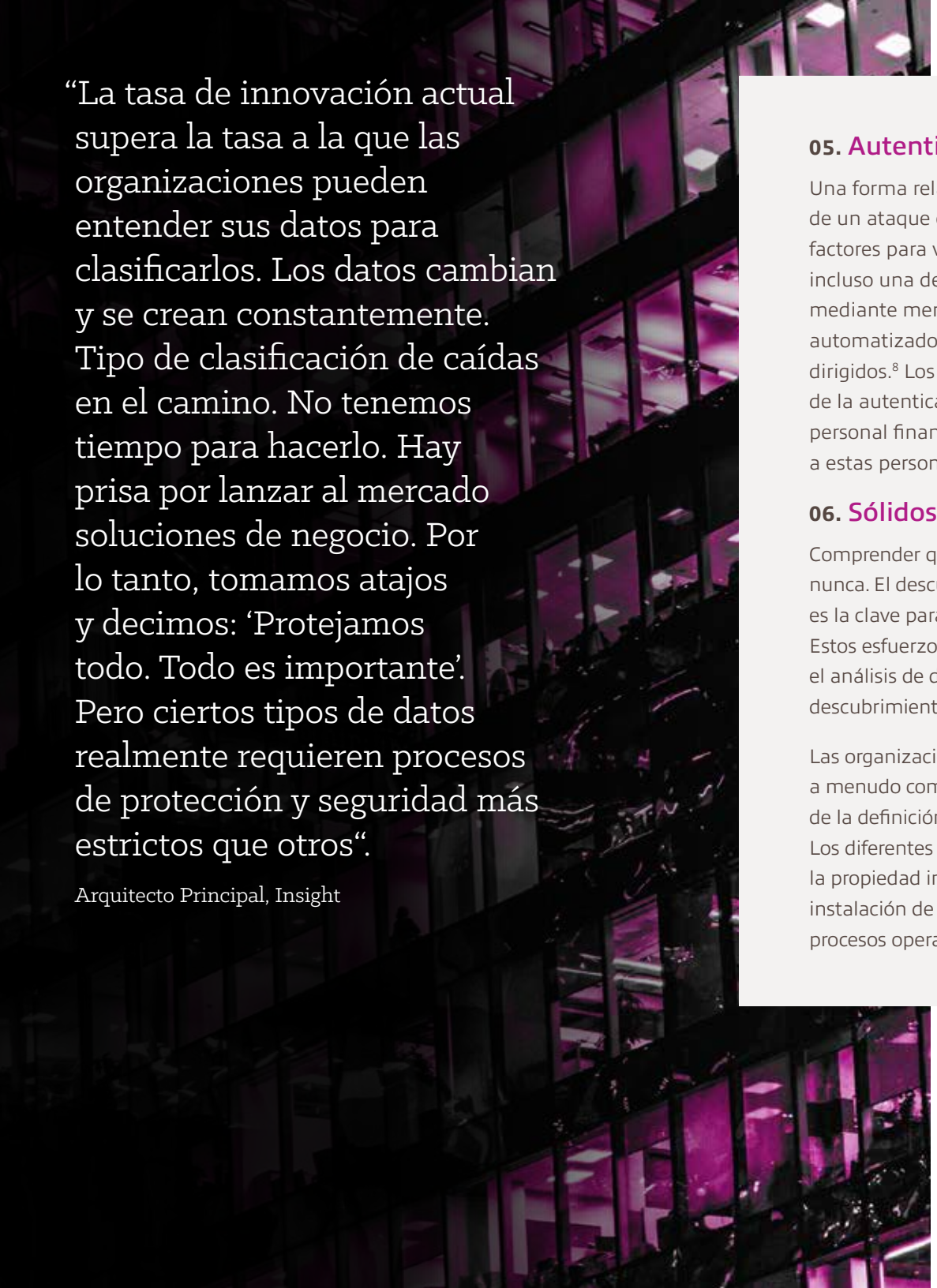
Hay muchas formas de hacer una copia de seguridad de los datos. Pero la cinta está volviendo debido a su capacidad de proporcionar un espacio vacío, una copia completamente fuera de línea e inaccesible de los datos sensibles. Las organizaciones pueden escribir la copia, manipular físicamente la cinta y enviarla a una instalación de almacenamiento seguro donde no nadie la toque hasta que se vuelva necesitar. La capacidad, el rendimiento, la durabilidad, el coste y la mayor compatibilidad de la cinta son otras cualidades que la hacen atractiva.

03. Todo-Flash

El almacenamiento flash es otra opción de almacenamiento de copias de seguridad que ayuda a las organizaciones a reducir el punto de recuperación y los objetivos de tiempo de recuperación. Puede ofrecer una replicación rápida o sincronizada y una conmutación por error automática, así como integrarse fácilmente en entornos cloud y de cloud híbrida.

04. Almacenamiento inmutable

Históricamente, el almacenamiento inmutable era una ventaja. Sin embargo, muchas soluciones modernas de protección de datos se basan ahora en la idea de que el almacenamiento inmutable es esencial. La inmutabilidad permite a las organizaciones tomar una instantánea de sus datos y establecer políticas sobre su caducidad, sabiendo que los datos no se verán afectados y serán completamente restaurables hasta ese momento, independientemente de cualquier violación involuntaria (error del usuario final) o intencionada (ciberataque) del entorno.



"La tasa de innovación actual supera la tasa a la que las organizaciones pueden entender sus datos para clasificarlos. Los datos cambian y se crean constantemente. Tipo de clasificación de caídas en el camino. No tenemos tiempo para hacerlo. Hay prisa por lanzar al mercado soluciones de negocio. Por lo tanto, tomamos atajos y decimos: 'Protejamos todo. Todo es importante'. Pero ciertos tipos de datos realmente requieren procesos de protección y seguridad más estrictos que otros".

Arquitecto Principal, Insight

05. Autenticación de dos factores

Una forma relativamente sencilla de que las organizaciones puedan mitigar el riesgo de un ataque es mediante la implementación de la autenticación de dos o varios factores para validar a los usuarios antes de conceder acceso a los datos. De hecho, incluso una de las formas más débiles de autenticación de dos factores (la verificación mediante mensajes de texto SMS) puede detener el 100 % de todos los ataques automatizados, el 96 % de los ataques de phishing masivo y el 76 % de los ataques dirigidos.[8] Los expertos sugieren utilizar claves de seguridad de hardware como parte de la autenticación de dos factores para los usuarios con privilegios (ejecutivos sénior, personal financiero y de RR. HH., etc.), ya que muchos delincuentes se dirigirán a estas personas con mucho esfuerzo. [9]

06. Sólidos procesos de descubrimiento y clasificación de datos

Comprender qué datos se almacenan y dónde se han vuelto más importantes que nunca. El descubrimiento y la clasificación de datos, que se realizan regularmente, es la clave para una protección y un almacenamiento de datos altamente eficaces. Estos esfuerzos también pueden simplificar el trabajo con los auditores y mejorar el análisis de datos. Sin embargo, muchas organizaciones pueden evitar el descubrimiento y la clasificación porque es una tarea considerable.

Las organizaciones que tienen éxito con el descubrimiento y la clasificación de datos a menudo comienzan con un ejercicio completo de descubrimiento de datos, seguido de la definición de categorías de datos de alto nivel (sensibles, críticas, reguladas, etc.). Los diferentes tipos de datos deben recibir un tratamiento diferente, por ejemplo, la propiedad intelectual de una empresa puede almacenarse fuera de línea en una instalación de cintas de alta seguridad, mientras que los documentos de Word de los procesos operativos de RR. HH. pueden almacenarse en la cloud.

07. Restauraciones de prueba a escala

Las organizaciones proactivas y seguras han hecho que la continuidad del negocio y la recuperación ante desastres sean prioridades principales. Hoy en día, esto significa realizar restauraciones de prueba a escala, en las que se restaura todo el entorno, a diferencia de archivos individuales, aplicaciones o máquinas.

Para conseguir restauraciones rápidas y completas, los escenarios de prueba deben proceder con la premisa de que el centro de datos primario ha sido cifrado, como es el caso de un ataque de ransomware. Los datos deben replicarse en un centro de datos secundario, la última línea de defensa para volver a poner en línea un entorno.

Es útil hacer las siguientes preguntas a su empresa:

- ¿Tenemos la capacidad de restaurar completamente nuestro entorno?
- ¿Cuál es nuestro proceso para restauraciones a gran escala?
- ¿Cuánto tiempo tardaríamos en restaurar por completo nuestro entorno?
- ¿Cuánto tiempo puede sobrevivir el negocio mientras logramos restaurar el entorno?

08. Esfuerzos continuos para la protección de datos

Los cambios en un entorno informático, en los datos empresariales y en todo el entorno externo deberían provocar cambios en la estrategia de protección de datos de una organización.

Desarrollar una plataforma de protección de datos sólida no es una actividad única, sino un compromiso continuo con las prácticas clave. Algunos ejemplos son:

- Descubrimiento y clasificación regular de datos
- Formación del usuario final para la concienciación sobre la seguridad
- Ensayos de metodología
- Modernización de infraestructuras
- Revisiones y actualizaciones del objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO)

Pensar más allá del ransomware

El ransomware y otras actividades de los ciberdelincuentes no son las únicas amenazas para los datos corporativos. Es importante considerar otras formas en que los datos pueden ser mal utilizados, corrompidos o perdidos al planificar una actualización o modernización de infraestructura y procesos de protección de datos.

Por ejemplo:

- Migraciones o consolidaciones de centros de datos y cloud, realizadas con una planificación mínima y/o sin la ayuda de expertos
- Acceso de usuario no autorizado, intencionado o no intencionado (las redes modernas también deben ser una prioridad principal).
- Configuraciones mal gestionadas

Cómo trazar un camino a seguir

Si existe alguna verdad sobre la protección de datos, es que no existe un mejor y único protocolo de acción.

La estrategia y la infraestructura de protección de datos óptimas serán únicas para su organización y sus necesidades, riesgos y objetivos específicos. Solo se deberán considerar sus muchas opciones para proteger los datos y mitigar el riesgo siempre presente de ransomware.

Si su organización desea apoyo externo, Insight está aquí para ayudarle. Nuestro equipo cuenta con una amplia experiencia en protección de datos, almacenamiento, gestión de datos y seguridad en todo el marco de ciberseguridad NIST. Los clientes aprecian lo que podemos ofrecer:

Más de 25 años
de experiencia en centros de datos

14 años
de pruebas de penetración, evaluación de vulnerabilidades y gestión de seguridad

16 años
de experiencia en gestión de incidentes y amenazas

Póngase en contacto con Insight para hablar sobre sus necesidades de ciberseguridad y protección de datos, y explore todas las formas en que podemos ayudarle a reforzar su estrategia. Contacte con nuestro equipo.

Acerca de Insight

Hoy, toda empresa es una empresa tecnológica. Insight Enterprises Inc. provee a organizaciones de todos los tamaños de Intelligent Technology Solutions™ y servicios para maximizar el valor de negocio de sus TI. Como proveedor global de soluciones y servicios de Digital Innovation, Cloud + Data Centre Transformation, Connected Workforce, y soluciones y servicios de Supply Chain Optimisation, formando parte del ranking Fortune 500, ayudamos a nuestros clientes a gestionar con éxito sus TI hoy y a transformarlas para el futuro. Desde la estrategia y el diseño de TI hasta su implementación y gestión, nuestros 11 000 compañeros ayudan a los clientes a innovar y a optimizar sus operaciones para dirigir su empresa de forma más inteligente.

Descubra más en es.insight.com

Insight®

solutions.insight.com | es.insight.com

Fuentes:
1. Sophos. (abril de 2021). El estado del ransomware 2021.
2. Barr, L. (6 de mayo de 2021). El secretario de DHS advierte que los ataques de ransomware van en aumento y los objetivos incluyen a las pequeñas empresas. ABC News.
3. Bing, C. (3 de junio de 2021). Exclusivo: EE. UU. dará a los ataques de ransomware una prioridad similar a la del terrorismo. Reuters
4. Tidy, J. (3 de febrero de 2022). Instalaciones petroleras europeas afectadas por los ciberataques. BBC News.
5. Rees, D. (18 de junio de 2021). Ciberataques en el sector de la atención sanitaria: la posición en toda Europa. Pinsent Masons.
6. Scroxton, A. (16 de febrero de 2022). La banda de ransomware BlackCat reivindica el ataque a Swissport. Computer Weekly.
7. IDG. (2021). Data Innovators Guide: Llevando los datos al siguiente nivel. Patrocinado por Hewlett Packard Enterprise.
8. Moscicki, A. y Thomas, K. (17 de mayo de 2019). Nueva investigación: Qué tan efectiva es la higiene básica de la cuenta para prevenir un secuestro. Blog de seguridad de Google.
9. Lemos, R. (n.d.). El estado de la MFA: 4 tendencias que presagian el fin de la contraseña individual. TechBeacon.