Cómo una mala contraseña acabó con una empresa de 158 años

Durante 158 años, KNP se adaptó y resistió, construyendo un negocio de transporte con una flota de 500 camiones en todo el Reino Unido. Pero en junio de 2025, una contraseña fácil de adivinar bastó para acabar con la compañía en cuestión de días.

La mayoría de las empresas no llega a cumplir cinco años. Los estudios indican que aproximadamente el 50% de las pequeñas empresas fracasan antes de alcanzar su quinto aniversario. Por eso, cuando KNP Logistics Group (antiguamente Knights of Old) celebró más de siglo y medio de actividad, parecía haber dominado el arte de la supervivencia. Durante 158 años, KNP se adaptó y resistió, construyendo un negocio de transporte con una flota de 500 camiones en todo el Reino Unido. Pero en junio de 2025, una contraseña fácil de adivinar bastó para acabar con la compañía en cuestión de días.

La empresa, con sede en Northamptonshire, fue víctima del grupo de ransomware Akira después de que unos hackers accedieran al sistema al adivinar la débil contraseña de un empleado. No hizo falta una sofisticada campaña de phishing ni explotar una vulnerabilidad zero-day: solo una contraseña tan simple que los ciberdelincuentes la acertaron por pura deducción.

Cuando la seguridad básica falla, todo se viene abajo

Da igual los mecanismos de seguridad avanzada que tenga tu organización: si las medidas básicas fallan, todo se derrumba. En el ataque a KNP, Akira apuntó a los sistemas expuestos a Internet, encontró unas credenciales de empleado sin autenticación multifactor (MFA) y logró adivinar la contraseña. Una vez dentro, desplegaron la carga útil de ransomware en toda la infraestructura digital de la compañía.

Pero los atacantes no se limitaron a cifrar los datos críticos del negocio. También destruyeron las copias de seguridad y los sistemas de recuperación ante desastres, garantizando que la empresa no pudiera recuperarse sin pagar el rescate. Los criminales exigieron unos 5 millones de libras, una cantidad inasumible para la compañía de transporte.

KNP cumplía con los estándares de cumplimiento normativo en TI y contaba con un seguro frente a ciberataques, pero nada de eso bastó para mantener la organización operativa. Las operaciones se paralizaron. Cada camión quedó fuera de servicio. Todos los datos del negocio permanecieron bloqueados. El equipo de respuesta a incidentes cibernéticos, enviado por la aseguradora, lo describió como “el peor escenario posible” para cualquier organización. En cuestión de semanas, KNP entró en administración concursal y 700 empleados perdieron su trabajo.

El problema de las contraseñas persiste

La historia de KNP pone de manifiesto una debilidad que sigue afectando a organizaciones de todo el mundo. Un estudio de Kaspersky que analizó 193 millones de contraseñas comprometidas reveló que el 45% podían ser descifradas por atacantes en menos de un minuto. Y cuando los atacantes pueden simplemente adivinar o descifrar credenciales en segundos, incluso las empresas más consolidadas quedan expuestas. Un fallo individual puede tener consecuencias a nivel organizativo que van mucho más allá de quien eligió “Password123” o usó su fecha de nacimiento como contraseña.

¿Te interesa saber cuántas contraseñas débiles se están utilizando ahora mismo en tu Active Directory? Ejecuta un análisis gratuito, de solo lectura, con Specops Password Auditor: descárgalo aquí.

Más allá del daño económico

El colapso de KNP demuestra que los ataques de ransomware generan consecuencias que van mucho más allá de la pérdida económica inmediata. Setecientas familias perdieron su principal fuente de ingresos. Una empresa con casi dos siglos de historia desapareció de la noche a la mañana. Y la economía local de Northamptonshire perdió a un empleador y proveedor de servicios clave.

Para las empresas que logran sobrevivir a un ataque de ransomware, el daño reputacional suele amplificar el golpe inicial. Las organizaciones se enfrentan a un escrutinio continuo por parte de clientes, socios y reguladores que cuestionan sus prácticas de seguridad. Los stakeholders exigen responsabilidades por las brechas de datos y los fallos operativos, lo que a menudo deriva en responsabilidades legales.

La crisis de ransomware que crece en el Reino Unido

KNP se suma a las aproximadamente 19.000 empresas británicas que sufrieron ataques de ransomware el año pasado, según encuestas del gobierno. Entre las víctimas más destacadas se encuentran grandes minoristas como M&S, Co-op y Harrods, lo que demuestra que ninguna organización es demasiado grande o consolidada como para no ser objetivo.

Y cada vez lo tienen más fácil. Las bandas criminales han reducido las barreras de entrada mediante el modelo de ransomware-as-a-service y tácticas de ingeniería social que no requieren grandes conocimientos técnicos. Hoy en día, los atacantes llaman rutinariamente a los servicios de asistencia de TI para engañar al personal y acceder a los sistemas corporativos, explotando la psicología humana en lugar de las vulnerabilidades del software.

Los estudios del sector indican que la demanda media de rescate en Reino Unido ronda los 4 millones de libras, y que aproximadamente un tercio de las empresas opta por pagar antes que arriesgarse a perderlo todo. Pero pagar no garantiza la recuperación de los datos ni evita futuros ataques: solo financia operaciones criminales que acabarán afectando a otras organizaciones.

Construyendo defensas resilientes

El incidente de KNP revela que los controles de seguridad son la defensa más crítica frente al ransomware. Cuando una única credencial débil puede destruir décadas, o incluso siglos, de actividad empresarial, no puedes permitirte tratar la seguridad de las contraseñas como un asunto secundario. Para reforzar tus defensas, deberías:

Implementar políticas de contraseñas robustas: tu primera línea de defensa son las políticas de contraseñas seguras, respaldadas por detección de contraseñas comprometidas. Puedes reducir drásticamente el riesgo de ataques a credenciales bloqueando contraseñas débiles o comúnmente utilizadas, y exigiendo la creación de frases de contraseñas largas y complejas.

Para lograr el máximo nivel de protección, considera implementar una solución automatizada como Specops Password Policy. Esta herramienta analiza continuamente las credenciales de Active Directory frente a miles de millones de contraseñas filtradas conocidas, ayudando a tu organización a aplicar políticas de contraseñas seguras y evitando el uso de credenciales fácilmente adivinables como la que provocó la caída de KNP.

Activar la autenticación multifactor (MFA): incluso cuando las contraseñas se ven comprometidas, los factores de autenticación adicionales pueden impedir el acceso no autorizado a los sistemas críticos. La ausencia de MFA en los sistemas expuestos a Internet de KNP permitió a los atacantes entrar como si la puerta estuviera abierta, una vez que adivinaron las credenciales iniciales.

Para aumentar tu nivel de seguridad, añade una segunda capa de protección con una solución de autenticación multifactor como Specops Secure Access. Además de reforzar la protección frente a ataques de contraseñas, Secure Access puede ayudarte a cumplir con los requisitos normativos y de los seguros de ciberseguridad.

Implementar una arquitectura zero trust y controles de mínimo privilegio: más allá de las contraseñas y la autenticación, necesitas limitar lo que los atacantes pueden hacer si logran acceder a tu red. Las arquitecturas zero trust asumen que la red ya está comprometida y verifican cada solicitud de acceso, sin importar la ubicación del usuario ni su autenticación previa. Los controles de acceso de mínimo privilegio complementan este enfoque, reduciendo el movimiento lateral dentro de la red y garantizando que una única cuenta comprometida no pueda desbloquear todos los recursos de la organización.

Probar regularmente las copias de seguridad y los planes de recuperación: tu organización debe asegurarse de que las copias de seguridad estén aisladas de la red principal y de que los procedimientos de restauración se prueben con regularidad. Cuando el ransomware golpea, disponer de backups funcionales puede marcar la diferencia entre sobrevivir o seguir el camino de KNP hacia la liquidación.

Si la idea de que una contraseña adivinada haya destruido una empresa de 158 años te deja un mal cuerpo, debería hacerlo: los fallos de ciberseguridad tienen consecuencias reales. Invertir hoy en controles de seguridad cuesta mucho menos que reconstruir un negocio desde cero, si es que eso llega a ser posible.

Fuente: https://www.silicon.es/

LINK DE LA NOTICIA