“Hay un ataque de ransomware cada 11 segundos: las empresas deben estar preparadas”

ANDREA BAGGIO
CEO DE REPUTATIONUP

ReputationUP y HelpRansomware lideran en ciberseguridad con soluciones para recuperación de datos, eliminación de filtraciones y gestión de crisis reputacionales.

El Grupo ReputationUP se posiciona como líder global en ciberseguridad y gestión de reputación. Con HelpRansomware asiste a las empresas en la recuperación de datos encriptados tras ataques de ransomware; y con ReputationUP, se encarga de eliminar datos que han sido filtrados y publicados tras un data leak, para prevenir la pérdida de confianza de los clientes.

Se dice que las empresas no deben preguntarse si serán atacadas, sino cuándo lo serán. ¿Es así?

Un ataque de ransomware ocurre cada 11 segundos. Esto implica que las empresas deben aceptar que, en algún momento, serán objetivo de un ataque.

¿Cuáles son los primeros pasos que una empresa debería tomar tras sufrir un ataque de ransomware y cómo ayuda HelpRansomware en esta fase crítica?

Lo primero y más importante es aislar los sistemas afectados para evitar que el ransomware se propague a otras áreas. A continuación, hay que notificar de inmediato al equipo de TI o al proveedor de servicios de ciberseguridad para que puedan intervenir rápidamente. Por último, es esencial evaluar el alcance del daño para saber exactamente a qué nos enfrentamos. En esta fase crítica, HelpRansomware proporciona un apoyo integral a las empresas mediante tres pasos clave: un análisis exhaustivo del ataque, un proceso de recuperación completo y la implementación de estrategias para prevenir el pago de rescates.

¿Por qué es tan importante no pagar el rescate?

Pagar a los ciberdelincuentes no asegura la recuperación de los datos, y, en muchas ocasiones, los atacantes exigen pagos adicionales. Además, esta acción fomenta la actividad criminal, creando un ciclo que perjudica a otras empresas. FBI, Europol y las autoridades de ciberseguridad en España desaconsejan firmemente el pago de rescates.

En los casos de filtración de datos sensibles tras un ataque, ¿cómo aborda ReputationUP la eliminación de esta información?

Primero, utilizamos herramientas de monitoreo especializadas que rastrean en tiempo real surface web, deep web y dark web. Esto nos permite localizar rápidamente los datos filtrados. Una vez que los identificamos, iniciamos el proceso de eliminación a través de solicitudes legales y acciones técnicas.

Esta capacidad de respuesta inmediata reduce significativamente el tiempo en que la información filtrada está disponible, limitando los daños reputacionales y financieros.

¿Qué estrategias proponen para que las empresas puedan recuperar su imagen pública tras un ataque?

En ReputationUP, junto a HelpRansomware, gestionamos las crisis en cuatro etapas. Primero, realizamos un análisis forense para identificar el ransomware, localizar el punto de acceso y evaluar los daños. Luego, eliminamos datos filtrados y prevenimos crisis reputacionales.

En comunicación, trabajamos en tres niveles: informamos internamente a empleados y proveedores; gestionamos la relación con medios y público; y coordinamos con autoridades para asegurar el cumplimiento normativo.

Finalmente, reforzamos la confianza a largo plazo mediante auditorías de ciberseguridad, certificaciones actualizadas y programas de compensación para clientes afectados, fortaleciendo las relaciones y garantizando la recuperación total de la empresa.

Desde su experiencia, ¿qué medidas preventivas recomiendan implementar a las empresas?

Existen tres medidas preventivas esenciales que, sorprendentemente, muchas empresas aún pasan por alto. En primer lugar, los simulacros de ciberataques reales, que son cruciales para preparar a los equipos y garantizar una reacción rápida y efectiva. En segundo lugar, la monitorización de datos sensibles en la dark web, que permite actuar antes de que el problema se agrave y minimizar el impacto. Por último, una estrategia de comunicación integrada, ya que, en una crisis, lo que se dice y cómo se dice puede ser determinante para perder o mantener la confianza de los clientes, el activo más valioso de cualquier empresa.

www.reputationup.com