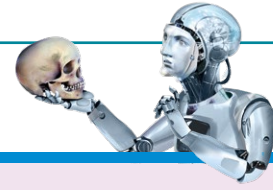
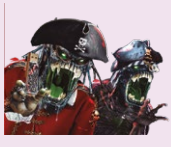
CAVILACIONES SEGURAS



Lecciones tras un ciberataque

En la anterior "cavilación segura", titulada "2024: diario de un CISO", algunos de mis más fieles lectores creyeron que era una descripción de mi realidad laboral. Todo lo contrario: se trataba de uno de mis sueños, o pesadillas, más frecuentes. Dicen que escribir las experiencias oníricas contribuye a que se conviertan en realidad si son sueños o a desecharlas sanamente si son pesadillas. Veremos. Tengan por seguro que les informaré puntualmente si así ocurre.

En esta ocasión, siguiendo el mismo guión, compartiré los pasos que, como CISO de una compañía que cotiza en el IBEX 35, he tenido que seguir tras haber sufrido un ciberataque que trascendió a los medios de comunicación hace unas semanas.



"Ante el ciberataque, respondí a la obligación de enviar más de cinco formularios de reporte a distintas entidades, todos ellos con una estructura distinta y con exigentes plazos de entrega"

Observar cómo abren los noticieros en radio y televisión, tanto de cadenas públicas como privadas, así como los principales portales de noticias, con la primicia de un grave incidente de ciberseguridad ocurrido en la empresa en la que tú eres el máximo responsable de su seguridad es una experiencia única de la que se puede aprender mucho si se mantiene la calma y se practica la prudencia.

El primer hecho con el que tuve que enfrentarme: la información de la que se hicieron eco los medios de comunicación poco, muy poco, tenía que ver con lo que en realidad había sucedido. Pronto vi que tenía que tratar con tres desafíos: primero, responder y contener el ciberincidente; segundo, reportar a las autoridades relacionadas con la protección de infraestructuras nacionales críticas; y, tercero, informar directamente a los medios para mitigar los posibles efectos negativos que la desinformación podría causar a nuestros clientes.

El primer reto es, sin duda, esencial para la supervivencia de la organización que proteges. Afortunadamente todos los años realizamos un simulacro de respuesta a un ciberincidente severo, involucrando no sólo a los equipos técnicos, sino también a nuestro consejo de dirección, proveedores y clientes. Siempre encontramos debilidades a mitigar y escenarios que requieren nuevos métodos de actuación que no habíamos planeado anteriormente cómo tratar.

Para la segunda dificultad, al ser nuestra compañía un componente esencial de la infraestructura crítica de nuestro país, siguiendo la legislación europea NIS2, tuve que reportar al Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) y, como también realizamos operaciones en Alemania, a la Oficina Federal de Seguridad de la Tecnología de la Información (BSI). El incidente nos causó una pérdida económica considerable, así que también tuve que denunciar el caso a las policías española y alemana. Al trabajar en un sector regulado, en paralelo, tuve que reportar lo sucedido, con todos sus detalles, a nuestra entidad reguladora nacional y a la europea. Los CERTs nacionales de los países en los que operamos también nos contactaron para conocer los detalles del ataque. En total, respondí a la obligación de enviar más de cinco formularios de reporte de ciber incidentes a distintas entidades, todos ellos con una estructura distinta y con exigentes plazos de entrega.

El tercer problema, la comunicación con el público, requirió la creación de un gabinete de prensa dentro de la compañía para gestionar directamente, sin intermediarios, las ventanas de información, el relato del impacto del incidente y los pasos que estábamos dando para volver a ponernos en pie: desde nuestra web y nuestra presencia en las redes sociales dábamos información consistente y real de nuestras actividades de respuesta y recuperación. De este modo evitábamos la desinformación, basada en rumores si cabe más perniciosos que la propia realidad.

Afortunadamente, hemos sobrevivido a esta "tormenta perfecta": hemos recuperado los sistemas impactados, hemos informado en todo momento a nuestros clientes y proveedores y el mercado ha premiado nuestra política de comunicación con una subida de la cotización de nuestras acciones.

En mi cuaderno de lecciones aprendidas he anotado los siguientes puntos: los simulacros anuales de ciberataques críticos son esenciales, dichas pruebas han de ser reales y deben involucrar a todas las partes presentes en la cadena de valor, tanto internas como externas. El proceso de reporte del incidente debe de realizarse de forma continuada y muy detallada para que podamos mantener el flujo de información requerido por las legislaciones nacional y europea, pero, preferiblemente, a través de un único canal, para evitar la duplicación de esfuerzo. Finalmente, el gabinete de prensa que gestione las crisis ciber reportará directamente al CISO y al CEO de la compañía e incluirá no sólo habilidades y experiencia en comunicación, sino también conocimiento en tecnología.

Así estaremos más preparados para resistir el próximo ciber incidente, que, tarde o temprano, afectará de nuevo a nuestros datos y sistemas.

Dr. Alberto Partida
linkedin.com/in/albertopartida