Canción triste de Hill Street... ¡Tengan cuidado ahí fuera!

Aquellos lectores nacidos en las penúltimas décadas del siglo pasado aún recordarán la serie policíaca "Canción triste de Hill Street", con el "capitán Furillo" al mando, cuya trama giraba en torno a posibles diferencias entre lo correcto y lo que funciona.

Justo un año después de esa serie, en 1988, la universidad Carnegie Mellon en Pennsylvania, Estados Unidos, acuñó, y patentó, el término "Computer Emergency Security Team" (CERT). Este primer CERT fue la respuesta a la aparición la noche del 2 al 3 de noviembre de 1988 del pionero de los software maliciosos y auto-replicantes: el gusano de Morris. Desde entonces, la necesidad de disponer de un equipo profesional de intervención rápida frente a emergencias digitales sólo ha crecido y crecido.

Un detalle controvertido pero crucial es conocer al equipo que protegerá tu información: su experiencia, su formación, su motivación y sus condiciones laborales y nivel de rotación.

Por cierto, como el nombre de CERT está patentado, se recomienda utilizar el término genérico "Computer Security Incident Response Team" (CSIRT) para cualquier otro equipo de emergencias digitales que exista. Los CSIRTs iniciales han evolucionado hasta los centros de operaciones de seguridad (SOCs) actuales, cuya misión es la monitorización en tiempo real de los eventos de seguridad de una organización y la respuesta frente a posibles incidentes de seguridad.

Hoy en día hay cientos de CSIRTs por todo el mundo, de origen privado y público, sectoriales, nacionales, multinacionales, etc. La organización que agrupa a más CSIRTs es FIRST (el "Forum of Incident Response and Security Teams"), creado en Carolina del Norte en 1990 como organización sin ánimo de lucro.

El servicio de respuestas a incidentes es esencial para cualquier empresa conectada a Internet, independientemente de su tamaño. Eurostat publicó en 2017 que el 66% de la población activa en la Unión Europea, unos 94 millones de personas, trabajan en pequeñas y medianas empresas (pymes). Un ataque certero a cualquiera de estas empresas, por ejemplo un "*phishing* a medida" o un "ransomware" bien inyectado, puede suponer un daño de reputación irreparable o, incluso, sencillamente su desaparición. Los recursos disponibles de estas pequeñas empresas no permiten la creación de su propio CSIRT. Desde esta columna sólo puedo recomendar a empresarios y autónomos que contraten un servicio profesional de respuesta a incidentes digitales. ¿Cómo elegir el adecuado? Aquí van algunas pistas para seleccionar el SOC adecuado:

- Averigua el tamaño medio de sus clientes, no te interesa ser el cliente "más diminuto de su cartera".
- Confirma cómo recogen inteligencia operativa de ataques reales en tu sector y cómo interactúan con CSIRTs públicos autonómicos, nacionales y europeos.
- Es importante que reciban y compartan información operativa con otros SOCs.
- Solicita información sobre su grado de automatización de respuestas frente a incidentes: en ocasiones aún estamos anclados en la imagen de un analista junior pegado a una pantalla de monitorización sin pestañear, confiando en que sepa reaccionar frente a todas las alertas que el SIEM ("Security Incident and Event Monitoring") de turno le muestre.
- Un detalle controvertido pero crucial es conocer al equipo que protegerá tu información: su experiencia, su formación, su motivación y, relacionado con este punto, sus condiciones laborales y nivel de rotación.
- Adicionalmente, infórmate sobre cómo pueden ayudarte en tus procesos de comunicación con clientes, fuerzas del orden, proveedores y empleados, tras sufrir un ataque digital.
- Finalmente, recomiendo que denuncies todo ataque exitoso. Tus atacantes son delincuentes digitales.

Como bien decía el "capitán Furillo", tengan cuidado ahí fuera... y busquen un SOC que les funcione.

Alberto Partida
Analista en Ciberseguridad
itsecuriteer@gmail.com
@itsecuriteer en twitter
https://linkedin.com/in/albertopartida