Mónica de la Huerga Ayuso,
miembro vocal del Grupo de
Calidad y Seguridad de Autelsi
y CISO de Sopra Steria España

En los ciberdelitos, los datos siguen siendo el elemento clave

Por sexto año consecutivo, Europol ha publicado el informe IOCTA (Internet Organised Crime Threat Assessment), cuyo objetivo es proporcionar una descripción general de las amenazas y tendencias actuales de los delitos cometidos "on-line".

Si bien el ciberdelito está en constante evolución, el IOCTA nos muestra que los datos siguen siendo el elemento clave.

Dentro de los ataques centrados en los datos, el "ransomware" aún es la forma de ataque cibernético más extendido. También se identificaron los ataques de denegación de servicio distribuida (DDoS) como otra amenaza importante. La ingeniería social y el phishing son las ciberamenazas transversales más importantes.

Una vez más, el informe muestra cómo la web oscura es el facilitador clave para el comercio de una amplia gama de productos y servicios criminales.

Ahora bien, ¿qué podemos hacer? Evidentemente, no lo eliminaremos, pero sí podemos poner en marcha acciones que nos protejan como:

1. Realizar evaluaciones de riesgos de seguridad. Ayudan a analizar el nivel de seguridad actual, identificar las vulnerabilidades y determinar los controles adecuados para mitigar el riesgo.
2. Establecer políticas de ciberseguridad. Guías fundamentales que definen las mejores prácticas a seguir en la organización.
3. Sensibilizar sobre la ciberseguridad. Uno de los medios más efectivos para combatir los ciberataques (phishing, SPAM y 'ransomware', entre otros) es la creación de una 'cultura de ciberseguridad', mediante capacitación y formaciones periódicas.
4. Mantener el software actualizado. Las aplicaciones, sistemas operativos y software de seguridad deben revisarse periódicamente y desplegar todas las actualizaciones y parches. Así, evitaremos ataques que se basan en explotar vulnerabilidades de los fabricantes de SW.
5. Antivirus y firewall. Debemos instalar un antivirus y un firewall, mantenerlos actualizados y realizar revisiones periódicas en los dispositivos. De esta forma, reduciremos el riesgo de que un malware se cuele en nuestro sistema.
6. Copias de seguridad periódicas. De este modo, en caso de 'ransomware', podremos reestablecer el servicio con mayor agilidad.
7. Contraseña segura. Se deben usar siempre contraseñas seguras (mayúsculas, minúsculas, números y caracteres especiales), renovarlas a menudo y no utilizar la misma en distintos servicios.
8. Autenticación de factor múltiple (MFA). Una de las mejores formas de proteger las cuentas es usar la autenticación de dos factores: para acceder, además del nombre de usuario y la contraseña, hay que indicar un código que se envía por mensaje de texto al teléfono móvil.
9. Control de usuarios privilegiados (PAM). El control de accesos a los sistemas es fundamental para evitar riesgos de seguridad, más aún en el caso de los usuarios privilegiados, ya que son el blanco principal de los ciberdelincuentes. •