CIBERSEGURIDAD 2025. AMENAZAS, DESAFÍOS, TENDENCIAS Y OPORTUNIDADES

La ciberseguridad se ha convertido en una prioridad para todo tipo de entidades y organizaciones y, muy especialmente, para las que gestionan infraestructuras esenciales y estratégicas, debido al aumento de las ciberamenazas. El autor comparte algunas reflexiones sobre lo que nos espera en 2025 donde, la IA generativa y la evolución del ransomware serán protagonistas, provocando ciberataques más específicos y peligrosos

Foto: freepick

ESPAÑA

Manuel Sánchez Gómez-Merelo

Los ciberataques globales alcanzan el 1.5% del PIB mundial actual. En España, según datos del Incibe, los ciberataques se configuran como la segunda mayor amenaza para la seguridad nacional.

La demanda y la oferta de servicios relacionados con la ciberseguridad está evolucionando rápidamente y, a medida que nos acercamos a 2025, las distintas entidades se enfrentan un panorama con crecientes amenazas y desafíos que marcan claras tendencias y oportunidades.

En este contexto, la legislación europea (en particular NIS2[1] y DORA[2]) plantea nuevas exigencias y responsabilidades en la gestión de los riesgos y la reacción ante un ataque. Por otra parte, nuevas tecnologías, como la inteligencia artificial (IA) o la computación cuántica, que están llegando o próximas a llegar, plantean desafíos adicionales.

AMENAZAS Y VULNERABILIDADES

Las infraestructuras críticas y esenciales seguirán sufriendo ataques en una tendencia alcista y un reto preocupante. Los gobiernos de algunas naciones alientan a grupos de hackers para atacar estas infraestructuras con objeto de desestabilizar una organización o a un país entero, en una estrategia de "guerra fría". Por este motivo, los sistemas OT (Tecnología Operativa) ya están siendo un objetivo clave, pues representan el soporte en sectores estratégicos y críticos. Fortalecer su ciberseguridad es y será prioritario, considerando su vulnerabilidad en conflictos recientes, con graves consecuencias para las infraestructuras y poblaciones afectadas.

Así, nos encontramos ciertas tendencias y retos que requerirán específicas soluciones de seguridad:

- **Amenazas contra los sistemas OT.** Los sistemas OT, esenciales en sectores críticos, como energía, transporte, logística, comunicaciones, etc. están cada vez más interconectados y globalizados, aumentando sus riesgos y vulnerabilidades ante ciberataques. Estos sistemas ya han sido considerados como objetivos de grupos de hackers apoyados por gobiernos, que se infiltran en las redes de los sistemas OT a través de códigos maliciosos ante su importancia en sectores estratégicos y un ciberataque podría ocasionar daños importantes.
- **Impacto de la IA generativa.** La inteligencia artificial generativa, ampliamente utilizada para crear contenidos como documentaciones, imágenes y videos, también se está empezando a emplear con fines maliciosos en las etapas iniciales de ataques persistentes avanzados. Con ella, los cibercriminales aprovechan su capacidad para suplantar personas y para analizar entre las grandes cantidades de datos en la *"dark web"* y para automatizar y perfeccionar sus ataques.
- **Dependencia creciente en la cadena de suministro.** Las empresas dependen cada vez más de sus proveedores, como en el caso de los suministros de electricidad, agua y otros bienes. También intercambian datos con otras organizaciones de manera habitual. Esto tiene como consecuencia que el impacto de un incidente grave o un ataque en un suministrador repercuta directamente en la propia organización.

Esto exigirá adaptar los sistemas de prevención y protección, así como avanzar en marcos legales que aborden los interrogantes abiertos por estas tecnologías, incluso en sus usos legítimos, éticos y beneficiosos.

TENDENCIAS EN CIBERSEGURIDAD

En paralelo con lo anterior, también los servicios y soluciones de ciberseguridad evolucionarán para responder a los riesgos de seguridad. En este contexto, hay ciertas tendencias que se están extendiendo de manera progresiva y general.

- **Uso de la IA en la detección de in-**


Foto: freepick

cidentes: la IA ya se está empleando en algunas técnicas existentes en ciberseguridad, como la confección de reglas de detección de incidentes en los SIEMs (Sistemas de Monitorización de Eventos), detección de comportamientos anómalos que pueden ser síntoma de una infección, etc. En el futuro, este uso crecerá de manera exponencial.

- **Integración de IA en operaciones de seguridad:** con el aumento de amenazas, los SOC evolucionarán para que los analistas de IA avanzada ejecuten la mayoría de los flujos de trabajo de detección y respuesta de forma autónoma, permitiendo a los analistas enfocarse en tareas estratégicas. La transparencia y la gestión de la IA en seguridad serán esenciales.
- **Arquitectura de ciberseguridad unificada:** las herramientas de seguridad para dispositivos de IT (Tecnologías de la Información) deben servir también para proteger una instalación, tanto en entorno local ("on premise") como en la nube ("on cloud"). Además, dado que los dispositivos de OT están conectados a redes de dispositivos de IT, deben proteger también los dispositivos OT. De esta manera, es cada vez más difusa la frontera entre la seguridad IT y OT.
- **Seguridad de los dispositivos IoT:** en 2025, la cantidad de dispositivos IoT que requerirán conexión a redes continuará en aumento. Organizaciones grandes y pequeñas tendrán problemas para controlar este crecimiento, ya que muchos de estos dispositivos no disponen de sistemas automatizados para gestionar sus identidades, lo que dificulta su administración y gestión, y su vulnerabilidad puede ser blanco de ciberdelincuentes. Además, algunos de ellos son introducidos o usados por los propios trabajadores de las organizaciones y no están inventariados.
- **Colaboración en la gestión de incidentes:** uno de los principios de la normativa europea (NIS2 y DORA ya mencionados) es la obligatoriedad de la notificación de incidentes de seguridad. Esto conlleva mayor responsabilidad para los puestos de responsables de seguridad (CISO y CSO, por ejemplo). Además, los organismos de coordinación (CERTs) van a tener más potestad para ejercer su trabajo de coordinación ante incidentes.
- **Criptografía post-cuántica:** algunos de los algoritmos criptográficos (de firma o de cifrado) que se utilizan en la actualidad, como RSA, AES, etc. se volverán completamente vulnerables frente a la inmensa potencia de cálculo de los ordenadores cuánticos. La criptografía post-cuántica (PQC), que actualmente está en fase de análisis inicial, tiene como objetivo reemplazar los sistemas criptográficos actuales por otros preparados para esa capacidad de cómputo.
- **Talento y formación en seguridad:** la brecha de escasez y talento en seguridad informática seguirá siendo un desafío en 2025. La falta de personal capacitado y especializado y la alta demanda de expertos en áreas emergentes como la criptografía cuántica y la IA mantendrán a las organizaciones bajo presión para mantenerse protegidas.

Estas son algunas tendencias notables que emergerán en la ciberseguridad para el próximo año 2025, un escenario con grandes desafíos marcados por el crecimiento del uso de la inteligencia artificial generativa también por parte del cibercrimen.

OPORTUNIDADES

El incremento previsto de ciberataques de alto impacto, hasta la aplicación e integración de la IA generativa y la criptografía cuántica darán lugar a nuevas oportunidades y soluciones eficientes, haciendo que las tendencias y predicciones para 2025 sirvan como guías esenciales para que las organizaciones definan sus estrategias de ciberseguridad y maximicen el potencial mediante la aplicación de principios como:

- La adopción de una estrategia para adaptación a la IA de una manera provechosa y no disruptiva.
- La preparación ante ataques que ahora empiezan a usar la IA.
- La adopción de una arquitectura de ciberseguridad que unifique los dispositivos IT y los OT.
- El diseño de la arquitectura anterior en el modelo de Confianza Cero.
- Fortalecer los sistemas de autenticación mediante soluciones multifactor y de biometría.
- Preparar los sistemas para la criptografía post-cuántica.
- Fortalecer la colaboración en ciberseguridad.
- Formar y concienciar a los trabajadores y clientes en las amenazas y riesgos de seguridad.
- Fomentar la resiliencia de las organizaciones ante situaciones de crisis.

Estos son algunos de los principales desafíos, amenazas, tendencias, que también representan oportunidades que prevemos serán centrales para la ciberseguridad en este año, en el que los sistemas y dispositivos OT serán el objetivo clave del cibercrimen, por su interconexión y su importancia, sobre todo en sectores esenciales y estratégicos, por lo que fortalecer su ciberseguridad será prioritario, considerando su vulnerabilidad demostrada en conflictos recientes.

Estar protegido en 2025 requerirá algo más que simples defensas básicas y cumplimiento normativo. Las entidades y organizaciones deberán adoptar estrategias proactivas, aprovechar sistemas avanzados y fomentar la concienciación y capacitación sobre ciberseguridad en toda su organización. ■

Referencias:

[1] *Directiva (UE) 2022/2555.*

[2] *Reglamento (UE) 2022/2554.*

Manuel Sánchez Gómez-Merelo,
consultor internacional de seguridad.
Más el autor:

Foto: freepick