LA VANGUARDIA Dinero
La Vanguardia -Dinero
España
08/11/26
Pr: Semanal (Domingo)
Tirada: 31.744
Dif: 25.456
Cod: 187205634
Pagina: 4
Secc: MERCADOS (Bolsa) Valor: 37.969,40 € Area (cm2): 492,3 Ocupac: 49,7 % Doc: 1/1 Autor: Transversal José García Montalvo Num. Lec: 336000

Transversal
José García Montalvo
Catedrático de Economía (UPF)

El frío, la sangre y el dinero



En apenas dos semanas, unos delincuentes han calentado congeladores de supermercados hasta los 50 grados, han intentado convertir en hornos las cámaras de plasma de un banco de sangre y han vaciado en veinte minutos las carteras de la mayor plataforma de criptomonedas del mundo. Mientras tanto, un fallo en el lenguaje de programación de buena parte de internet ha obligado a parchear millones de servidores a toda prisa, incluidos los de WordPress, donde tengo alojada mi página web. No son sucesos aislados. Muestran un ecosistema digital que ha crecido más rápido que su seguridad.

El 21 de octubre, el proyecto PHP publicó parches para dos vulnerabilidades críticas que permiten a un atacante sin credenciales ejecutar código en un servidor web, con una gravedad de 9,2 sobre 10. El segundo frente es más físico. Cientos de supermercados franceses de Intermarché, Coopérative U y Carrefour vieron cómo alguien tomaba el control remoto de sus equipos de frío. Hubo temperaturas de hasta 50 grados e incluso incendios. Ese mismo lunes, los atacantes entraron en Coolworld, proveedor de refrigeración del Establecimiento Francés de la Sangre. Intentaron subir tres cámaras de plasma de 30 grados bajo cero a 110 grados. El 29 de octubre se produjo el mayor robo de la historia. Binance perdió unos 6.300 millones de dólares en sus carteras conectadas a internet. Según la propia empresa, la mayor parte salió en solo veinte minutos.

Estos casos encajan en una tendencia de fondo: la aceleración de los ciberataques. La agencia europea Enisa identifica el *ransomware* (el secuestro de sistemas a cambio de rescate) como la amenaza más dañina. El *phishing* es la vía de entrada en el 60% de los casos, y la explotación de vulnerabilidades en el 21,3%. A principios del 2025, las campañas apoyadas en inteligencia artificial ya suponían más del 80% de la ingeniería social observada. El delito se vende ya como un servicio: alquilar un kit de *phishing* o de *ransomware* no exige saber programar.

Para el ciudadano de a pie, la ciberseguridad ya no es cosa de informáticos. Las amenazas más frecuentes contra particulares son las compras fraudulentas (17%), las llamadas falsas o *vishing* (15%) y los SMS engañosos o *smishing* (10%). La línea gratuita de ayuda 017 atendió 142.767 consultas en el 2025, casi un 45% más que el año anterior. También hay efectos indirectos: alimentos retirados de las tiendas, servicios caídos, datos personales filtrados en webs mal mantenidas y, cada vez más, voces y vídeos clonados con IA que suplantan a un familiar o a un banco. Las pymes son el eslabón empresarial más débil. Seis de cada diez incidentes gestionados por el Incibe afectaron a pymes y autónomos. Según Verizon, el *ransomware* aparece en el 88% de las brechas sufridas por pymes, frente al 39% en las grandes organizaciones. Una pyme rara vez tiene un responsable de seguridad, copias de seguridad probadas o capacidad de aguantar semanas sin facturar. Para un pequeño comercio un solo ataque puede suponer el cierre.

Los mayores retos son cuatro. El primero es que el ataque puede ser indirecto, a un proveedor, en lugar de directo. Hoy se ataca al suministrador del frío, no al supermercado ni al hospital. Se ataca al consultor, no al banco. La participación de terceros en brechas digitales se ha multiplicado. La convergencia entre informática y mundo físico rápidamente convierte una contraseña débil en comida podrida o plasma inservible. En segundo lugar, el ciberespacio es utilizado por algunos estados para financiarse o para sabotear sin declarar la guerra. La gran capacidad humana y financiera de los atacantes se une a la debilidad de las organizaciones que sustentan software vital, fundaciones sin ánimo de lucro con unos pocos desarrolladores que se sostienen a partir de donaciones o colaboran sin retribución. Por ejemplo, la fundación de PHP tiene solo una persona a tiempo completo y 13 o 14 desarrolladores a tiempo parcial. Linus tiene a su creador, Linus Torvalds, y unos 30 desarrolladores principales independientes. ¿Se imaginan estas estructuras atacadas por hackers de Corea del Norte o Rusia provistos de una IA de frontera? En tercer lugar, la velocidad a la que se explotan los fallos de seguridad es meteórica. A veces son pocas horas. En cuarto lugar, persistimos en los errores más comunes. Por ejemplo, dejar contraseñas de fábrica y equipos de gestión expuestos directamente a internet, como en el caso de las neveras. Confiar a ciegas en los proveedores. Usar el mismo portátil para todo, sin segmentar redes ni limitar privilegios. Así, un solo equipo comprometido acaba abriendo la caja fuerte, como en Binance.

Cuántica
La computación cuántica obligará a sustituir buena parte de la criptografía que hoy protege bancos, firmas digitales y criptomonedas

Y en el horizonte hay un riesgo de otra escala. Casi toda la criptografía de clave pública que protege la banca en línea, las firmas digitales o las propias carteras de criptomonedas serían susceptibles a un ordenador cuántico suficientemente grande. Hoy esa máquina no existe, pero las estimaciones sobre la fecha de su nacimiento bajan deprisa. El peligro, sin embargo, ya ha empezado. Se llama "cosechar ahora, descifrar después": copiar hoy comunicaciones cifradas para leerlas cuando exista la máquina. La respuesta es la criptografía poscuántica, es decir, nuevos algoritmos resistentes a estos ordenadores como el ML-KEM, el ML-DSA y el SLH-DSA. Pero el problema es práctico más que matemático. Muchas organizaciones no saben dónde usan criptografía, y cambiarla afecta a tarjetas, terminales, sistemas industriales y equipos con décadas de vida útil. Si un supermercado europeo todavía tenía en el 2026 controladores con contraseñas de fábrica, cuesta imaginar que todo su parque esté listo para la era cuántica en pocos años.

La paradoja de este otoño es que los ataques más llamativos explotaron debilidades muy corrientes: un portátil, un controlador antiguo, un parche pendiente o la ingenuidad de un empleado en una entrevista de trabajo. La ciberseguridad se parece cada vez más a la salud pública. Funciona cuando se cumplen rutinas aburridas: actualizar, separar redes, usar doble verificación, hacer copias de seguridad y exigir lo mismo a los proveedores. La computación cuántica no cambiará esa lógica, solo acortará el plazo para cumplirla. |

Ciberseguridad cotidiana
La mayoría de los grandes ataques siguen aprovechando fallos básicos: contraseñas débiles, parches pendientes o redes mal segmentadas