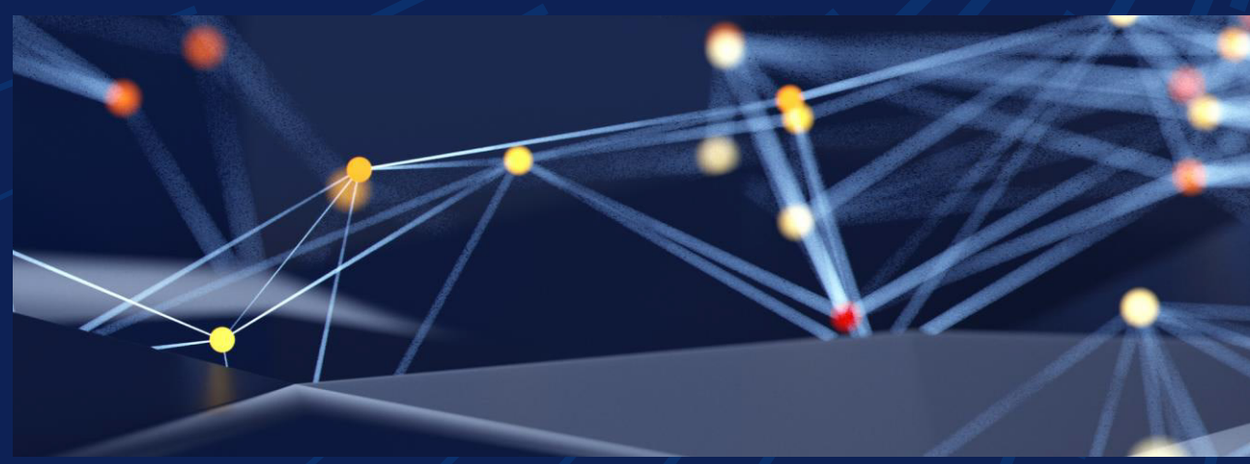
El futuro de la ciberseguridad:

Adaptación a la nueva era digital



Aunque los profesionales de ciberseguridad suelen centrarse en prevenir ataques y crear planes de recuperación, el sector evoluciona constantemente. Por lo tanto, es importante prepararse para lo que está por venir.

De cara al futuro, destacan tres áreas: la criptografía postcuántica, el cambiante panorama normativo y las amenazas emergentes. Las empresas deben actuar cuanto antes e implementar las últimas soluciones.

Los inicios de la criptografía postcuántica

La computación cuántica promete transformar muchos sectores con una potencia asombrosa capaz de resolver problemas fuera del alcance de los ordenadores clásicos. Sin embargo, esta misma potencia podría hacer que los métodos criptográficos actuales queden obsoletos. Los algoritmos como el RSA y el ECC, que sustentan gran parte de las comunicaciones seguras de hoy en día, podrían ser descifrados en cuestión de segundos por un equipo cuántico lo suficientemente avanzado. Esta amenaza inminente hace que la criptografía postcuántica sea aún más urgente.

La criptografía postcuántica (PQC) se centra en el desarrollo de algoritmos criptográficos que sean seguros en la era de la computación cuántica. El Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos ha reconocido este riesgo inminente y lidera la tarea de estandarizar algoritmos resistentes a esta computación.

Las empresas deben prepararse para esta transición. La adopción temprana de soluciones PQC garantizará la seguridad de los datos cuando los atacantes tengan acceso a la computación cuántica.

Tal y como señala Bobbie Stempfley, vicepresidenta de ciberseguridad y directora de seguridad de la unidad de negocio en Dell, las organizaciones deben comenzar centrándose en dos áreas clave:

Identificar e inventariar todos los modelos criptográficos que se utilizan actualmente.

Se deben considerar tanto los datos en transferencia como los datos en reposo. Piense en la gestión de claves, la firma de código, la identificación de dispositivos, el acceso seguro y la telemetría. Cree un inventario completo y una hoja de ruta.

Conocer la situación de los proveedores.

Las empresas modernas pueden tener miles de proveedores, así que tenga en cuenta los posibles riesgos relacionados. Asegúrese de que también se están preparando para el cambio.

Después de estos primeros pasos, realice evaluaciones de riesgos para identificar sistemas vulnerables, analice la implementación de modelos criptográficos híbridos para continuar con las operaciones durante la transición y colabore con proveedores que ya están explorando soluciones postcuánticas. Ahora bien, tenga en cuenta que no habrá un proveedor ni una tecnología que ofrezca soluciones listas para usar.

Cambios normativos en un mundo globalizado

Otro factor que determina el futuro de la ciberseguridad es la evolución de las normativas. Ahora, son mucho más que requisitos legales. Se están convirtiendo en un marco clave para inculcar responsabilidad, impulsar actualizaciones tecnológicas y proteger a la ciudadanía en un mundo interconectado y basado en los datos. No obstante, están evolucionando rápidamente y son muy distintas según la región, lo que aumenta la complejidad del cumplimiento.

Dicho esto, las normativas no solo marcan las sanciones en caso de infracción, sino que también impulsan mejores prácticas de ciberseguridad. Las empresas que coordinan sus políticas con los requisitos normativos afianzan la confianza del mercado y la eficiencia operativa. Para ello, deben establecer marcos de gobernanza flexibles que se adapten a los cambios legales, llevar a cabo auditorías periódicas de cumplimiento normativo e invertir en formación para que el personal gestione la información confidencial de acuerdo con los últimos estándares.

Durante el proceso, es importante que los equipos encargados de la seguridad se comuniquen con claridad. A menudo, hablan con términos especializados que los clientes, las autoridades y otras partes interesadas desconocen. Es vital que los profesionales de la seguridad se aseguren de que todo el mundo les entiende.

> El paso a la criptografía postcuántica es como recoger y trasladar una casa completamente amueblada. Será así de complejo, y el reto es no romper nada en el proceso".
>
> ***Bobbie Stempfley***
> *Vicepresidenta de ciberseguridad y directora de seguridad de la unidad de negocio en Dell Technologies*

La evolución de las amenazas y las defensas

La IA es toda una revolución para las empresas: aumenta la productividad y desvela nuevos horizontes para el potencial humano. Aun así, en lo que respecta a la ciberseguridad, la IA beneficia tanto a los agentes maliciosos como a los sistemas de defensa:

Uso en ataque: La IA permite ataques más sofisticados, como el spear phishing y los deepfakes muy convincentes.

Uso defensivo: La IA facilita la defensa ante ataques porque permite:

- Procesar grandes cantidades de datos de seguridad rápidamente.
- Priorizar las amenazas con mayor eficacia.
- Mejorar las capacidades de detección y respuesta.

Sin embargo, las herramientas de ciberseguridad solo seguirán mejorando gracias al procesamiento del lenguaje natural, que permite a los profesionales del sector interactuar más directamente con sus sistemas y potenciarlos para tomar medidas correctivas de forma proactiva.

Las organizaciones deben esforzarse para aprovechar estas capacidades y, al mismo tiempo, mantener al día su formación y otros mecanismos defensivos. La formación es la mejor manera de evitar que el personal sea víctima de ataques más sofisticados.

Adiós a las contraseñas

Las contraseñas ya no son los métodos más seguros para la identificación y la gestión de accesos.

Los sistemas tradicionales basados en contraseñas presentan vulnerabilidades significativas, por lo que son una solución cada vez más inadecuada para las necesidades de ciberseguridad modernas. Las contraseñas son susceptibles a ataques como el relleno de credenciales, el phishing y los intentos de fuerza bruta, lo que a menudo expone a las organizaciones a riesgos innecesarios. Además, los comportamientos deficientes de los usuarios, como usar contraseñas reutilizadas o débiles, agravan estas vulnerabilidades.

Los métodos de autenticación sin contraseña, como los datos biométricos, los certificados y los tokens de hardware, son una alternativa más segura y sólida, ya que los ataques relacionados con las contraseñas quedan descartados. Pasar a este tipo de sistemas es una evolución crucial en la gestión de identidades y accesos, porque supone una medida de seguridad a la altura de las ciberamenazas cada vez más sofisticadas.

La adopción de tecnologías sin contraseña también ofrece numerosos beneficios, como reducir la superficie de ataque, mejorar la experiencia del usuario mediante inicios de sesión más rápidos y fluidos, y rebajar los costes de TI al disminuir los incidentes relacionados con contraseñas. El uso de métodos avanzados garantiza un estado de seguridad más sólido y ayuda a las organizaciones a cumplir los estándares normativos. La transición a sistemas sin contraseñas no es solo una tendencia; es un paso necesario para crear un ecosistema digital más seguro y eficiente para particulares y empresas.

Conclusión

La ciberseguridad está entrando en una era transformadora, moldeada por la computación cuántica, las normativas cambiantes y las amenazas cada vez más sofisticadas. Para mantenerse a la vanguardia, las empresas deben adoptar innovaciones como la criptografía postcuántica, las defensas basadas en IA y la autenticación sin contraseña. Al priorizar la preparación, la colaboración y la inversión estratégica, podrán crear un entorno digital más seguro y resiliente. Es el momento de actuar.

Productos y soluciones Dell que pueden serle útiles

Solución Dell recomendada	Descripción
Cybersecurity Advisory Services	Orientación de expertos para prepararse ante las amenazas en evolución, tanto actuales como emergentes.
vCISO	Un director de seguridad de la información virtual y experto en ciberseguridad que puede ayudarle a identificar y gestionar riesgos, así como a guiar la toma de decisiones estratégicas.

Descubra cómo afrontar algunos de los principales retos de ciberseguridad actuales en **dell.com/cybersecuritymonth**

DELL Technologies