Día Mundial de la Contraseña: por qué es hora de decirles adiós

01/05/2025

Cada año, el primer jueves de mayo, los profesionales de la ciberseguridad instan al público a fortalecer la higiene de sus contraseñas. Pero en 2025, esta tradición podría haber caducado. ¿Por qué? Porque **nuestra excesiva dependencia de las contraseñas se está convirtiendo en el riesgo que buscamos evitar.**

«Los ciberdelincuentes aprovechan la situación actual donde todavía un gran porcentaje de la validación de identidad de los usuarios depende de contraseñas, ejecutando diversos ataques logrando robar las credenciales y suplantar la identidad del usuario. Si se considera la premisa que las credenciales pueden ser robadas de alguna forma, llegaremos a la conclusión que es obligatorio adoptar tecnologías donde se debe validar al usuario de múltiples formas, como el doble factor de autenticación o la seguridad biométrica», afirma

Alejandro Botter, gerente de ingeniería de Check Point para el sur de Latinoamérica

Según el Informe de Investigaciones de Filtraciones de Datos de Verizon (2024), **el 81 % de las filtraciones aún involucran contraseñas débiles o robadas.** A medida que los actores de amenazas evolucionan y la IA se convierte en parte de sus herramientas, incluso las contraseñas más seguras pueden descifrarse en minutos, no en meses. Es hora de preguntarnos: ¿nos aferramos a un método de seguridad obsoleto que nos frena?

El problema de las contraseñas hoy

Los datos son contundentes. Según Nordpass, la **contraseña débil «123456» persiste como contraseña**, siendo fácilmente descifrada en un segundo por hackers. Una encuesta de seguridad en línea realizada por Google y Harris Poll en febrero de 2019 reveló que al menos el 65 % de las personas reutilizan sus contraseñas en varios sitios, si no en todos, lo que las expone a ataques de robo de credenciales a gran escala.

Las nuevas amenazas solo están acelerando este riesgo. Los ataques de fuerza bruta han pasado de las CPU a las GPU de alta velocidad, algunas capaces de adivinar más de un millón de combinaciones de contraseñas por segundo, lo que significa que lo que antes tardaba años en descifrarse ahora se puede hacer en minutos utilizando herramientas mejoradas con IA.

La economía del cibercrimen

El mercado negro de credenciales robadas es vasto y lucrativo. **Se estima que más de 24 600 millones de combinaciones de nombre de usuario y contraseña circulan actualmente en los mercados cibercriminales**, aunque la escala real es difícil de verificar debido a la reventa repetida de

datos robados. En grandes cantidades, estas credenciales son incluso más baratas, como se vio en la estafa de Booking.com, donde se vendieron miles por tan solo 2000 dólares y se ofrecían nuevas credenciales cada mes, dependiendo de las brechas de seguridad y las filtraciones. Los inicios de sesión más valiosos incluyen cuentas bancarias, de correo electrónico, en la nube, de criptomonedas, de VPN corporativas y de redes sociales, que se reutilizan comúnmente para phishing, robo de identidad, campañas de malware y la vulneración de correos electrónicos empresariales.

Detrás de estos robos se encuentran algunos de los grupos de amenazas más sofisticados del mundo, como Kimsuky (Corea del Norte), MuddyWater (Irán) y APT28/29 (Rusia), que a menudo utilizan malware como las plataformas Lumma y MaaS, atacando tokens MFA y monederos de criptomonedas, y propagándose a través de bots de Telegram, lo que permite que el robo de información sea escalable y rentable. Se informó que, solo en 2024, 3900 millones de credenciales se vieron comprometidas mediante infecciones de malware en 4,3 millones de dispositivos.

Incluso la autenticación multifactor (MFA), aunque crucial, se ve comprometida por herramientas como EvilProxy, que puede interceptar tokens MFA. Esta creciente economía del cibercrimen no es solo una amenaza técnica, sino un ecosistema geopolítico y económico, ya que estas amenazas ahora pueden provenir de cualquier lugar gracias a las plataformas MaaS y Phishing como servicio (PhaaS). Junto con el robo de información como servicio y los kits de phishing de alquiler, estos ataques ya no se limitan a actores estatales; están disponibles para cualquiera con una billetera Bitcoin.

El auge de la autenticación sin

contraseña

En contraste, la seguridad sin contraseña no solo es posible, sino también práctica. Empresas como Google, Microsoft y Shopify están implementando claves de acceso: claves criptográficas cifradas vinculadas a la autenticación biométrica o basada en dispositivo.

Microsoft quiere que sus más de mil millones de usuarios dejen de usar contraseñas para iniciar sesión en sus cuentas de Microsoft, mientras que Gartner predice que el 60 % de las empresas las eliminarán para la mayoría de los casos de uso para 2025.

En sectores como las finanzas, la salud y la administración pública, los tokens de hardware, los inicios de sesión multifactor y la identificación biométrica están tomando la delantera. Incluso en países como Singapur e India, los sistemas de identidad digital respaldados por el gobierno están acelerando la adopción de la autenticación sin contraseña para el acceso a la banca, los seguros y la atención médica. Esto se debe al deseo de mejorar la seguridad, optimizar la experiencia del usuario y agilizar las interacciones digitales.

En Singapur, por ejemplo, el sistema de Identidad Digital Nacional (NDI), basado en Singpass, conecta a más de 700 agencias gubernamentales y empresas privadas.

Opciones como el reconocimiento facial, las tarjetas de identificación digital y los códigos QR confirman la identidad del usuario rápidamente y son más seguras que las contraseñas tradicionales. Aadhaar de India, el sistema biométrico más grande del mundo, admite la verificación segura de la identidad digital mediante OTP y biometría, mientras que la hoja de ruta de la identificación digital de Australia invierte en marcos federados sin contraseñas.

¿Por qué seguimos aferrándonos a las contraseñas?

A pesar de los avances en seguridad, las personas aún confían en lo que saben y las contraseñas nos resultan familiares. Pero esa familiaridad tiene un precio. Las contraseñas son fáciles de adivinar, olvidar, compartir o robar.

Check Point señala que la mala higiene de las contraseñas (como reutilizarlas, anotarlas o usar datos personales) sigue siendo un punto débil importante en la seguridad corporativa y personal.

Peor aún, los ataques de phishing (muchos generados por IA) continúan robando credenciales de inicio de sesión a gran escala, a pesar de la presencia de la autenticación de dos factores (2FA). El aumento de los ataques de phishing y deepfake impulsados por IA solo aumenta la vulnerabilidad de los sistemas basados en contraseñas.

Riesgos de usar contraseñas en un mundo pos IA

- La evolución de la IA está dejando obsoleta la autenticación basada en contraseñas:
- Los modelos de aprendizaje profundo se entrenan con miles de millones de contraseñas filtradas y pueden predecir patrones comunes más rápido que nunca.
- Los ataques de suplantación de identidad por voz y vídeo que utilizan deepfakes pueden eludir incluso la autenticación multifactor si se basan en capas de identidad débiles.
- Las GPU basadas en la nube están democratizando la capacidad de descifrar contraseñas a gran escala, lo que permite que grupos de ransomware y script kiddies comprometan los sistemas rápidamente.

En resumen: cuanto más esperemos para prescindir de las contraseñas, más nos exponemos.

Qué deben hacer ahora las organizaciones

- Probar sistemas sin contraseñas utilizando biometría, tokens o claves de acceso.
- Utilizar herramientas como Check Point Harmony para evitar la reutilización de contraseñas y el phishing.
- Implantar soluciones de Gestión de Acceso Privilegiado (PAM) y arquitecturas de Confianza Cero.
- Capacitar a los equipos no solo sobre contraseñas más seguras, sino también sobre su eliminación gradual. Check Point enfatiza la longitud, diversidad y singularidad de las contraseñas, pero también está alineado con la necesidad de explorar enfoques posteriores a las contraseñas.

El Día Mundial de la Contraseña no debería centrarse únicamente en crear contraseñas más seguras. Debería ser un incentivo para imaginar un futuro sin ellas. Las herramientas existen. Las amenazas lo exigen. Lo único que falta es nuestra disposición a renunciar a ellas.

Fuente: Ámbito Financiero.