LITORALPRESS

Fecha: 30-05-2025
Medio: El Mercurio
Supl. : El Mercurio - Chile Tecnológico
Tipo: Columnas de Opinión
Título: COLUMNAS DE OPINIÓN: Repensando la autenticación digital

Pág. : 10
Cm2: 577,2

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

COLUMNA DE OPINIÓN

Repensando la autenticación digital

MAURICIO FIERRO,
líder de Ciberseguridad de IBM Consulting Chile

Los esquemas de validación de identidad o autenticación digital generan una gran carga en los hombros de las personas. Desde memorizar múltiples contraseñas hasta navegar en procesos de autenticación de dos pasos, la seguridad de las cuentas recae en los usuarios, quienes se convierten en un objetivo de los ciberdelincuentes. De hecho, uno de cada tres ciberincidentes resultó en el robo de identidad en el último año.

Si bien la educación en seguridad ayuda, no puede evitar que las personas sean engañadas con tácticas de ingeniería social (que además están en constante evolución o usan IA) para que entreguen sus credenciales, es decir, sus nombres de usuario y contraseñas. Entonces, está claro que el problema no está en las personas, sino en los esquemas que las colocan en el último eslabón, el más expuesto.

Ante este escenario, ¿cómo se puede repensar la autenticación? Estos son tres métodos que considerar:

AUTENTICACIÓN BASADA EN RIESGOS

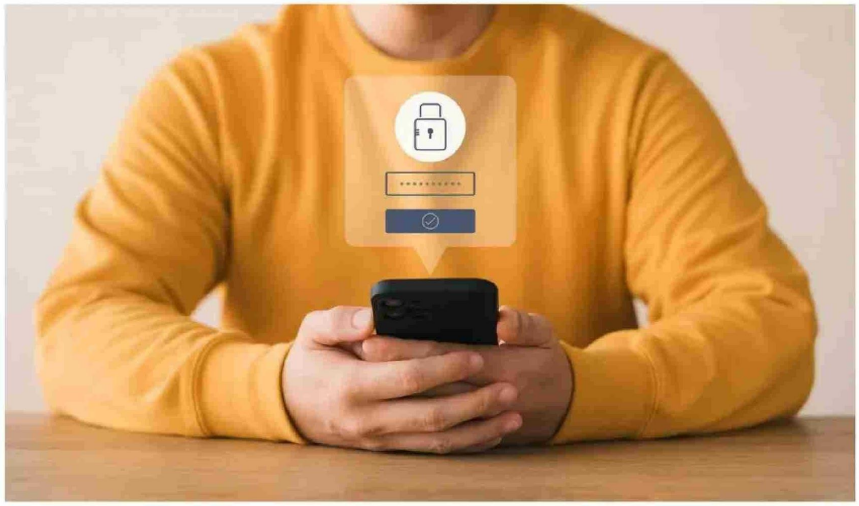
Este método ajusta dinámicamente las medidas de seguridad en función de factores contextuales como la ubicación del usuario, el dispositivo utilizado e incluso la biometría del comportamiento. De esa manera, las organizaciones pueden entender mejor los intentos de inicio de sesión, reducir los falsos positivos e identificar y mitigar eficazmente las actividades de alto riesgo.

AUTENTICACIÓN CONTINUA

Este método mantiene una evaluación constante de la identidad del usuario durante toda la sesión que fue iniciada, aprovechando algoritmos de aprendizaje automático para adaptar con precisión las políticas de acceso que tiene el usuario a lo largo de su interacción digital, garantizando que cualquier desviación de los patrones normales active controles de seguridad adicionales.

AUTENTICACIÓN SIN CONTRASEÑA (*PASSWORDLESS*)

Este método libera a los usuarios del yugo de pensar, escribir y recordar credenciales diferentes para cada cuenta en línea y elimina la vulnerabilidad más explotada en la cadena de autenticación: las contraseñas. Para iniciar sesión, los usuarios se autentican con datos biométricos como el reconocimiento facial, las huellas dactilares, la biometría del comportamiento o una credencial protegida por *hardware*.



Además de mejorar la seguridad durante el proceso de autenticación, estos métodos también le ayudan a las organizaciones en la era de la inteligencia artificial. Con la llegada de los agentes de IA, se vislumbra un nuevo paradigma en la autenticación con la proliferación de identidades no humanas, pues estos agentes necesitan interactuar con tecnologías para obtener información y realizar acciones en los sistemas.

Hoy, repensar la autenticación no es solo una opción, sino una necesidad. Las organizaciones están en el momento indicado para resolver los desafíos existentes y prepararse para los cambios que vienen con la IA. ¿Estamos listos para abrazar nuevas formas de autenticación? De la respuesta a esta pregunta depende la capacidad para allanar el camino hacia un futuro digital más seguro y eficiente para todos.

> “Si bien la educación en seguridad ayuda, no puede evitar que las personas sean engañadas con tácticas de ingeniería social (que además están en constante evolución o usan IA) para que entreguen sus credenciales”.

> “Con la llegada de los agentes de IA, se vislumbra un nuevo paradigma en la autenticación con la proliferación de identidades no humanas, pues estos agentes necesitan interactuar con tecnologías para obtener información y realizar acciones en los sistemas”.

> “Repensar la autenticación no es solo una opción, sino una necesidad. Las organizaciones están en el momento indicado para resolver los desafíos existentes y prepararse para los cambios que vienen con la IA”.