Autenticación, ¿estás seguro de quién es?

No hay duda de que el aumento de los **ataques informáticos**, sumado a las conductas inseguras de las personas, como el uso de contraseñas débiles e iguales en varios servicios como Facebook, Twitter, LinkedIn, Google y Apple, por ejemplo, hacen **necesario utilizar métodos de autenticación complementarios más robustos.**

Para Sebastián Stranieri, CEO de VU, los números son alarmantes: según un estudio realizado por McKinsey, 81% de los *breaches* de seguridad se dan por **contraseñas débiles o robadas.** A raíz de esto, tanto empresas como entidades gubernamentales, han comenzado a implementar estrategias de segundo factor de autenticación para robustecer el acceso a información sensible.

El segundo factor de autenticación es un sistema que complementa la autenticación tradicional en los servicios que requieren credenciales de acceso con un factor de autenticación adicional como un **código de seguridad**, una clave de única vez, que puede ser generada desde una aplicación en un dispositivo móvil o bien recibida por SMS/Email, los más avanzados utilizan notificaciones push para enviar dichos códigos u operaciones de validación.

“No importa el orden que elija la empresa para autenticar, siempre y cuanto se utilicen dos factores para validar que la persona es quien dice ser. Los sistemas de autenticación se dividen en simple factor, que es algo que el usuario recuerda como una contraseña, su fecha de nacimiento, etc. El doble factor es algo que el usuario posee: su teléfono, un número de teléfono, una tarjeta, etc.

“Existe un tercer factor que es algo que **el usuario es en si mismo,** como su rostro, voz, huella dactilar. La principal ventaja de utilizar este doble factor es el punto extra de seguridad que damos a nuestra cuenta personal, ya que siempre será más seguro que utilizar únicamente un usuario y contraseña”, explicó Stranieri .

¿Por qué implementarlo?

Teniendo en cuenta que los usuarios manejan cada vez más información sensible en sus cuentas, resulta lógico que los **cibercriminales** destinen mayores recursos al robo de las contraseñas que la protegen.

Según un informe realizado por VU sobre 600 participantes latinoamericanas en 18 países de la región, 29% de los encuestados indicó que lo que genera más posibilidades de violación de seguridad es compartir contraseñas y claves de acceso.

“Ahora bien, si los usuarios conocen este riesgo, ¿por qué toman esta conducta? Simplemente, porque suelen estar desbordados por la **cantidad de usuarios y contraseñas**, y las anotan, comparten, y repiten con el objetivo de no olvidarlas.

“Lo cierto es que debido a **diversos ataques que involucran el robo de contraseñas**, y que han afectado a importantes empresas, muchas corporaciones privadas y organismos del Estado han tomado la decisión de implementar sistemas de doble autenticación para contribuir a la seguridad y protección de la información de sus usuarios”, agregó Stranieri.