El mundo al revés

¿Qué pensarías de mi si te dijera que un PIN (ya sabes, un código generalmente numérico) es más seguro que una contraseña (un código alfanumérico)? Que estoy loco, ¿verdad? Que incluso aunque tuvieran ambos el mismo número de caracteres, las posibles permutaciones de contraseñas son, claramente, de unos cuantos rangos superiores a las que podemos obtener si reducimos el conjunto de caracteres únicamente a los números del 0 al 9, como suele ocurrir con el PIN... Y vaya, ahí tengo que darte la razón.

Lo que quizás estés obviando es que la robustez de un sistema de identificación no solo se basa en su fortaleza frente a ataques de fuerza bruta (ya sabes, lo típico de ir probando 0000, 0001, 0002... hasta que demos con el PIN que ha usado el usuario), sino en una muy dilatada amalgama de vectores de ataque y riesgos del propio ecosistema (el digital), que es lo que me lleva a decir con total tranquilidad que en algunas ocasiones, el PIN es más seguro que una contraseña.

Y esto es justo lo que ocurre en Windows10, por cierto.

Desde hace unos cuantos meses Microsoft anda lanzando la monserga marketiniana de que quiere hacer nuestros dispositivos «Passwordless», es decir, libres de contraseñas.

Por supuesto la alternativa que a muchos se nos viene a la mente para conseguir tal manida Odisea pasa por forzar el uso de Windows Hello y sus sistemas de identificación basados en la biometría. A fin de cuentas, la seguridad de un sistema biométrico, por la propia complejidad del sistema de verificación que hay detrás (difícilmente un usuario de la calle va a poder emularlo en su casa sin conocimientos y sin recursos) ya sirve de desincentivo para los interesados en lo ajeno.

Sin embargo, la propuesta de Microsoft no es solo que deleguemos nuestra seguridad en un sistema biométrico, que como ya sabrás entraña sus propios riesgos (una contraseña/PIN robada puedes cambiarla y ya está, una huella dactilar o un iris robado no lo puedes cambiar, ya que pertenece a una parte de tu propio cuerpo que por razones obvias no es intercambiable), sino que aseguran que su sistema de identificación basado en PIN es más seguro que cualquier contraseña.

PIN vs. contraseña

¿Tiene sentido considerar un PIN más seguro que una contraseña alfanumérica?

Partiendo de la base de que un PIN no deja de ser una contraseña con un subconjunto de caracteres mucho más bajo, a priori parece algo absurdo. Es más, la mayoría de PINs se pueden descubrir por fuerza bruta (en sistemas desprotegidos, claro) en apenas unos minutos.

Sin embargo Microsoft agrega un matiz, y es que su PIN se gestiona únicamente en local.

El sistema de login tradicional (usuario y contraseña) está asociado a nuestra cuenta de Microsoft, que por supuesto está sincronizada con la nube... y a cuyos permisos probablemente en algún momento hemos dado acceso a algún servicio externo.

Es decir, que al final ese sistema de identificación, pese a ser más robusto frente a ataques puramente locales, es mucho más inseguro frente a ataques masivos (hackeo a una compañía que tenga acceso a nuestra cuenta exponiendo nuestros datos junto con los de millones de usuarios más, por ejemplo).

La robustez de un sistema de identificación no solo se basa en su fortaleza frente a ataques de fuerza, sino en una muy dilatada amalgama de vectores de ataque y riesgos del propio ecosistema digital.

Y sin embargo, el PIN de Windows Hello se gestiona únicamente en local (depende de cada dispositivo), sin compartirse con ninguna nube, sin depender de Internet para confirmar su validación, y sin estar asociado por tanto a nuestra cuenta.

Ergo, pese a ser más débil per sé frente a ataques de fuerza bruta, en la práctica es más seguro que el sistema de contraseñas tradicional, por la sencilla razón, y aquí viene la guinda del pastel, de que resulta más sencillo exponer tu cuenta mediante el hackeo de millones de cuentas (riesgo global) que hacerlo específicamente atacándote a ti (riesgo local).

Y aunque así fuera (alguien accede a tu dispositivo físicamente, por ejemplo robándotelo), ahí está el propio sistema para limitar el alcance de los ataques de fuerza bruta (bloqueos temporales y escalares tras confundirse al meter la contraseña mal unas cuantas veces seguidas).

Y como añadido hay que avisar también que es posible generar PINs alfanuméricos. Así que al final podemos tener el mismo nivel de robustez de una contraseña pero solo almacenada en local. Es decir, bajo la premisa de seguridad offline del PIN de Windows Hello.

Lo mejor de ambos mundos, vaya.

No te acostumbres mucho, que sobre todo en seguridad informática, esto no suele ocurrir muy a menudo. ☺

Pablo F. Iglesias,
Consultor de Presencia Digital y Reputación Online
@PYDotCom

Resulta más sencillo exponer tu cuenta mediante el hackeo de millones de cuentas (riesgo global) que hacerlo específicamente atacándote a ti (riesgo local).