Mobile Connect

En el post anterior hablaba de los diferentes riesgos y amenazas que existen y como afectaban a las organizaciones. Además, durante los anteriores posts hemos estado viendo como las contraseñas son una de las cosas más complicadas, ya que los usuarios pueden abandonar o dejar de utilizar los servicios que ofrece una compañía por el simple hecho del olvido de las mismas o por considerar que son poco seguras.

En el apuro por abrir nuevos canales digitales, las empresas no pueden darse el lujo de perder de vista la necesidad de identificar y conectarse con aquellos individuos que usan una enorme cantidad de dispositivos móviles. El dominio de las identidades digitales puede transformar la posición de una organización en la economía digital. La simple verdad es esta: las empresas que logren aprovechar el tema de la identidad podrán sacar poderosos productos y servicios con más rapidez y efectividad que las que no lo logren. Un estudio de Oracle descubrió que casi dos tercios (64%) de los encuestados

dice que los canales digitales son altamente importantes para los ingresos de sus compañías (el 27% piensa que son fundamentales para la misión y el 37% que son muy importantes). 72% dice que el tema de la seguridad es el principal peligro para manejar la identidad personal y solo el 19% está muy bien preparado para cumplir con los requisitos de seguridad. Permitir que los clientes controlen sus propios datos de identidad es considerado como una medida altamente eficaz para el 48% de los adoptantes. [1]

Según diferentes líderes en seguridad biométrica, para 2020 las contraseñas desaparecerán en países que realicen altas inversiones en mecanismos robustos de seguridad. [2] Y según la Asociación de operadores móviles y compañías relacionadas (GSMA), actualmente los gobiernos y empresas están buscando una autenticación más fuerte para reducir los riesgos, especialmente en los dispositivos móviles. Cuentan con un programa llamado Vision 2020 que tiene como objetivo encontrar una solución de autenticación basada en la red móvil para abolir el uso de contraseñas y dar paso a la autenticación digital desde dispositivos móviles. [2] Según datos de GSMA, el 87% de las personas abandonan los sitios web cuando se les pide que se registren, el 40% admite haber utilizado la función de “recuperar contraseña” al menos una vez al mes, y el 83% de los usuarios están preocupados por el uso de su información personal cuando acceden a Internet o a las apps. [3]

El Grupo de Trabajo Técnico y Terminales (TECT) de GSMA Latino América se

reunió en marzo del año pasado en Río de Janeiro, Brasil, y sirvió como catalizador para seguir actualizando a los operadores móviles en los temas técnicos que la GSMA impulsa a nivel global. El encuentro atrajo a más de 60

ejecutivos de las áreas de las operadoras y los principales fabricantes del ecosistema móvil latinoamericano. Se habló sobre distintos temas, pero el que a nosotros nos importa es el seminario de servicios de identidad, en el cual se dio a conocer el Mobile Connect. Se trata de un servicio de autenticación que los operadores han lanzado en todo el mundo que pretende dar una alternativa a los numerosos usuarios y contraseñas del mundo digital. Además, se revisaron las evoluciones del servicio para dar servicios de autorización, atributos, pagos o identidad. [4]

Hoy en día muchas compañías telefónicas ofrecen el uso de esta tecnología de una forma gratuita y segura, simplemente tendrás que recordar tu número de teléfono para poder loguearte en todo tipo de páginas webs y apps, sin necesidad de recordar contraseñas. [5]

La inquietud que me surge es que si los mecanismos de autenticación más seguros son los biométricos (huellas, voz, etc.) y los menos seguros los basados en “algo que tú sabes o tienes” (contraseñas, tarjeta de proximidad, etc.). ¿Cómo sabemos que este método es seguro, si se trata de un mecanismo de autenticación basado en algo que tú tienes (el móvil)? Es decir, si en algún momento pierdo el móvil o me lo roban, pierdo esa seguridad y cualquiera podría entrar a cualquier portal que pueda activar con mi dispositivo. ¿No debería tener una estrategia de doble autenticación? En cualquier caso, me parece una buena idea siempre que las páginas que necesiten un grado más elevado de seguridad lo combinen con otros mecanismos de autenticación.

Referencias

[1] Mercado. <<El gran problema de la identidad digital>>. Acceso el 31 de octubre de 2017. http://www.mercado.com.ar/notas/8019653

[2] Reporte digital. <<Autenticación digital, la tendencia que revoluciona la identidad digital>>. Acceso el 31 de octubre de 2017. http://reportedigital.com/seguridad/autenticacion-digital-identidad/

[3] El País. <<Movistar lanza el servicio que elimina las contraseñas para registrarse>>. Acceso el 1 de noviembre de 2017. https://elpais.com/economia/2016/04/14/actualidad/1460620789_925132.html

[4] GSMA. <<Reunión del TECT en Brasil: trabajo conjunto para traer la estrategia Vision 2020 de la GSMA a América Latina>>. Acceso el 1 de noviembre de 2017. https://www.gsma.com/latinamerica/es/reunion-del-tect-en-brasil-trabajo-conjunto-para-traer-la-estrategia-vision-2020-de-la-gsma-a-america-latina

[5] Orange. <<Mobile Connect: La solución universal, segura y cómoda para registrarse sin contraseñas>>. Acceso el 1 de noviembre de 2017. http://mobileconnect.orange.es/