Diego Espitia: Autenticación de dos factores, medida para proteger la información

En nuestros días tener la garantía de que nadie tiene acceso a tus servicios en Internet es una necesidad que se valora más. Sin embargo, las cifras de ataques cibernéticos evidencian que esto no siempre se tiene asegurado, sobre todo en lo que respecta a herramientas de comunicación como el correo electrónico que utilizamos diariamente y que contiene información sensible propia y de terceros.

El correo electrónico es la principal arma de ataque de los grupos de delincuentes, donde el 94% del malware que se envía en un día, utiliza este mecanismo para propagarse y generar perdidas muy importantes en las empresas, como lo demuestra el estudio de IC3 (Internet Complaint Center) en el 2020. Los ataques de BEC (Business Email Compromise) y EAC (Email Account Compromise) generaron pérdidas por $1800 millones de dólares en el 2020.

El estudio de GreatHorn en el 2021 también evidencia un crecimiento en ataques que tienen como objetivo comprometer las cuentas, pasando del 8% de los incidentes en el 2020 al 10% en el 2021.

Esta situación conllevó a que Google, una de las empresas más grandes de tecnología, publicar oficialmente que el futuro de su plataforma sería sin contraseñas en mayo del 2021. Con esta comunicación, la empresa hizo un cambio en la plataforma

forzando a los usuarios a usar el 2FA (Doble Factor de Autenticación), una iniciativa similar se promueve en Telefónica desde 2016.

Esta medida ha mostrado frutos en menos de un año, como lo ha demostrado Google en su blog oficial a propósito del Día del Internet Seguro , indicando que las cuentas comprometidas en ataques cibernéticos se redujeron en un 50% tras la aplicación de esta medida simple.

Como siempre en seguridad nada ni nadie puede garantizar que no se pueda comprometer las cuentas que tienen habilitado el 2FA, incluso se han publicado hasta 5 métodos de romper la seguridad de esta medida, donde uno de ellos afecta directamente el control más robusto que ofrece Google, que son las llaves seguridad titan.

A pesar de esto, la medida mitiga casi en su totalidad los ataques directos a las cuentas de correos empresariales, los cuales no solo se ven afectados por intentos de phishing sino por las fugas de información, aumentando la probabilidad de que la contraseña sea comprometida y usada en ataques más dañinos para las empresas como el Ransomware.

Cabe resaltar que, el uso del 2FA se puede aplicar en casi todos los servicios que usamos en internet, como las redes sociales, correos electrónicos, billeteras de criptomonedas, plataformas de pago y otros. Además, existen varias formas de utilizar esta medida, como en las siguientes:

- **Los SMS:** Este es el método usado por varios servicios, pero es el menos seguro de los sistemas de 2FA, porque los SMS no fueron diseñados para autenticar al usuario, sino que se asocia con el identificador del móvil y es muy factible a ataques de SIM Swap.

- **El correo electrónico:** Este método es muy útil para servicios a los que se accede desde un dispositivo diferente a donde se tiene el correo, con el fin de agilizar la carga de código enviado. Aunque es más confiable hay que tener en cuenta que los ataques de terceras partes suelen acceder a correo para obtener estos códigos.

- **Aplicación de Autenticación:** Al basarse en un protocolo y garantizar la autenticación del usuario al acceder al dispositivo, es uno de los mecanismos más seguros en sus formas de TOTP (Time based One Time Password) y en HOTP (Hash based One Time Password) y existen varias aplicaciones móviles que pueden usar para esto, como LATCH e integrar en estas todas las cuentas de servicios en Internet.

- **Llaves Físicas:** Sin duda es el mecanismo más seguro pues si no se coloca el hardware en el equipo donde se va a usar el servicio, no es posible acceder a los servicios.

Sin duda cualquiera de los métodos que se use, sirve para mejorar la seguridad de todos los servicios en línea a los que se esté inscrito y permite mitigar los ataques empresariales.

Telefónica Tech es la empresa líder en transformación digital. La compañía ofrece una amplia gama de servicios y soluciones tecnológicas integradas en Ciberseguridad, Cloud, IoT, Big Data y Blockchain. Para más información, visite: https://tech.telefonica.com/. En Perú, Telefónica Tech ofrece sus servicios y capacidades a través de Movistar Empresas.