Métodos de autenticación fuerte: ¿Está usted detrás de la curva?[1]

Si los usuarios no pueden recordar sus contraseñas, considérelo una señal positiva. En 2015, el fútbol, el béisbol, y varias referencias a Star Wars encabezaron la lista de las peores 25 contraseñas, según SplashData, junto con los favoritos de siempre: 123456 y contraseña.

Pero más allá de eso, ¿por qué las empresas siguen teniendo esta discusión? Los nombres de usuario y contraseñas, por sí solos, son una forma vulnerable de autenticación. Las contraseñas se olvidan, se escriben, y se dan a conocer sin querer a los phishers adeptos a la elaboración de señuelos de correo electrónico. La autenticación de múltiples factores (MFA) –que requiere la verificación a partir de dos o más credenciales independientes como una contraseña, token de seguridad o identificación biométrica– puede ofrecer más capas de defensa, pero todavía no es la norma. ¿Por qué no hay más empresas que adopten métodos de autenticación fuerte? La respuesta puede estar en la incertidumbre acerca de las mejores opciones tecnológicas, las estrategias y los costos de implementación.

Consideraciones estratégicas

Comience por comprender su caso de uso. ¿La base de usuarios es pequeña y se concentra en un pequeño conjunto de aplicaciones? Un equipo legal dentro de una gran empresa puede tener que hacer frente a grandes volúmenes de información confidencial almacenada en los sistemas de gestión de documentos y las aplicaciones de descubrimiento electrónico (e-discovery). Una empresa puede decidir que quiere usar, comprar y distribuir un número limitado de dispositivos de hardware para la generación de contraseñas de una sola vez (OTP). Un pequeño número de usuarios que tratan con datos muy valiosos puede justificar enfoques más costosos que otros escenarios.

Por otra parte, para las empresas que proporcionan software como servicio (SaaS) o que tienen un gran número de empleados que utilizan métodos de autenticación fuerte puede no resultar práctico utilizar hardware especializado y en vez de ello optarán por aplicaciones para dispositivos móviles.

Considere cómo la autenticación fuerte funcionará con su infraestructura de autenticación y gestión de identidad existente. Por ejemplo, si su empresa tiene Active Directory Federation Services en Windows Server 2012, puede utilizar la autenticación de certificados o un servicio de terceros, como el agente de autenticación RSA SecurID para Microsoft Active Directory Federation Services o el servicio de validación y protección de identidades de Symantec (VIP).

Los proveedores de la nube, como Amazon Web Services y Microsoft Azure, son cada vez componentes más importantes de la infraestructura empresarial. Idealmente, un fuerte mecanismo de autenticación funcionará tanto en las instalaciones como en plataformas en la nube. Tenga cuidado con la necesidad de soportar varias aplicaciones MFA, como el VIP de Symantec para los sistemas informáticos locales y Google Authenticator para la autenticación de múltiples factores de AWS.

1 http://searchdatacenter.techtarget.com/es/cronica/Metodos-de-autenticacion-fuerte-Esta-usted-detras-de-la-curva

Los servicios de inicio único de sesión (SSO), como Okta y OneLogin, proporcionan beneficios de SSO en entornos de nube y SaaS. Tenga en cuenta cómo se integrará MFA con un organismo de normalización si utiliza uno. ¿Su proveedor de SSO respalda el sistema de MFA elegido? ¿Desea implementar MFA a través del proveedor de SSO si sólo una aplicación garantiza la MFA? Esta pregunta puede ser especialmente importante de realizar si sólo un pequeño número de usuarios necesitan acceder a aplicaciones y datos sensibles que requieren MFA.

Es una práctica bien entendida en la seguridad evitar algoritmos propietarios relacionados con el cifrado. Favorezca los métodos que se basan en normas públicas, que hayan sido objeto de una revisión rigurosa. Los algoritmos propietarios pueden albergar vulnerabilidades imprevistas.

La autenticación de múltiples factores será nueva para muchos usuarios que se han acostumbrado a trabajar con nombres de usuario y contraseñas. Ellos pueden no estar familiarizados con las aplicaciones y dispositivos MFA, por lo que los escritorios de soporte deben estar preparados para las llamadas de asistencia. Guías y tutoriales bien desarrolladas sobre un portal de autoservicio pueden ayudar a reducir la posibilidad de un aumento en las llamadas al centro de soporte.

Una estrategia MFA complementa las contraseñas, no las reemplaza. Todavía es importante hacer cumplir las políticas de contraseñas fuertes. Estas políticas deben incluir la reducción de la vida útil de las contraseñas, longitud mínima y la variedad de caracteres, límites de reutilización y así sucesivamente.

La autenticación fuerte debe ser parte de un amplio conjunto de prácticas de seguridad de la información que incluyen funciones de separación y rotación, monitoreo y registro de eventos en sistemas de gestión de identidades así como la realización de auditorías de rutina.

Tecnologías de autenticación

Los métodos de autenticación fuerte implican típicamente OTP generadas dinámicamente o autenticación basada en certificados y en contextos.

El OTP emplea un dispositivo de seguridad en posesión del usuario y un servidor back-end. El dispositivo de seguridad puede estar basado en hardware, como por ejemplo un llavero de control remoto a prueba de manipulaciones, o basado en software, como por ejemplo, una aplicación de teléfono móvil. Las contraseñas de un solo uso pueden suministrarse también a teléfonos móviles que utilizan SMS. Ambos tipos dispositivos de usuario comparten un secreto con el servidor back-end de autenticación. El secreto se utiliza para generar una OTP limitada en el tiempo. Los dispositivos basados en software tienen la ventaja de una distribución más fácil. Los usuarios simplemente tienen que descargar una aplicación, y las empresas no tienen la sobrecarga de administración del inventario físico de los llaveros.

Hay dos formas comunes para la generación de OTP: basados en tiempo y basados en algoritmos. Los que están basados en el tiempo utilizan el tiempo, junto con un secreto compartido o token, para generar una contraseña. El algoritmo de contraseñas de una sola vez basado en tiempo es un estándar IETF para la generación de contraseñas de vida corta y de una sola vez. Los algoritmos no basados en tiempo empiezan con una función hash y un valor de semilla para generar contraseñas. Después de que se genera la clave de acceso inicial, la contraseña anterior se utiliza como entrada para generar la siguiente contraseña. Otras normas OTP incluyen la S/KEY One-Time Password System (RFC 1760), el sistema de contraseñas de una sola vez (RFC 2289) y el algoritmo de contraseñas de una sola vez basado en MAC.

La autenticación basada en certificados emplea criptografía de clave pública para generar las claves públicas y privadas. Las claves privadas se pueden almacenar en un dispositivo portátil, como una unidad USB, o almacenarse de forma segura en la computadora de un usuario. El uso de un dispositivo basado en USB mitiga el riesgo de que un usuario asegure incorrectamente un archivo de clave privada, pero añade la sobrecarga de administración de otro dispositivo físico.

La autenticación basada en el contexto utiliza la información sobre un usuario, como la ubicación geográfica, para autenticarlo. Este tipo de autenticación se utiliza generalmente en conjunción con otros métodos de autenticación. Para entornos de alta seguridad, por ejemplo, se puede requerir que un usuario proporcione un nombre de usuario, contraseña, OTP y pase una verificación de la ubicación geográfica del dispositivo que inicia la sesión. Otras técnicas incluyen el registro del dispositivo o las huellas dactilares, la reputación de la dirección IP de origen y análisis del comportamiento.

Errores que deben evitarse

La tecnología de autenticación no existe en el vacío. Independientemente del rigor matemático detrás de un método de autenticación, una vez que se implementa –y que funciona en la compleja mezcla de usuarios, aplicaciones e infraestructuras– se introducirán vulnerabilidades. Por ejemplo, Trend Micro documentó el caso de ataques a los clientes de bancos europeos que fueron atraídos a descargar una aplicación maliciosa supuestamente diseñada para generar OTP para sus cuentas bancarias en línea.

La educación de los usuarios finales es esencial y se extiende desde instruir a los usuarios sobre cómo instalar una aplicación OTP para evitar introducir un una OTP en un sitio web sospechoso.

Al igual que con cualquier inversión en TI, los métodos de autenticación deben justificarse sobre la base de que los beneficios son superiores a los costes. Las aplicaciones que gestionan la información a disposición del público no pueden presentar un caso fuerte para la inversión en tecnología de autenticación fuerte. Los sistemas financieros, bases de datos de asistencia sanitaria y otras aplicaciones de gestión de información privada y protegida son los mejores candidatos para el despliegue inicial de la MFA.

El costo de los sistemas MFA ha sido un obstáculo para la adopción. Sin embargo, el empuje hacia la consumerización de métodos de autenticación fuerte puede cambiar la estructura de costos. La Alianza Nacional de Seguridad Cibernética está trabajando con proveedores de servicios de consumo, tales como Google, Dropbox, Microsoft y Facebook para promover mejores prácticas para asegurar las cuentas en línea.

La autenticación de múltiples factores es una práctica de seguridad bien establecida. Aunque existen desafíos para implementar y mantener sistemas de MFA, éstos proporcionan ventajas significativas sobre los mecanismos de autenticación por contraseña única. A medida que los servicios de consumo de las principales compañías de internet y las empresas de servicios financieros presionan por el uso de la MFA, el costo de la tecnología de autenticación puede caer. Al mismo tiempo, la conciencia de los usuarios finales acerca de la necesidad de una autenticación fuerte y el entendimiento de cómo usarlo aumentará. El balance de costos y beneficios está claramente a favor de métodos de autenticación fuerte para muchos casos de uso empresarial.

Como la seguridad de cuentas de usuario puede evitar los ataques de recuperación de contraseña[2]

Muchos profesionales de seguridad de la información piensan que los atacantes normalmente se dirigen a las personas o páginas de mayor valor a la hora de realizar sus ataques – y dados los controles de seguridad, procesos y la forma en que ocurren esos ataques – los fraudes pueden tener éxito.

No importa cuán fuerte sea la contraseña… si la empresa tiene un proceso de recuperación de contraseña débil, ya que los hackers pueden comprometer todo el sistema.

Y por desgracia para el CEO de CloudFlare Inc. esto se ha convertido en realidad. CloudFlare usa cuentas de Gmail de Google Inc. para acceder a las Apps de Google y gestionar los datos sensibles de las ofertas de CloudFlare. A través de una serie de ataques planificados, un atacante consiguió el control de la cuenta del CEO desde la que inicio el ataque y pudo tener acceso a la información de uno de los clientes de CloudFlare. Sin lugar a dudas este es uno de los peores momentos para una organización.

Entonces ¿Cómo ha sido posible que los controles de autentificación, las contraseñas seguras empeladas en los correos y los servicios de uno de los mayores proveedores en la nube hayan fallado? La realidad es que el problema reside en el proceso de recuperación de contraseñas. Por eso dedicamos este consejo a ver cuáles fueron los pasos de los atacantes y como pueden protegerse adecuadamente esos datos.

Seguridad en cuentas de usuario: errores y prácticas recomendadas

El primer paso del atacante fue dar con la cuenta de Gmail del CEO; esto le permitió obtener acceso no solo a su correo sino también a las herramientas de Google Apps con solo logarse en el sistema. Puesto que la mayor parte de las páginas web empresariales incluyen el nombre de sus ejecutivos y dado que muchas empresas usan correos vinculados al nombre del ejecutivo (p.e., jsmith@gmail.com o john.smith@gmail.com), con el envío de algunos correos basados en las variaciones del nombre de la persona pueden ser suficientes para descubrir su correo. Con esto empieza el proceso

Este problema puede evitarse a través de dos acciones. Puesto que la mayor parte de sistemas de mensajería empresarial cuentan con directorios o paginas blancas, no es preciso dar a conocer a cada empleado la dirección de sus compañeros. Además también se debería dejar de lado esa forma de crear correos corporativos. Una solución sería usar las iniciales del empleado acompañado de cuatro o cinco números aleatorios (p.e., jps29581@gmail.com) lo que dificulta notablemente el phishing. Para los sistemas que usan las cuentas de correo como credenciales para acceder a datos sensibles, como Google Apps, la segunda forma de evitar que el atacante obtenga acceso a tales

2 http://searchdatacenter.techtarget.com/es/consejo/Como-la-seguridad-de-cuentas-de-usuario-puede-evitar-los-ataques-de-recuperacion-de-contrasena

datos es usar una cuenta de correo para el mundo en general y otra diferente para los accesos sensibles. Incluso en los entornos en la nube, el hecho de tener una cuenta de correo que no esté asociada con la persona puede ser útil para evitar que un atacante descubra (seguramente comprometa) esa cuenta. En el caso de CloudFlare tener una cuenta de correo como jps2958@gmail.com y otra cuenta aparte como torbox3953@gmail.com para acceder a Google Apps podía haber evitado que el atacante identificase las cuentas de correo con las del CEO.

Cuando la recuperación de contraseñas falla

Una vez que el atacante conoce la cuenta de correo del CEO de CloudFlare contacta con el soporte al cliente de Google para recuperar su contraseña. Después de semanas de intentos el atacante es capaz de convencer al sistema de recuperación de contraseñas de Google para añadir un correo electrónico de recuperación, lo que permite al atacante cambiar la contraseña de la cuenta de Gmail del CEO y acceder a su contenido.

No importa cuán fuerte sea la clave (en este caso más de 20 caracteres aleatorios) si la empresa dispone de un sistema de recuperación de contraseñas débil los atacantes pueden acceder al sistema mediante el uso de detalles personales, sin necesidad de “reventar” una contraseña fuerte. Solo tienen que cambiarlo. Por ejemplo si la respuesta a la pregunta de seguridad es algo sencillo o algún detalle conocido de la persona. Con Facebook, LinkedIn y otras redes sociales almacenando grandes cantidades de datos personales los empleados pueden, sin querer, hacer públicos los datos de toda su vida al público en general: nombres de mascotas, de escuelas y universidades, nombres de niñeras y otros muchos detalles personales que son muy fáciles de encontrar en la red. Esto supone que las formas más potentes de identificación, como la autentificación biométrica, sería lo que realmente necesita Internet para poder proteger la integridad de los datos, sobre todo a medida que las empresas están cada vez más expuestas en la red o, como en el caso de cloudFlare se usan servicios en la nube.

Para la mayor parte de los ataques en Internet, estos tres pasos serian suficientes para evitarlos. Pero en el caso de la cuenta de CloudFlare, esta contaba con doble autentificación. Esto solo muestra cuán sofisticado, inteligente y decidido era el atacante. Para poder acceder y resetear la cuenta de Gmail del CEO el atacante tuvo que lograr acceso al número PIN… que fue enviado a la cuenta de correo móvil de AT&T del CEO.

El atacante también fue capaz de superar este reto. Según apuntan las investigaciones el atacante fue capaz de llamar a AT&T y hacerse pasar por el CEO. Aunque el atacante no conocía la respuesta a la pregunta de seguridad de la cuenta del CEO, el conocía los cuatro últimos números del numero de Seguridad Social del CEO. Pero dado que la cuenta es corporativa, no debería haber estado conectada con ese número. Esto permitió al atacante poder redirigir el correo de voz del CEO a un teléfono controlado por el atacante. De nuevo, a la hora de tener acceso a la cuenta – en este caso al correo móvil del CEO – el atacante usa el aspecto más débil de la seguridad para poder resetear y ejecutar el proceso de recuperación de contraseñas. A raíz de este incidente tanto AT&T como Google han cambiando el proceso de verificación para hacerlo más seguro

Conclusión

Del análisis de los hechos y actos realizados por los atacantes se desprende que estos pueden llegar a acceder a cuentas de alto valor. La percepción común del crio de 16 años sentado en su cuarto, en casa de papá y mamá mientras ataca sistemas ya es parte de la historia. A la vista de este y otros

sucesos similares, se hacen evidentes las cuestiones de contracultura organizativa, que planifican la realización de ataques sobre la América corporativa

A medida que las empresas plantean sus esquemas de autentificación en Internet, deben ser conscientes de que el proceso de autentificación puede hacerles perder el control de sus operaciones. Proveedores en la nube, IPS móviles, proveedores de internet y otros socios pueden gestionar procesos de reseteo de contraseñas, gestión de cuentas y procesos de pagos que deben ser plenamente entendidos y analizados para reforzar los aspectos más débiles.

Lo bueno de este incidente es que Google y AT&T han trabajado junto con CloudFlare para investigar este ataque, aun cuando estas empresas no eran conscientes de sus debilidades hasta el caso CloudFlare. Solo si se piensa de forma integral en el ecosistema del usuario en la red y en la nube, pueden identificarse las debilidades del sistema. Ahora, por desgracia, CloudFlare es consciente de lo que un atacante puede llegar a hacer para infiltrarse en su red. La pregunta es ¿tiene su empresa que esperar a que los atacantes le perjudiquen para ponerse en marcha?