beazley

Conocimiento de la industria

La amenaza del robo de credenciales: ¿Qué deben tener en cuenta las organizaciones?

junio 22, 2023

Las organizaciones y los sitios web sufren a diario incidentes de ciberseguridad, algunos de ellos ponen en peligro datos de los clientes. Los datos comprometidos suelen incluir listas de nombres de usuario y contraseñas, que permiten a los criminales que las poseen acceder a recursos en línea como sitios web y aplicaciones móviles. Estas contraseñas se intercambian y venden en Internet, en la llamada ‘dark web’ y en sitios web de acceso público. Algunas de estas listas de contraseñas pueden comprarse por tan solo 5 dólares. Además, hoy en día, las contraseñas pueden compartirse o adivinarse fácilmente, principalmente cuando las contraseñas son muy débiles (por ejemplo, "password" o "123456").

Las contraseñas pueden ser un gran negocio. Según varios estudios, una persona media puede tener más de 150 registros online diferentes. Debido a una insuficiente concienciación en materia de seguridad, la mayoría de la gente utiliza la misma contraseña para varias cuentas, e incluso puede utilizar la misma contraseña para cuentas personales, aplicaciones empresariales sensibles accesibles desde Internet o para conexiones remotas a la red de su empresa (VPN o Citrix). Así, una contraseña de una cuenta personal que se haya visto comprometida puede proporcionar a los criminales credenciales válidas para acceder a los sistemas de una organización de forma remota.

Es relativamente fácil y barato para los actores de amenazas realizar ataques de ‘credential stuffing’, que son solicitudes de inicio de sesión automatizadas a gran escala utilizando credenciales robadas (una solicitud de autenticación por usuario). Estos ataques suelen ser difíciles de detectar por los equipos de seguridad informática, ya que quien inicia la amenaza utiliza realmente nombres de usuario y credenciales válidos en lugar de ataques de fuerza bruta.

El impacto de un ataque de este tipo depende del tipo de datos o del acceso de las cuentas comprometidas. Puede variar desde el acceso a una suscripción a una revista, hasta el acceso remoto a los sistemas de información de una organización utilizando accesos privilegiados. Afortunadamente, hay maneras de que minimizar estos riesgos y proteger a su empresa o institución.

LO MÁS IMPORTANTE QUE SU ORGANIZACIÓN PUEDE HACER ES HABILITAR LA AUTENTICACIÓN MULTIFACTOR, O MFA.

El concepto de autenticación multifactor (MFA) no es nuevo. Antes de que se inventaran las llaves (hace más de 6.000 años), era necesario identificarse con un mensaje secreto para poder acceder a un evento o reunión. Años después, y a medida que los humanos descubrían lo fácil que era encontrar o adivinar un mensaje secreto, se inventaron las llaves. La llegada de la llave representó las primeras versiones de 2-FA (autenticación de dos factores): algo que sabías (la ubicación de la puerta), y algo que tenías (una llave física).

Podemos aplicar el mismo concepto en Ciberseguridad: aquello que conocemos", como el nombre de usuario, contraseña o PIN; pero que también puede ser conocida por los cibercriminales, por lo que necesita el segundo factor, que es lo que tenemos: un teléfono móvil, un código generado en un token físico o software instalado en su dispositivo móvil, un dispositivo inscrito en la empresa, etc.

MFA es una forma muy eficaz de proteger tu cuenta de los ataques oportunistas mencionados. Incluso si un criminal consigue acceder a una contraseña válida, el segundo factor de su MFA le impediría utilizarla para conectarse a sus cuentas en línea.

Recientemente, los ciber delincuentes han desarrollado herramientas para eludir algunas implementaciones de MFA, y algunas de estas herramientas se han hecho públicas (por ejemplo, EvilProxy). Estos son dos de los principales incidentes:

- **El primero** fue un ataque a Uber, en el que el delincuente accedió primero a los sistemas de la empresa desde la cuenta de un empleado (cuya contraseña había sido comprometida previamente) y enviándole repetidamente notificaciones push de MFA. Después de más de una hora, el autor de la amenaza se puso en contacto con el mismo empleado a través de WhatsApp haciéndose pasar por un empleado de soporte de TI de Uber y diciendo que las notificaciones MFA se detendrían una vez que el objetivo aprobara el inicio de sesión. El empleado lo aprobó y el autor de la amenaza obtuvo acceso inmediatamente.

- **El segundo** fue un incidente de pirateo de Twilio, en el que los empleados fueron redirigidos a páginas de inicio de sesión falsas a través de SMS. Esto permitió al actor de la amenaza recuperar los tokens MFA y utilizarlos para conectarse remotamente (este es un ejemplo de cómo se elude MFA).

No todas las soluciones MFA ofrecen el mismo nivel de seguridad. En la mayoría de los casos, los incidentes de evasión de MFA se aprovechan de prácticas de configuración débiles que pueden solucionarse cambiando la configuración predeterminada (por ejemplo, bloqueando

la autenticación heredada o legacy authentication). Por lo tanto, las soluciones MFA más débiles pueden hacerse más seguras con una configuración de seguridad adecuada (consulta las recomendaciones de Microsoft).

LA CONCIENCIACIÓN SOBRE LA SEGURIDAD Y UN CORRECTO MANTENIMIENTO DE CONTRASEÑAS SEGURAS TAMBIÉN SON ESENCIALES

La concienciación en materia de ciberseguridad sigue siendo clave para ayudar a las personas a adoptar las mejores prácticas en el manejo de contraseñas. Las mejores prácticas incluyen el uso de contraseñas únicas, largas y/o complejas que no puedan adivinarse a partir de información que pueda encontrarse en Internet, como el nombre, los apellidos, el nombre de la empresa, la dirección del usuario o la edad. Un gestor de contraseñas personales (como Bitwarden, que es gratuito y de código abierto) proporciona a una persona una manera fácil de generar y almacenar una contraseña única y compleja para cada una de sus cuentas en línea. Formar a los empleados para que sepan identificar nombres de dominio falsos o suplantados también es clave para protegerse de las recientes técnicas de elusión de la MFA.

Las organizaciones que no prevén que haya empleados o clientes que se conecten desde lugares específicos, pueden controlar las conexiones remotas procedentes de otros países, regiones o continentes aplicando restricciones de geolocalización. En función de la ubicación y de la hora de la conexión, una organización puede decidir si bloquear una conexión o exigir verificaciones adicionales utilizando un tercer factor, como un enlace enviado por correo electrónico, una pregunta con una respuesta secreta preconfigurada, una llamada telefónica o una notificación en un dispositivo móvil.

Supervisar las credenciales filtradas es otra forma de mantener unas buenas prácticas de ciberseguridad. Algunas organizaciones que han sufrido una filtración de datos se toman la molestia de notificar a los clientes y empleados que se vieron afectados por el incidente, sin embargo otras no lo hacen. Saber cuándo se filtran sus datos o contraseñas puede ser útil, ya que le permite tomar las medidas adecuadas cuando sea necesario, por ejemplo, cambiar una contraseña que se utiliza para varias cuentas, activar MFA si no está habilitado o alertar a su banco si su número de tarjeta de crédito ha sido robado. Hay varios sitios web que permiten a los particulares saber si sus datos han sido revelados en violaciones de dominio público (como haveibeenpwned.com).

Los gestores de contraseñas (incluidos Bitwarden y el gestor de contraseñas de Google Chrome) ofrecen funcionalidades que permiten a los usuarios saber si sus contraseñas se encuentran en una filtración de contraseñas revelada, y a menudo se ofrecen de forma gratuita. Además, los proveedores de servicios especializados ofrecen servicios que notifican a las organizaciones cuando sus datos se encuentran en la Dark Web, a veces incluso antes de que la filtración se haga pública. Este servicio suele llamarse "Vigilancia de la Dark Web".

A medida que los ciber criminales continúan aprovechándose de sus víctimas, las técnicas de seguridad como la implementación de una MFA segura y la implementación de buenas prácticas de gestión de contraseñas segura son esenciales para todas las organizaciones.

Jad Nehmé es director de cyber services del equipo de Beazley Cyber services internacional. Desde Francia presta apoyo a los clientes de Beazley durante un incidente de ciberseguridad o una fuga de datos. También ayuda a los clientes en la gestión de riesgos de privacidad y ciberseguridad, así como en controles preventivos. Antes de incorporarse a Beazley, Jad desempeño funciones en Alcatel-Lucent y KPMG, cubriendo tanto los aspectos técnicos como organizativos de la ciberseguridad.

Las opiniones expresadas aquí son las del autor.

beazley