beazley

Aperçu de l'industrie

La menace du vol des informations d'identification: ce que les entreprises doivent savoir

Jad Nehmé

Les organisations et les sites web subissent quotidiennement des incidents de cybersécurité, dont certains conduisent à la compromission des données des clients. Les données compromises incluent souvent des listes de noms d'utilisateur et de mots de passe, qui permettent aux acteurs malveillants qui les possèdent d'accéder à des ressources en ligne telles que des sites web et des applications mobiles. Ces mots de passe sont ensuite échangés et vendus sur Internet, principalement sur des marchés du dark web, mais aussi sur des sites web accessibles au public. Certaines de ces listes de mots de passe peuvent être achetées pour seulement 5€. De plus, de nos jours, les mots de passe peuvent être facilement mal partagés ou devinés, en particulier lorsque les utilisateurs utilisent des mots de passe faibles (ex. "mot de passe" ou "123456") ou encore avec l'abondance d'informations personnelles disponibles sur Internet.

Zoom sur la problématique des mots de passe

Les mots de passe sont un sujet important. Selon plusieurs études, une personne peut avoir en moyenne plus de 150 comptes différents en ligne. En raison d'une sensibilisation insuffisante à la sécurité, la plupart des gens utilisent le même mot de passe pour plusieurs comptes, et peuvent même utiliser le même mot de passe pour des comptes personnels, des applications professionnelles sensibles accessibles depuis Internet ou pour des connexions à distance au réseau de leur entreprise (comme un VPN ou Citrix). Ainsi, un mot de passe de compte personnel compromis, même à partir d'un site hébergeant des données non sensibles telles que dailyquizz.me, peut fournir aux pirates des informations d'identification valides pour

accéder à distance aux systèmes d'une organisation.

Il est relativement facile et peu coûteux pour les pirates d'effectuer des attaques de bourrage d'identifiant, qui sont des demandes de connexion automatisées à grande échelle utilisant des informations d'identification volées (une demande d'authentification par utilisateur). Ces attaques sont souvent difficiles à détecter par les équipes de sécurité informatique, car l'auteur de la menace utilise des noms d'utilisateur et des informations d'identification valides plutôt que des attaques brutes.

L'impact d'une telle attaque dépend du type de données ou d'accès des comptes compromis. Cela peut aller de l'accès à un abonnement à un magazine à l'accès à distance aux systèmes d'information d'une organisation à l'aide d'un accès privilégié. Heureusement, votre organisation peut se protéger de plusieurs manières contre ce risque.

La chose la plus importante que votre organisation puisse faire est d'activer l'authentification multifacteur, ou MFA.

Le concept derrière l'authentification multifacteur (MFA) n'est pas nouveau. Avant l'invention des clés (il y a plus de 6 000 ans), il fallait s'identifier avec un message secret avant d'avoir accès à une salle de réunion importante. Des années plus tard, et alors que les humains découvraient à quel point il était facile de trouver ou de deviner un message secret, des clés ont été inventées. L'avènement de la clé a représenté les premières versions de 2-FA (authentification à deux facteurs) : quelque chose que vous saviez (l'emplacement de la porte) et quelque chose que vous aviez (une clé physique)

Nous pouvons appliquer le même concept pour sécuriser l'accès informatique de nos jours : la partie que "vous connaissez" (nom d'utilisateur et mot de passe ou code PIN) peut également être connue par plusieurs acteurs malveillants, vous avez donc besoin du deuxième facteur, qui est la partie que "vous avez »: cela peut inclure un téléphone mobile avec une carte SIM, un code généré sur un jeton physique ou un logiciel installé sur votre appareil mobile, un appareil inscrit en entreprise, etc.

MFA est un moyen très efficace de protéger votre compte contre les attaques mentionnées ci-dessus. Même si un pirate a accès à un mot de passe valide, le deuxième facteur de votre MFA l'empêcherait de l'utiliser pour se connecter à vos comptes en ligne.

Exemples de MFA contournés

Récemment, des acteurs malveillants ont développé des outils pour contourner certaines implémentations MFA, et certains de ces outils ont été rendus publics (ex. EvilProxy).

Il y a eu deux incidents majeurs au cours desquels le MFA a récemment été contourné :

- Le premier était un piratage d'Uber, pour lequel le hacker a d'abord eu accès aux systèmes de l'entreprise en ciblant le compte d'un employé individuel (dont le mot de passe avait été précédemment compromis) et en lui envoyant à plusieurs reprises des notifications

push MFA. Après plus d'une heure, l'auteur de la menace a contacté le même employé sur WhatsApp en prétendant être un employé du support informatique d'Uber et en disant que les notifications MFA s'arrêteraient une fois que la cible aurait approuvé la connexion. L'employé a approuvé et l'auteur de la menace a obtenu l'accès immédiatement.
- Le second était un piratage de Twilio, dans lequel les employés ont été redirigés vers des fausses pages de connexion via SMS. Cela a permis à l'auteur de la menace de récupérer les jetons MFA et de les utiliser pour se connecter à distance (voici un exemple de la façon dont MFA est contourné).

Toutes les solutions MFA n'offrent pas le même niveau de sécurité. Dans la plupart des cas, les incidents de contournement MFA exploitent des pratiques de configuration faibles qui peuvent être corrigées en modifiant la configuration par défaut (par exemple, en bloquant l'authentification héritée). Ainsi, les solutions MFA plus faibles peuvent être rendues plus sécurisées avec une configuration de sécurité appropriée (consultez les recommandations de Microsoft).

La sensibilisation à la sécurité et l'hygiène des mots de passe sécurisés sont également essentielles

La sensibilisation à la sécurité reste essentielle pour aider les individus à adopter les meilleures pratiques lors de la gestion des mots de passe. Les meilleures pratiques incluent l'utilisation de mots de passe uniques, longs et/ou complexes qui ne peuvent pas être devinés sur la base d'informations pouvant être trouvées sur Internet, telles que le prénom, le nom de famille, le nom de l'entreprise ou l'adresse d'un utilisateur. Un gestionnaire de mots de passe personnel (par exemple Bitwarden, qui est gratuit et open source) offre à un individu un moyen simple de générer et de stocker un mot de passe unique et complexe pour chacun de ses comptes en ligne. La formation des employés pour identifier les noms de domaine faux ou usurpés est également essentielle pour se protéger contre les récentes techniques de contournement MFA.

Les organisations qui ne s'attendent pas à ce que leurs employés ou leurs clients se connectent à partir d'emplacements spécifiques peuvent contrôler les connexions à distance provenant d'autres pays, régions ou continents en mettant en place des restrictions de géolocalisation. En fonction du lieu et de l'heure de la connexion, une organisation peut décider de bloquer une connexion ou d'exiger des vérifications supplémentaires à l'aide d'un troisième facteur tel qu'un lien envoyé par e-mail, une question avec une réponse secrète préconfigurée, un téléphone appel ou une notification sur un appareil mobile.

Informations d'identification divulguées

La surveillance des informations d'identification divulguées est un autre moyen pour les entreprises et les particuliers de pratiquer une hygiène sécurisée des mots de passe. Certaines organisations qui ont subi une violation de données font l'effort d'informer les clients et les employés qui ont été touchés par l'incident, mais d'autres ne le font pas. Savoir quand vos données ou mots de passe sont divulgués peut être utile car

cela vous permet de prendre les mesures appropriées en cas de besoin, par exemple changer un mot de passe utilisé pour plusieurs comptes, activer MFA s'il n'est pas activé ou alerter votre banque si votre numéro de carte de crédit a été volé. Il existe plusieurs sites Web qui permettent aux individus de savoir si leurs données ont été divulguées dans des violations connues du public (comme haveibeenpwned.com).

Les gestionnaires de mots de passe (y compris Bitwarden et le gestionnaire de mots de passe de Google Chrome) offrent des fonctionnalités qui permettent aux utilisateurs de savoir si leurs mots de passe font partie d’une fuite de mot de passe divulguée, et ceux-ci sont souvent offerts gratuitement. De plus, des prestataires de services spécialisés proposent des services qui informent les organisations lorsque leurs données sont trouvées sur le dark web, parfois même avant que la violation ne soit rendue publique. Ce service est souvent appelé "Surveillance du Dark Web".

Alors que les acteurs malveillants continuent de s'attaquer aux proies faciles, les techniques de sécurité telles que la mise en œuvre d'une MFA sécurisée et la pratique de l'hygiène des mots de passe sécurisés sont des composants essentiels de la gestion des risques pour chaque organisation. Se renseigner, ainsi que vos collègues, sur les derniers risques et prendre des mesures pour les atténuer vaut bien le temps et les efforts.

Jad Nehmé

Client Experience Manager

beazley