4 mesures efficaces pour limiter la compromission de comptes en ligne

La migration des ressources vers le Cloud a été le dénominateur commun des stratégies commerciales des entreprises au cours des deux dernières années. Comme souvent, les cybercriminels ont suivi le mouvement pour en tirer profit.

En conséquence, le nombre d'incidents impliquant le vol d'informations sensibles et de mots de passe d'utilisateurs sur des plateformes Cloud n'a eu de cesse d'augmenter.

Selon le Rapport sur les fuites de données réalisé par Verizon en 2021, 29 207 incidents de sécurité en temps réel ont été détectés sur l'année 2020, dont 5 258 étaient des fuites de données confirmées.

Ce rapport indique que les attaques sur les applications Web constituaient toujours un enjeu important en matière de cybersécurité, représentant 89 % des cyberattaques en 2020, dont 61 % exploitaient des informations d'identification usurpées.

Les informations d'identification peuvent être volées, achetées, devinées ou trouvées sur le Dark Web, en particulier si les utilisateurs ne protègent pas leurs mots de passe ou si une structure sécurisée fait défaut au niveau technologique.

Ce problème concerne en premier lieu les utilisateurs, mais il est également fortement préjudiciable pour les entreprises car, en cas de fuite de données, c'est leur réputation qui peut être impactée.

La mise en œuvre de stratégies de gestion des identités et de contrôle des accès est essentielle pour protéger les informations confidentielles d'une entreprise.

Lorsque les utilisateurs accèdent à un service protégé, la demande d'informations supplémentaires en plus du mot de passe procure un autre niveau de sécurité et constitue un outil fiable pour réduire les fuites de données dans les applications mobiles. **L'authentification multifacteur (MFA) doit aujourd'hui devenir incontournable pour l'accès à des applications et comptes utilisateurs hébergeant des données, et cela même si lesdites données ne sont pas sensibles.**

Concrètement, le MFA demande aux utilisateurs de fournir deux types d'informations ou plus, tels que le mot de passe associé au nom d'utilisateur et une notification push, un mot de passe à usage unique (OTP) ou d'autres facteurs pris en charge par leur service ou leur application.

Autre solution efficace pour prévenir ce type de vol de compte : la protection des postes de travail (EPP).

Grâce à un portefeuille de techniques basées sur la mise en cache locale, l'analyse heuristique et les flux d'intelligence, les plateformes de sécurité peuvent détecter les malwares et d'autres types de menaces qui pourraient conduire à des fuites de données – comme le vol d'identifiants par hameçonnage – au niveau des postes de travail.

Un autre élément commun est **l'adoption de l'authentification en tant que service (AaaS).** À mesure que les entreprises migrent leurs services vers le Cloud, les DSI intègrent des services dotés de capacités d'authentification dans le Cloud lors de la mise en œuvre de leur stratégie, afin que les institutions puissent vérifier les clients en toute sécurité grâce à l'authentification multifacteur (MFA). Les entreprises peuvent ainsi protéger l'accès à n'importe quelle application, depuis n'importe quel appareil, partout dans le Cloud.

Compte tenu du risque de vol d'identifiants, il ne faut pas oublier le rôle important joué par les sondes installées sur le réseau, qui ont pour but d'identifier et collecter des données (liées aux fichiers, processus, connexions réseau et clés de registre des hôtes sur lesquelles elles sont installées) sur tout type d'anomalie détectée et les envoyer dans le Cloud pour analyse.

La manière dont les données sont collectées est entièrement configurable dans ce type de solution. Grâce à ces informations, les systèmes de sécurité peuvent prendre des mesures appropriées pour faire face à certains types de menaces en fonction de la configuration, afin d'empêcher le vol d'identifiants. Ce type de vol peut se produire lorsqu'une personne qui a obtenu l'accès à l'ordinateur d'un utilisateur tente d'obtenir un accès privilégié aux serveurs par la force, par exemple.

Avec la crise du Covid, la transformation numérique des entreprises s'est fortement accélérée. Le Cloud est désormais omniprésent dans les entreprises, et dans notre vie quotidienne. Pour les attaquants, ces nouveaux usages génèrent des opportunités sans précédent. Comme souvent, les usages se mettent en place et la cybersécurité est prise en considération plus tard…

Malheureusement, plus tard, c'est trop tard. Et beaucoup d'entreprises, petites et grandes, peuvent en témoigner. Ces quelques bonnes pratiques et technologies de cybersécurité présentées plus haut, donnent de premières pistes incontournables pour disposer d'une base solide face à des attaques omniprésentes.