Le défi des mots de passe admin statiques

Je l'ai trouvé sur le site d'un client lors d'une procédure d'analyse. Le client ne savait même pas que ce mot de passe existait. Ça n'aurait déjà pas été une bonne nouvelle s'il s'était agi du mot de passe d'un compte utilisateur. Mais là, en l'occurrence, c'était un mot de passe administrateur qui donnait un accès privilégié à un système critique de son réseau…

La protection des mots de passe admin

Réfléchissons un peu à la sécurité d'un certain type de mots de passe : les mots de passe admin. Dans le monde IT, la plupart des administrateurs système doivent gérer des mots de passe administratifs pour les comptes privilégiés. Le compte administrateur Windows par défaut est un exemple de compte privilégié.

C'est une bonne pratique de sécurité que de changer continuellement ces mots de passe. Dans certaines organisations, on change les mots de passe admin pour se conformer aux réglementations comme PCI-DSS, HIPAA ou RGPD. Parfois, l'on change les mots de passe admin lorsqu'un employé qui connaît les identifiants quitte la société. Quoiqu'il en soit, ces mots de passe doivent être changés fréquemment pour la sécurité de l'organisation et des données que celle-ci doit protéger.

Comprendre le problème de sécurité des mots de passe privilégiés

Malheureusement, toutes les organisations ne sont pas proactives dans la protection de leurs mots de passe administratifs. Dans bon nombre des entreprises, le service IT va au plus simple en utilisant le même nom de compte admin et le même mot de passe, souvent assez basique, pour plusieurs systèmes. Et dans la plupart des cas, ce mot de passe n'a pas été changé depuis la mise en place et le déploiement de ces systèmes.

De plus, les employés notent les mots de passe sur des bouts de papier, ce qui crée une menace croissante pour l'entreprise. De l'édition 2018 du rapport Bomgar sur les menaces liées aux accès privilégiés, il ressort que**65% des entreprises reconnaissent annoter « parfois » les mots de passe**, soit 10% de plus que l'année précédente. Confier des mots de passe à des collègues posait problème à 46% des entreprises en 2017 contre 54% en 2018. Cette progression peut être révélatrice d'un problème croissant ou d'une prise de conscience des entreprises par rapport à l'an dernier. Dans tous les cas, ces chiffres témoignent d'un problème qu'il convient de résoudre.

Vous vous demandez si ce problème est réellement sérieux ? Jugez-en par vous-même en répondant à ces questions :

- Combien de personnes connaissent vos mots de passe admin ?
- Est-ce que ces personnes travaillent toujours dans votre entreprise ?
- Si certaines de celles qui connaissaient vos mots de passe admin ne travaillent plus pour l'entreprise, sont-elles parties en de bons termes ?

- Plusieurs ou tous vos systèmes partagent-ils le même mot de passe admin ?
- Vos mots de passe admin sont-ils suffisamment complexes et changés fréquemment ?

Plus il y a de personnes à connaître un secret, plus il y a de chances que ce secret soit divulgué. C'est ce qu'il risque de se produire avec le mot de passe admin utilisé pour plusieurs ou tous les systèmes, et partagé avec l'ensemble du groupe IT. C'est ainsi que les entreprises commencent à détecter des machines avec des configurations inappropriées, et qu'elles découvrent que des utilisateurs lambda connaissent le mot de passe admin partagé.

Quand les mots de passe secrets vous échappent

Si tous ceux qui connaissent les mots de passe travaillent toujours dans l'entreprise et sont des salariés heureux et loyaux, le risque lié à l'accès est quelque peu atténué. Mais on ne sait jamais quand un utilisateur malveillant risque d'agir. Si un salarié ou un sous-traitant a quitté l'entreprise en mauvais termes, vous avez peut-être affaire à un élément perturbateur qui sait comment s'infiltrer sur votre réseau au moyen d'un compte intraçable. Et il est bien difficile d'en élaborer un portrait type. Voici un exemple récent d'une ancienne salarié IT qui s'est connectée au réseau de son ancien employeur pour perturber les opérations.

Ce n'est pas un fait isolé. J'ai connu des gens qui se connectaient aux systèmes de leur précédent employeur simplement parce qu'ils le pouvaient. Cela est révélateur des mauvaises pratiques liées au maintien des mots de passe admin qui devraient être changés, mais c'est surtout inquiétant de constater les dommages qu'ils auraient pu commettre s'ils avaient été mal intentionnés.

Pourquoi l'âge des mots de passe compte ?

L'âge des mots de passe compte car c'est votre arme face au problème de vol d'identifiants. Le mot de passe âgé de 18 ans que j'ai mentionné au début de cet article en est un bon exemple.

Un mot de passe que l'on ne change pas fréquemment donne tout le temps qu'il lui faut au criminel pour se l'approprier. Et une fois qu'il connaît le mot de passe, il obtient un accès permanent à tous les systèmes partageant ce même mot de passe jusqu'à ce qu'il soit mis à jour. Si cela arrive un jour.

Ce qu'il faut retenir c'est qu'avec la volonté de dérober un mot de passe admin et de s'infiltrer sur les systèmes d'un réseau, tout ce dont quiconque a besoin, c'est d'un peu de temps. Mais en changeant de façon continue et automatique les mots de passe des comptes privilégiés, vous ôtez à vos adversaires les outils qu'il leur faut pour perpétrer leur méfait**.**

Crédit photo © Brian A Jackson – Shutterstock