Une politique de mots de passe efficace pour les PME

La sécurité des systèmes et réseaux informatiques passe nécessairement par l'utilisation correcte des mots de passe. La politique de mots de passe - ou Password Policy - régit la création, la conservation et l'utilisation des mots de passe.

Principales informations à connaître :

- Faites la liste de tous les accès au système et aux applications de l'entreprise protégés par mot de passe.
- Définissez dans une politique de mots de passe les exigences relatives à la création, la conservation et l'utilisation des mots de passe pour tous les accès précédemment identifiés.
- Contrôlez régulièrement que la politique de mots de passe est strictement respectée.
- Sensibilisez l'ensemble des collaborateurs aux risques liés à une utilisation inappropriée des mots de passe.

Pourquoi mettre en place une politique de mots de passe ?

L'association d'un nom d'utilisateur et d'un mot de passe reste la méthode d'authentification et d'autorisation la plus utilisée dans les espaces numériques de travail. Cette combinaison permet notamment d'établir l'identité d'un utilisateur souhaitant accéder à des réseaux, se connecter à des systèmes informatiques ou utiliser des services et des applications, mais aussi d'assurer la sécurité de ces accès. Les identifiants (noms d'utilisateurs et mots de passe) jouent par conséquent un rôle central dans la cybersécurité.

Il n'est donc pas étonnant que les cybercriminels mettent tout en œuvre pour accéder, que ce soit à travers des attaques de piratage, de phishing ou d'ingénierie sociale, à ces précieuses informations qui leur permettront d'usurper l'identité numérique de la personne visée.

L'utilisation des mots de passe est tellement courante que les utilisateurs ne sont souvent pas conscients des dangers qui y sont associés. Voilà pourquoi il est indispensable, et tout particulièrement en entreprise, de mettre en place une politique de mots de passe claire pour guider les utilisateurs et les prémunir contre des erreurs qu'ils pourraient commettre dans ce contexte.

Qu'est-ce qu'une politique de mots de passe et comment la rendre efficace ?

Une politique de mots de passe est un ensemble de règles visant à renforcer la cybersécurité en aidant les collaborateurs à créer des mots de passe forts, à les conserver et à les utiliser de manière sécurisée. La Password Policy doit faire partie du règlement d'une organisation et devrait être incluse dans la formation concernant la sensibilisation à la sécurité (programme de sensibilisation).

Une politique de mots de passe doit être conçue sur mesure en fonction des besoins (infrastructure du système) et des exigences (niveau de sécurité) de l'organisation concernée, afin de garantir une protection optimale pour un investissement raisonnable. Il convient donc dans un premier temps d'établir une liste de tous les accès au système et aux applications de l'entreprise protégés par mot de passe et d'évaluer le niveau de protection requis. Tous les

accès ainsi identifiés devront être pris en compte dans la politique de mots de passe.

Afin de pouvoir faire face à l'évolution constante des menaces, il sera ensuite nécessaire de vérifier régulièrement l'actualité et l'efficacité de la Password Policy.

Quels doivent être les principaux points de la politique de mots de passe ?

La Password Policy doit régler de manière exhaustive l'utilisation des mots de passe dans l'entreprise et fournir aux utilisateurs des instructions concrètes sur leur manière d'agir. Ces recommandations doivent porter sur les points suivants :

1. L'utilisation des mots de passe

Comme évoqué plus haut, la connaissance d'un mot de passe suffit souvent pour usurper complètement l'identité numérique d'une personne. En général, il convient donc de prendre toutes les précautions nécessaires pour éviter toute utilisation abusive de cette information.

Les mots de passe sont strictement personnels et confidentiels. En particulier, il convient de respecter les points suivants :

1. Les mots de passe ne doivent en aucun cas être transmis ni partagés activement, ni même être rendus accessibles à des tiers.
2. La conservation et la transmission des mots de passe doivent toujours être cryptées.
3. Au moment de la saisie du mot de passe, l'utilisateur doit s'assurer que cette opération n'est pas visible à d'autres personnes.

La politique de mots de passe fixe des directives au sens dirigiste du terme concernant l'utilisation des mots de passe.

2. La force des mots de passe

La force d'un mot de passe indique la difficulté pour un attaquant de découvrir le mot de passe rien qu'en le devinant ou à force de tentatives. Plus un mot de passe est imprévisible, complexe et long, plus il est fort et donc sûr.

Une bonne politique de mots de passe doit mettre l'accent sur la création de mots de passe forts et encourager les utilisateurs à choisir des mots de passe plus longs et imprévisibles. (Guide « Mots de passe sûrs » (https://www.ebas.ch/fr/4-proteger-les-acces-internet/#passwords))

En outre, la création de mots de passe forts devrait être étayée par des moyens techniques, comme par exemple la mise à disposition d'un gestionnaire de mots de passe (https://www.ebas.ch/fr/4-proteger-les-acces-internet/#passwords) , et réglementée par la politique de mots de passe.

3. L'expiration des mots de passe

Les mots de passe sont des informations faciles à transmettre et susceptibles, au fil du temps, de tomber entre de mauvaises mains. Il peut arriver par exemple que des collaborateurs partagent leurs mots de passe sans y penser avec d'autres personnes, ou qu'ils les notent et les conservent sur des supports non protégés. Il peut arriver également que les mots de passe des utilisateurs soient involontairement révélés à la suite de pannes ou autres incidents. Or il n'est en principe pas possible de récupérer des informations ayant ainsi déjà circulé.

Dans de tels cas, le seul moyen de rétablir efficacement la sécurité est de modifier les mots de passe en question pour les rendre inutilisables.

La création et la gestion des nouveaux mots de passe forts devraient être étayées par des moyens techniques, comme par exemple la mise à disposition d'un gestionnaire de mots de passe, et être réglementées dans la politique de mots de passe.

4. L'historique des mots de passe
Les utilisateurs ont souvent tendance à réduire le nombre de mots de passe à retenir, en utilisant par exemple des mots de passe déjà utilisés précédemment. Une pratique bien connue des cybercriminels qui utilisent régulièrement des listes d'anciens mots de passe lors de leurs attaques. Pour éviter cela, il convient de priver les utilisateurs de la possibilité de réactiver d'anciens mots de passe.

La politique de mots de passe doit faire en sorte que les systèmes gardent en mémoire les mots de passe des utilisateurs afin d'empêcher leur réutilisation.

5. La modification du mot de passe
Les utilisateurs devraient avoir la possibilité de modifier seuls et à tout moment leurs mots de passe. Il convient toutefois de s'assurer que ces changements de mots de passe soient effectivement réalisés par les utilisateurs légitimes et non par un hacker.

La politique de mots de passe définit le cadre technique et organisationnel permettant de procéder en toute sécurité à une modification du mot de passe. Il est recommandé par exemple d'introduire une méthode d'authentification à deux facteurs pour sécuriser le processus de modification du mot de passe.

Les mots de passe restent aujourd'hui encore l'élément de sécurité le plus utilisé pour protéger les accès dans un environnement numérique. Dans ces conditions, on ne s'étonnera pas que les cybercriminels mettent tout en œuvre, à travers des attaques de piratage, de phishing ou d'ingénierie sociale, pour accéder à cette information.

Une politique de mots de passe (Password Policy) garantit clarté et sécurité dans l'utilisation des mots de passe.