OBJET

La gestion efficace des mots de passe est la première ligne de défense dans la sécurité électronique d'une organisation. Au sein d'un Conseil scolaire, il n'est pas rare que la plupart des employées et employés aient de multiples mots de passe pour accéder aux courriels, aux boîtes vocales, aux applications informatiques et aux portails. Chaque Conseil scolaire doit mettre en place une stratégie de mot de passe dans le cadre de la stratégie relative à la sécurité générale.

Le présent document est destiné à servir de ligne directrice pour l'élaboration de procédures relatives au mot de passe. Il contient les points à examiner et les stratégies pouvant être utilisées pour élaborer des procédures pour la création et le maintien de mots de passe sécuritaires.

Avantages d'une procédure relative au mot de passe

- Accès approprié pour tout le personnel;
- Gestion de l'identité et vérification de l'accès efficaces;
- Conservation et protection des informations personnelles qui vous sont confiées;
- Protection de VOS informations personnelles.

Meilleures pratiques/Recommandations

L'adoption réussie d'une procédure relative au mot de passe repose sur la capacité de l'organisation de la mettre en œuvre. Certains conseils scolaires disposent de technologies d'avant-garde pouvant offrir une automatisation et un soutien importants à un grand nombre d'utilisatrices et d'utilisateurs. D'autres peuvent disposer de ressources limitées et devront élaborer une procédure qui est réalisable de façon plus manuelle. Il est important de comprendre que, peu importe le groupe auquel le Conseil scolaire appartient, les procédures relatives au mot de passe demeurent essentielles à la gestion efficace de la sécurité.

Au moment de créer une procédure relative au mot de passe, il est important de tenir compte des éléments qui peuvent être configurés au moyen de la sécurité logicielle et de ceux qu'il faut apprendre aux utilisatrices et aux utilisateurs. Des éléments tels que la longueur minimale d'un mot de passe et le cycle d'expiration des mots de passe sont généralement configurés à l'aide du logiciel système. Parmi les points à enseigner aux utilisatrices et aux utilisateurs, il convient de mentionner la nécessité de ne pas afficher des mots de passe sur des feuillets autoadhésifs et de ne pas partager les mots de passe.

La conservation d'un mot de passe est un autre point important à examiner au moment de l'élaboration d'une procédure relative au mot de passe. Malgré la mise en place des meilleures procédures, des mots de passe seront échangés ou seront connus au fil du temps, affaiblissant la sécurité. Il est donc nécessaire de les changer régulièrement. La plupart des systèmes permettent à l'administratrice ou à l'administrateur du système de configurer un paramètre entraînant l'expiration des mots de passe et nécessitant leur remise à zéro par l'utilisatrice ou l'utilisateur. Ce paramètre est

Dans le but d'alléger ce texte, le «Conseil scolaire» comprend aussi les administrations scolaires.

généralement configuré entre 30 et 90 jours, selon le nombre d'utilisatrices et d'utilisateurs, le niveau de risque et la gérabilité de la procédure. L'expiration du mot de passe augmente la charge de travail du personnel technique puisque les utilisatrices et les utilisateurs oublient souvent leurs nouveaux mots de passe et ont besoin d'aide pour les modifier. Aussi, une bonne façon est de forcer la remise à zéro d'un mot de passe la première fois qu'une utilisatrice ou un utilisateur se connecte à un système quelconque.

FACTEURS TECHNIQUES À EXAMINER

- Longueur du mot de passe – Les mots de passe devraient contenir au moins six caractères pour assurer une protection adéquate, mais ne devraient pas être longs à un point tel que le personnel ait de la difficulté à s'en souvenir.
- Caractères mélangés – Les mots de passe devraient contenir au moins un des éléments suivants : lettres majuscules et minuscules, chiffres et caractères spéciaux (@#$!% etc.). Lorsque la technologie ne permet pas l'application de cette recommandation, il faut en informer les utilisatrices et les utilisateurs.
- Conservation du mot de passe – Les mots de passe devraient être remis à zéro régulièrement et devraient expirer après une période déterminée. Cette période peut varier de 30 jours à deux fois par année, selon la culture du Conseil scolaire et le soutien technique disponible.
- Historique – L'historique des mots de passe doit être conservé et configuré de façon à ce que les utilisatrices et les utilisateurs ne puissent pas utiliser le même mot de passe deux fois à l'intérieur d'une période définie. L'historique devrait comprendre au moins trois mots de passe, mais le Conseil scolaire peut configurer le nombre de son choix.

Éducation des utilisatrices et des utilisateurs

Pour assurer la protection des utilisatrices et des utilisateurs, les mots de passe créés doivent être difficiles à deviner. Les points suivants offrent des conseils sur les meilleures pratiques pour la création d'un mot de passe :

- Le mot de passe ne doit pas être identique au nom de l'utilisatrice ou de l'utilisateur, même si on y ajoute un chiffre ou un symbole.
- Les mots de passe ne doivent pas contenir de informations personnelles, tels que le nom ou le numéro de la rue, le nom de l'entreprise, la date de naissance, etc.
- Les mots de passe ne doivent jamais contenir de noms des membres de la famille, des animaux de compagnie, des amies et amis ou des collègues de travail.
- Les mots de passe ne doivent pas être une phrase commune suivie d'un chiffre qui change lorsque le mot de passe expire.

Les utilisatrices et les utilisateurs devraient toujours respecter les principes suivants :

- N'échangez pas de mots de passe avec quiconque. Si vous vous retrouvez dans une situation où vous devez le faire, n'oubliez pas de changer le mot de passe dès que la situation a été résolue.
- N'utilisez jamais le même mot de passe que celui que vous utilisez pour vos comptes personnels (comptes bancaires, etc.).
- N'écrivez pas les mots de passe et ne les incluez pas dans un courriel.
- Ne sauvegardez pas les mots de passe électroniquement, à moins qu'ils ne soient cryptés.
- N'utilisez jamais la fonction « Mémoriser mon mot de passe » sur aucun système; cette fonction devrait être désactivée lorsque cela est possible sur le plan technique.

Voici quelques exemples de mots de passe forts et faibles :

Mot de passe	Force	Raison
Wam4uG	Bon	Six caractères, lettres majuscules et un chiffre
soleil	Faible	Trop court, trop facile à pirater/deviner
charles1	Faible	Utilisation du prénom de l'utilisateur – trop facile
22965	Faible	Identique au NIP bancaire personnel de l'utilisateur ou de l'utilisatrice – constitue des risques additionnels pour l'utilisateur ou l'utilisatrice
3z2tt4cy	Très bon	Mot de passe créé par le système qui change tous les trois mois

Conclusion

Au moment d'élaborer une procédure relative au mot de passe, il faut tenir compte de nombreux facteurs. Des procédures rigoureuses assurent une plus grande sécurité, mais elles nécessitent un plus grand soutien des utilisatrices et des utilisateurs et peuvent entraîner un faible taux de conformité. Des politiques beaucoup moins strictes seront probablement mieux respectées par les utilisatrices et les utilisateurs, mais il est possible qu'elles ne protègent pas les informations du Conseil scolaire de façon adéquate. La clé de l'efficacité de la procédure relative au mot de passe consiste à établir un équilibre entre les besoins en matière de sécurité du Conseil scolaire et leur culture, ainsi qu'à respecter les lignes directrices définies dans les présentes.

De nombreuses ressources disponibles en ligne peuvent être utilisées conjointement avec le présent document. Le SANS (SysAdmin, Audit, Network, Security) Institute, www.sans.org, offre un modèle de politique relative au mot de passe qui peut être modifié par une organisation. De nombreux conseils scolaires de l'Ontario ont élaboré des politiques ou des procédures relatives au mot de passe et sont prêts à les partager avec d'autres conseils scolaires.