ARBONIA
IT SECURITY

Nouvelle directive relative aux mots de passe du groupe Arbonia

Chères collaboratrices, chers collaborateurs,

Un mot de passe fort est la première ligne de défense de nos systèmes et données.

L'objectif principal des attaques est, entre autres, le vol des données d'accès aux comptes utilisateurs afin d'obtenir un premier accès à nos réseaux, serveurs et systèmes informatiques et, dans le pire des cas, de mener des activités telles que le vol de données, l'espionnage ou l'installation de logiciels malveillants sans se faire remarquer. C'est pourquoi les mots de passe faibles ou compromis, ainsi qu'une mauvaise manipulation de ceux-ci, constituent un risque important. Afin de mieux répondre à nos exigences en matière de sécurité et de mieux vous protéger contre ces menaces, une nouvelle politique relative aux mots de passe a été définie pour le Groupe Arbonia.

Modification de la directive relative aux mots de passe

Vous trouverez ci-dessous une présentation claire de la stratégie complète en matière de mots de passe. La modification concerne principalement la longueur minimum du mot de passe, sa validité maximum et sa complexité.

La longueur minimum du mot de passe est portée de 8 à 12 caractères afin de rendre plus difficile le piratage d'un mot de passe, mais dans le même temps, la validité du mot de passe est étendue à 360 jours minimum. Si vous utilisez un mot de passe plus long (≥ 16 caractères), la validité du mot de passe est prolongée à 540 jours. Dans tous les cas, un niveau élevé de complexité (= mot de passe fort) doit être assuré pour les nouveaux mots de passe. Ceci est rendu possible par une combinaison de lettres en majuscules/en minuscules/de chiffres de 0–9/de signes de ponctuation ou de caractères spé-

De plus, l'utilisation de mots de passe déjà compromis et accessibles librement sur Internet ainsi que de mots figurant sur une liste noire (par ex. le nom d'une entreprise) est automatiquement blo-

Si le mot de passe apparaît dans une base de données de mots de passe compromis pendant sa durée de validité, vous serez automatiquement invité à le modifier.

La nouvelle directive relative aux mots de passe est automatiquement activée lors de la prochaine modification de votre mot de passe Windows ou sur demande de votre service informatique local. Un rappel vous sera envoyé respectivement 14 jours avant l'expiration du mot de passe. **La directive vaut néanmoins pour tous les systèmes TIC du groupe Arbonia, c'est-à-dire également pour les systèmes autres que Windows. En tant que titulaire du compte, vous êtes dans tous les cas responsable du respect de la politique relative aux mots de passe, même si celle-ci n'est pas obligatoire techniquement.**

Créer un mot de passe fort

Il existe différentes techniques pour créer un mot de passe fort et s'en souvenir. Créez, par exemple, un mot de passe fort à partir d'une phrase ou en substituant des chaînes de caractères définies :

- Sélectionnez une phrase dont vous vous souviendrez facilement et transformez-la en mot de passe. par ex.: *«Il n'est pas si dur de choisir un mot de passe fort.»* Utilisez la lettre initiale ou plusieurs lettres des différents mots et enrichissez le mot de passe avec des chiffres et des caractères spéciaux. Par ex. : *«In'epsddc1mdpf.»*
- Sélectionnez un mot dont vous pourrez vous souvenir facilement, par ex. «Anaconda» et définissez une suite de caractères spéciale, par ex. *«1$1»*. Remplacez alors des parties/lettres définies du mot avec la suite de caractères sélectionnée pour obtenir un mot de passe fort. Par ex. : *«aut1$1m1$1bile»*

Nous vous remercions de votre attention et vous adressons nos meilleures salutations.
Arbonia Security Team

ARBONIA
IT SECURITY

Stratégie en matière de mots de passe			
Historique des mots de passe (nombre des derniers mots de passe ne pouvant pas être réutilisés)	5	**Nombre de tentatives de connexion échouées jusqu'à ce que le compte soit bloqué**	6
Longueur minimale du mot de passe	12 caractères	**Durée de blocage du compte**	Jusqu'au déverrouillage par un administrateur
Durée de validité maximale du mot de passe	360 jours (12–15 caractères) ou 540 jours (≥16 caractères)	**Durée avant que le compteur de tentatives de connexion échouées ne soit réinitialisé**	≥ 60 minutes
Complexité	➢ Lettres majuscules ➢ Lettres minuscules ➢ chiffres de 0–9 ➢ Signes de ponctuation ou caractères spéciaux	**Spécial (mots de passe Windows – interne à Arbonia et appliqué automatiquement)**	Le mot de passe ne doit pas contenir de chiffres en première et dernière position et pas trois caractères identiques consécutifs

N'utilisez aucun des mots de passe cité en exemple dans ce document. Ces exemples de mots de passe sont maintenant «compromis» et inclus dans la liste noire.

En plus de cette lettre d'information, veuillez également tenir compte de la politique relative aux mots de passe en vigueur (IS-ISP-GROUP-001-PASSWORD-POLICY) disponible à l'adresse https://security.arbonia.com

Lorsque vous modifiez votre mot de passe Windows, les conditions à remplir s'affichent directement.