ARBONIA
IT SECURITY

Nova política de palavras-passe do Grupo Arbonia

Caras/os colaboradoras/es,

Uma palavra-passe forte é a primeira linha de defesa dos nossos sistemas e dados.

O principal objetivo dos autores dos ataques é, entre outros, o roubo de dados de acesso a contas de utilizadores para obter acesso inicial às nossas redes, servidores e sistemas DE TI e, no pior dos casos, para levar a cabo atividades como o roubo de dados, espionagem ou a instalação de malware sem serem detetados. Por esta razão, as palavras-passe fracas ou comprometidas, bem como a sua gestão incorreta, representam um risco considerável. A fim de melhor satisfazer os nossos requisitos de segurança e de melhor o proteger contra estas ameaças, foi definida uma nova política de palavras-passe para o Grupo Arbonia.

Alteração da política de palavras-passe

De seguida, pode encontrar a estratégia completa de palavras-passe claramente representada. A alteração refere-se sobretudo ao comprimento mínimo da palavra-passe, à validade máxima e à sua complexidade.

O comprimento mínimo da palavra-passe será aumentado dos atuais 8 para 12 caracteres para que seja mais difícil decifrar uma palavra-passe, mas, ao mesmo tempo, a validade da palavra-passe será prolongada para pelo menos 360 dias. Se utilizar uma palavra-passe mais longa (≥ 16 caracteres), a validade da palavra-passe é prolongada até 540 dias. Em todo o caso, deve ser assegurado um elevado nível de complexidade (= palavra-passe forte) para as novas palavras-passe. Isto consegue-se através de uma combinação de maiúsculas/minúsculas/dígitos 0–9/sinais de pontuação ou caracteres especiais.

Além disso, é automaticamente impedida a utilização de palavras-passe já comprometidas e livremente acessíveis na Internet, bem como de palavras de uma lista negra (por ex. nome da empresas).

Se a palavra-passe constar numa base de dados de palavras-passe comprometidas enquanto for válida, será automaticamente alertado para alterar a palavra-passe.

A nova política de palavras-passe ficará automaticamente ativa aquando da sua próxima alteração da palavra-passe do Windows ou do pedido do seu departamento local de TI. Receberá um lembrete 14 dias antes de expirar a palavra-passe. **No entanto, a política aplica-se a todos os sistemas de TIC do Grupo Arbonia, ou seja, também aos sistemas não-Windows. Na qualidade de titular da conta, será sempre responsável pelo cumprimento da política de palavras-passe, mesmo que esta não seja um requisito técnico.**

Criar uma palavra-passe forte

Existem várias técnicas para criar e decorar uma palavra-passe forte. Por exemplo, crie uma palavra-passe forte com base numa frase ou através da substituição de sequências definidas:

- Escolha uma frase de que se recorde bem e transforme-a numa palavra-passe. Por ex.: «*Não é assim tão difícil, escolher uma palavra-passe forte.»* Utilize a primeira letra ou várias letras de cada palavra e fortaleça a palavra-passe com dígitos e caracteres especiais. Por ex.: *«Néatd,e1P-pf.»*
- Escolha uma palavra de que se recorde bem, por ex. «Primavera» e defina uma sequência especial, por ex. «1$1». Agora substitua as partes/letras definidas da palavra pela sequência que escolheu para obter uma palavra-passe forte. Por ex. «Aut1$1m$1$vel».

Obrigado pela vossa atenção e melhores cumprimentos
Arbonia Security Team

ARBONIA
IT SECURITY

Estratégia de palavras-passe			
Histórico de palavras-passe (número de palavras-passe recentes que não podem ser reutilizadas)	5	**Número de tentativas de início de sessão falhadas até que a conta seja bloqueada**	6
Comprimento mínimo da palavra-passe	12 caracteres	**Duração do bloqueio da conta**	Até um administrador a desbloquear
Validade máxima da palavra-passe	360 dias (12–15 caracteres) ou 540 dias (≥16 caracteres)	**Duração até à reposição do contador de tentativas de início de sessão falhadas**	≥ 60 minutos
Complexidade	➢ Maiúsculas ➢ Minúsculas ➢ Dígitos 0–9 ➢ Sinais de pontuação ou caracteres especiais	**Casos específicos (palavras-passe do Windows – aplicadas internamente pela Arbonia e automaticamente)**	A palavra-passe não deve conter incluir dígitos na primeira e na última posição, nem conter 3 caracteres idênticos consecutivos

Não utilize as palavras-passe que são apresentadas como exemplos neste documento. Estes exemplos de palavras-passe estão agora «comprometidos» e constam na lista negra.

Para além desta nota informativa, queira também consultar a política de palavras-passe em vigor (IS-ISP-GROUP-001-PASSWORD-POLICY) em https://security.arbonia.com

Ao alterar a sua palavra-passe do Windows, os requisitos que devem ser preenchidos são exibidos de imediato.