ARBONIA
IT SECURITY

Neue Passwortrichtlinie der Arbonia Gruppe

Geschätzte Mitarbeiterinnen und Mitarbeiter

Ein starkes Passwort ist die erste Verteidigungslinie unserer Systeme und Daten.

Das Hauptziel von Angreifern ist unter anderem der Diebstahl von Zugangsdaten eines Benutzerkontos, um sich einen initialen Zugang zu unseren Netzwerken, Servern und IT-Systemen zu verschaffen und im schlimmsten Fall unbemerkt Tätigkeiten wie z.B. Datendiebstahl, Spionage oder Installation von Schadsoftware durchzuführen. Aus diesem Grund stellen schwache oder kompromittierte Passwörter sowie ein unsachgemässer Umgang mit ihnen ein erhebliches Risiko dar. Um unseren Sicherheitsanforderungen noch besser gerecht zu werden und um Sie besser vor diesen Bedrohungen zu schützen, wurde für die Arbonia Gruppe eine neue Passwortrichtlinie definiert.

Änderung der Passwortrichtlinie

Die vollständige Passwortstrategie finden Sie weiter unten übersichtlich dargestellt. Die Änderung betrifft hauptsächlich die minimale Passwortlänge, die maximale Passwortgültigkeit sowie die Komplexität.

Die minimale Passwortlänge wird von derzeit 8 auf 12 Zeichen angehoben, um das Knacken eines Passworts zu erschweren, gleichzeitig wird aber die Passwortgültigkeit auf mindestens 360 Tage verlängert. Wenn Sie ein längeres Passwort (≥ 16 Zeichen) verwenden, wird die Passwortgültigkeit auf 540 Tage verlängert. In allen Fällen muss für die neuen Passwörter eine hohe Komplexität (= starkes Passwort) sichergestellt werden. Das wird erreicht durch eine Kombination von Gross- / Kleinbuchstaben / Ziffern 0-9 / Interpunktions- oder Sonderzeichen.

Weiter wird die Verwendung von bereits kompromittierten und im Internet frei zugänglichen Passwörtern sowie Wörtern aus einer Sperrliste (z.B. Firmennamen) automatisch verhindert.

Sollte das Passwort während seiner Gültigkeit in einer Datenbank mit kompromittierten Passwörtern auftauchen, werden Sie automatisch dazu aufgefordert, das Passwort zu ändern.

Die neue Passwortrichtlinie wird automatisch bei Ihrem nächsten Windows Passwortwechsel oder der Aufforderung Ihrer lokalen IT-Abteilung aktiv. Sie erhalten jeweils 14 Tage vor dem Ablauf des Passworts eine Erinnerung. **Die Richtlinie gilt jedoch für alle ICT-Systeme der Arbonia Gruppe, d.h. auch für nicht Windows Systeme. Sie sind als Kontoinhaber in jedem Fall für die Einhaltung der Passwortrichtlinie verantwortlich, auch wenn diese technisch nicht erzwungen wird.**

Starkes Passwort erstellen

Es gibt verschiedene Techniken, um ein starkes Passwort zu erstellen und sich dieses zu merken. Bilden Sie z.B. ein starkes Passwort basierend auf einem Satz oder durch Ersetzen von definierten Zeichenfolgen:

- Wählen Sie einen Satz, welchen Sie sich gut merken können und transformieren Sie ihn in ein Passwort. Z.B.: *"Es ist gar nicht so schwierig, ein starkes Passwort zu wählen."* Verwenden Sie die Anfangsbuchstaben oder mehrere Buchstaben der einzelnen Wörter und reichern Sie das Passwort mit Ziffern und Sonderzeichen an. Z.B.: *"Eignss,1sPzw."*
- Wählen Sie ein Wort, welches Sie sich gut merken können z.B. "Nachmittag" und definieren Sie eine spezielle Zeichenfolge z.B. *"1$1"*. Nun ersetzen Sie definierte Teile / Buchstaben des Wortes mit Ihrer gewählten Zeichenfolge, um ein starkes Passwort zu erhalten. Z.B.: *"N1$1chmitt1$1g"*

Vielen Dank für Ihre Kenntnisnahme und freundliche Grüsse
Arbonia Security Team

ARBONIA
IT SECURITY

Passwortstrategie			
Passworthistorie (Anzahl letzter Passwörter, welche nicht wiederverwendet werden dürfen)	5	**Anzahl fehlgeschlagener Anmeldeversuche bis das Konto gesperrt wird**	6
Minimale Passwortlänge	12 Zeichen	**Dauer der Kontosperrung**	Bis ein Administrator entsperrt
Maximale Passwortgültigkeit	360 Tage (12-15 Zeichen) bzw. 540 Tage (≥16 Zeichen)	**Dauer bis der Zähler fehlgeschlagener Anmeldeversuche zurückgesetzt wird**	≥ 60 Minuten
Komplexität	➢ Grossbuchstaben ➢ Kleinbuchstaben ➢ Ziffern 0-9 ➢ Interpunktions- oder Sonderzeichen	**Spezielles (Windows Passwörter – Arbonia intern und automatisch durchgesetzt)**	Das Passwort darf keine Ziffern an der ersten und letzten Stelle sowie keine 3 aufeinanderfolgenden identischen Zeichen enthalten

Verwenden Sie keine Passwörter, die in diesem Dokument als Beispiel angegeben sind. Diese Beispielpasswörter sind jetzt "kompromittiert" und in der Sperrliste enthalten.

Beachten Sie zusätzlich zu diesem Informationsschreiben auch die gültige Passwortrichtlinie (IS-ISP-GROUP-001-PASSWORD-POLICY) unter https://security.arbonia.com

Beim ändern Ihres Windows Passworts werden Ihnen direkt die Anforderungen angezeigt, welche erfüllt werden müssen.