Tema 4 Managementul riscurilor

Acest document prezintă procedura de gestionare a parolelor pentru organizația imaginară, aliniată la cerințele ISO/IEC 27001 și NIST. Procedura este proiectată pentru a asigura securitatea datelor critice din sectorul energetic.

1. **Scopul procedurii**

Protejarea sistemelor informatice și a datelor sensibile (date ale clienților, infrastructură critică, date operaționale) prin:

* Limitarea accesului neautorizat
* Reducerea riscului de breșe cauzate de parole slabe
* Conformitatea cu standardele internaționale

2. **Domeniul de aplicare**

**Sisteme afectate:**

* Sisteme SCADA (controlul rețelelor electrice)
* Baze de date ale clienților
* Servere UNIX/Linux și Active Directory

**Utilizatori:**

* Angajați permanenți
* Contractori și furnizori externi

| **Criteriu** | **ISO 27001** | **NIST** | **Politica implementată** |
| --- | --- | --- | --- |
| Lungime minimă | 8 caractere | 8 caractere | 12 caractere |
| Caractere permise | A-Z, a-z, 0-9, speciale | Orice ASCII (inclusiv spații/emoji) | A-Z, a-z, 0-9, !@#$%^&\* |
| Complexitate | Mix majuscule/minuscule, numere, simboluri | Elimină cerințe obligatorii | 3 din 4 categorii |
| Actualizare | La 90 zile | Doar după incident | La 180 zile + verificare după incident |
| Istoric parole | Blocare reuse ultimele 5 | Verificare similaritate | Blocare reuse ultimele 8 |

4. **Proceduri operaționale**

**4.1 Crearea parolelor**

* **Angajați:** Folosesc generator integrat în portalul HR care aplică regulile de complexitate.
* **Sisteme tehnice:** Parole generate automat cu algoritmi PBKDF2 sau bcrypt.

**4.2 Stocarea securizată**

bash

*# Exemplu configurare Active Directory*

Set-ADDefaultDomainPasswordPolicy -Identity domain.com `

-MinPasswordLength 12 `

-PasswordHistoryCount 8 `

-ComplexityEnabled $True

powershell

*# Importă modulul Active Directory*

Import-Module ActiveDirectory

*# Setează politica de parole pentru domeniu*

Write-Host "Configurarea politicii de parole pentru domeniu..."

*# 1. Lungimea minimă a parolei*

Set-ADDefaultDomainPasswordPolicy -Identity "domain.com" -MinPasswordLength 12

Write-Host "Lungimea minimă a parolei a fost setată la 12 caractere."

*# 2. Numărul minim de zile înainte de schimbarea parolei*

Set-ADDefaultDomainPasswordPolicy -Identity "domain.com" -MinPasswordAge 1.00:00:00

Write-Host "Numărul minim de zile înainte de schimbarea parolei a fost setat la 1 zi."

*# 3. Numărul maxim de zile înainte ca parola să expire*

Set-ADDefaultDomainPasswordPolicy -Identity "domain.com" -MaxPasswordAge 90.00:00:00

Write-Host "Numărul maxim de zile înainte ca parola să expire a fost setat la 90 zile."

*# 4. Istoricul parolelor (câte parole anterioare sunt reținute)*

Set-ADDefaultDomainPasswordPolicy -Identity "domain.com" -PasswordHistoryCount 8

Write-Host "Politica de istoric al parolelor a fost setată la 8 parole anterioare."

*# 5. Activarea cerințelor de complexitate pentru parolă*

Set-ADDefaultDomainPasswordPolicy -Identity "domain.com" -ComplexityEnabled $True

Write-Host "Cerințele de complexitate pentru parolă au fost activate."

*# Confirmare finală*

Write-Host "Politica de parole a fost configurată cu succes în Active Directory."

**4.3 Utilizarea parolelor**

* Interzis partajarea parolelor între utilizatori
* Obligatoriu MFA pentru acces la sisteme critice
* Blocare automată după 10 încercări eșuate

**4.4 Actualizarea**

* Notificări automate la 7/14/21 de zile înainte de expirare
* Resetarea parolelor pierdute necesită validare biometrică + token fizic

5. **Monitorizare și conformitate**

* Scaneare lunară a bazelor de date pentru parole slabe folosind instrumente Hashcat + rainbow tables
* Audit trimestrial al jurnalelor de autentificare
* Rapoarte de conformitate generate automat pentru ISO 27001 A.9.4.3 și NIST SP 800-53 AC-6

6. **Responsabilități**

* **Echipa IT:** Implementare politică în Active Directory/UNIX
* **Responsabil securitate:** Analiza incidentelor și actualizarea listei neagre de parole
* **Angajați:** Semnare declarație de conformitate anuală