**1. Descriere**

Parolele sunt una din cele mai importante componente a securității informațiilor. Parolele servesc pentru a proteja accesul la conturile de utilizator, datele și sistemele. Cu toate acestea, o parolă compusă fără respectarea regulilor specifice de alcătuire a parolelor sau ușor de ghicit crește riscul potențial de acces neautorizat la sistemul informațional al companiei. Acest ghid oferă cele mai bune practici pentru crearea de parole puternice. Toți angajații BIG SOFTWARE COMPANY (inclusiv contractorii și terții) sunt responsabili pentru respectarea cerințelor acestei politici.

**2. Scop**

Scopul acestui ghid este de a oferi standarde pentru crearea de parole puternice, protecția acestora, stocarea și frecvența actualizărilor.

**3. Domeniul de aplicare**

Acest ghid se aplică întregului personal care are acces sau poartă răspundere pentru accesarea tuturor nivelurilor de informații confidențiale (sau orice formă de acces care acceptă sau necesită o parolă) pe orice sistem, echipament care accesează (sau stochează informații confidențiale) rețeaua corporativă a companiei. Personalul include angajați, contractanți, consultanți, lucrători temporari și alți lucrători, precum și întregul personal afiliat cu terți. Acest ghid se aplică tuturor parolelor, inclusiv, dar fără a se limita la, conturi la nivel de utilizator, conturi la nivel de sistem, conturi web, conturi de e-mail, protecție cu economizor de ecran (screensaver), mesagerie vocală și autentificări la router local.

**4. Politică**

**4.1 Cerințe**

Parolele pentru conturile de sistem (administrator de domeniu, administrator local, root etc.) trebuie schimbate fiecare trei luni.

Toate parolele pentru conturile de sistem, precum și parolele pentru aplicații și echipamente active, trebuie să fie stocate într-o bază de date criptată, la care accesul este restricționat.

Parolele conturilor de domen nu trebuie să fie utilizate mai mult de 9 luni.

Parola pentru un cont de utilizator care are privilegii administrative obținute prin apartenența la grup sau cu ajutorul programelor (de exemplu sudo) trebuie să fie unică față de parole ale altor conturi utilizatorului.

Este interzisă transferarea parolelor către utilizatori prin intermediul mesajelor de e-mail sau în orice alt mod deschis prin Internet.

Parola primită de utilizator trebuie schimbată la prima conectare in sistem.

În cazul utilizării protocolului SNMP, este necesar ca șiruri de conexiune (Community Name) utilizat să difere de valorile standard „public”, „privat”, „sistem” și șă difere față de parola utilizată pentru autentificarea în sistem.

Parolele pentru toate tipurile de conturi trebuie să conțină litere ale alfabetului latin, dar în mod obligatoriu și cifre și/sau simboluri speciale. Numărul cifrelor și/sau simbolurilor speciale trebuie să fie 2 minimum.

Parolele puternice sunt lungi, cu cât o parolă are mai multe caractere, cu atât este mai puternică. Minimul stabilit este de 15 caractere în toate parolele de lucru.

Se încurajează utilizarea frazelor de acces, parole formate din mai multe cuvinte. Exemplele includ „Este t1mpul pentru vacanta!”. Frazele de acces sunt ușor de reținut și de tastat, dar îndeplinesc cerințele de putere.

Se permite utilizarea în parole ale caracterelor specifice limbilor română, germană, franceză, italiană, portugheză, suedeză. În cazul utilizării, caracterele specifice limbilor mențioate nu se echivalează cu simboluri speciale.

Spargerea sau ghicirea parolelor poate fi efectuată periodic sau aleatoriu de către Echipa Securitate Informațională sau delegații săi. Dacă o parolă este ghicită sau spartă în timpul uneia dintre aceste scanări, utilizatorului i se va cere să o schimbe.

Toate parolele de utilizator, precum și parolele de sistem trebuie să respecte această politică.

**4.2 Instrucțiuni**

Instrucțiuni pentru crearea unei parole.

BIG SOFTWARE COMPANY folosește parole în diverse scopuri. Printre acestea: acces la contul de utilizator, la interfețe web, la e-mail, pentru a proteja screen saver-ul, parole de mesagerie vocală și acces la routere. În continuare sunt prezentate istrucțiunile pentru a alege o parolă puternică.

Parolele proaste, slabe au următoarele caracteristici:

Conține mai puțin de 15 caractere.

Acestea conțin termeni și nume de computer, comenzi, nume de site-uri, companii, echipamente, software.

Conține numele companieis și numele geografice.

Conține datele de naștere și alte informații personale, cum ar fi adrese și numere de telefon.

Model de cuvinte sau numere precum aaaaaaaabbbbbbbb, qwertyqwertyqwerty, 123451234512345 etc.

Exemplele anterioare cu un număr/literă la începutul sau la sfârșitul parolei.

Opțiuni pentru parole puternice

Conține o combinație de litere mari și mici (de exemplu, a-z, A-Z).

Include numere și semne de punctuație, de exemplu, 0-9, !@#$%^&\*()\_+|~-=\`{}[ [ ] ]:";'<>?,./).

Este formată din 15 sau mai multe caractere.

Nu se bazează pe informații personale, cum ar fi numele de familie, data nașterii etc.

Nu a fost niciodată înregistrat sau stocat online.

Creați parole ușor de reținut. O modalitate de a crea astfel de parole este să folosești cântece, poezii și alte expresii captivante. De exemplu, din expresia: „This may be a way to remember” puteți obține următoarele parole: „TmB1w2R!” sau „Tmb1W>r~” și alte opțiuni.

Atenție: Nu utilizați niciunul dintre exemplele anterioare ca parolă!

**Reguli de protejare a parolelor**

Nu utilizați aceeași parolă pentru a accesa conturile BIG SOFTWARE COMPANY și alte resurse (de exemplu, acces la Internet de acasă, sisteme de comerț electronic etc.). Dacă este posibil, nu utilizați aceeași parolă pentru a accesa diferite resurse din cadrul companiei. De exemplu, utilizați o parolă pentru aplicații și alta pentru administrarea resurselor.

Nu împărtășiți parola cu nimeni, nici colegilor. Toate parolele sunt informații confidențiale ale BIG SOFTWARE COMPANY.

**Lista acțiunilor interzise.**

Nu comunicați parola nimănui prin telefon.

Nu trimiteți parola prin e-mail.

Nu comunicați parola șefului tău.

Nu vorbi despre parola ta în preajma unor străini.

Nu menționați conținutul parolei (de exemplu, „ziua mea de naștere”).

Nu introduceți parola în chestionare.

Nu împărtășiți parola cu membrii familiei dvs.

Nu împărtășiți parola cu colegii înainte de a pleca în vacanță.

Nu notați parola și nu o păstrați la locul de muncă.

Nu stocați parola într-un fișier de pe un computer, inclusiv unul portabil, fără criptare.

Nu utilizați funcția „Reține parola” în aplicații precum browser, Eudora, Outlook sau Netscape Messenger.

Dacă cineva vă cere parola, consultați acest document sau cereți-i să sune departamentul de securitate a informațiilor.

Dacă credeți că contul sau parola dvs. a fost compromisă, raportați-o departamentului de securitate a informațiilor al BIG SOFTWARE COMPANY și schimbați toate parolele.

Persoanele autorizate ale BIG SOFTWARE COMPANY pot ghici sau încerca în mod regulat să spargă parolele. Dacă o parolă este ghicită sau compromisă în timpul acestor evenimente, vi se va cere să vă schimbați parola.

**Standarde de dezvoltare a aplicațiilor**

Dezvoltatorii de aplicații ar trebui să ofere următoarele măsuri de securitate în programele lor:

Aplicațiile ar trebui să accepte autentificarea pentru utilizatori individuali, nu pentru grupuri.

Aplicațiile nu ar trebui să stocheze parolele în text simplu sau într-o formă ușor accesibilă.

Aplicațiile trebuie să ofere un transfer de drepturi, astfel încât un utilizator să poată îndeplini funcțiile altuia fără a-și cunoaște parola.

Aplicațiile ar trebui să accepte întotdeauna TACACS+, RADIUS și/sau X.509 bazat pe LDAP.

**Utilizarea parolelor și frazelor de acces pentru accesul de la distanță**

Pentru a controla accesul de la distanță la rețelele BIG SOFTWARE COMPANY, utilizați fie parole unice, fie un sistem de chei asimetrice cu o expresie de acces puternică.

Frazele de acces sunt diferite de parole. O frază de acces este o versiune mai lungă a unei parole și, prin urmare, mai sigură. Frazele de acces sunt utilizate în mod obișnuit pentru autentificare în sistemele de criptare asimetrică. Un sistem de cheie asimetrică definește o relație matematică între o cheie publică cunoscută de toată lumea și o cheie privată cunoscută doar de proprietarul său. Fără o frază de acces care să ofere acces la cheia privată, utilizatorului nu i se va acorda acces.

Fraza de acces constă de obicei din mai multe cuvinte, fiind mai rezistentă la atacurile din dicționar. O expresie de acces bună este relativ lungă și conține o combinație de litere mari și mici, precum și numere și semne de punctuație. Iată un exemplu de expresie de acces bună: „The\*?#>\*@TrafficOnThe101Was\*&#!#This Morning”

Toate regulile pentru crearea de parole puternice se aplică și frazelor de acces.

**5. Respectarea politicii**

**5.1 Măsurarea conformității**

Echipa de Securitate Informațională va verifica conformitatea cu această politică prin diferite metode, inclusiv, dar fără a se limita la, exerciții de spargere a parolelor, rapoarte de instrumente de afaceri, audituri interne și externe și feedback pentru proprietarul politicii.

**5.2 Excepții**

Orice excepție de la politică trebuie să fie aprobată de echipa de Securitate Informațională în prealabil.

**5.3 Neconformitate**

Un angajat constatat că a încălcat această politică poate fi supus unor măsuri disciplinare.

**6. Standarde, politici și procese conexe**

Politica de gestionare VPN.

**7. Definiții și termeni**

**8. Istoricul revizuirilor**

|  |  |  |
| --- | --- | --- |
| Data Modificării | Responsabil | Descriere |
| Dec 2013 | BSC Policy Team | Adăugarea exemplelor de fraze de acces. |
|  |  |  |