

DRŽAVNI IZPITNI CENTER
Kajuhova 32U
1000 Ljubljana



Politika gesel

1. Povzetek

Gesla so pomemben vidik informacijske varnosti in predstavljajo prvo obrambno linijo zaščite uporabniških imen. Slabo izbrana gesla so lahko vzrok za zlorabo na celotnem omrežju podjetja. Vsi zaposleni na RIC-u, vključno z vsemi zunanjimi izvajalci in poslovnimi partnerji, ki imajo dostop do informacijskega sistema podjetja so odgovorni za izvajanje ukrepov in postopkov, ki bodo podani v nadaljevanju, za izbiro in varovanje gesel.

2. Namen

Namen te politike je vzpostavitev standardov za kreiranje varnih gesel, varovanje teh gesel in pogostost spreminjanja teh gesel.

3. Področje veljavnosti

Ta politika se nanaša na vse zaposlene, ki jim je bil dodeljen ali so odgovorni za uporabniški račun (kakršen koli dostop do sistema, pri katerem je potrebno vnesti geslo) na katerem koli sistemu v okviru RIC-a, imajo dostop do omrežja podjetja ali shranjujejo kakršne koli zaupne podatke na sistemih v okviru RIC-a.

4. Politika

4.1. Splošno

- Vsa sistemska gesla produkcijskih sistemov morajo biti vpisana v register sistemskih gesel, ki ga vodi služba za varovanje informacij.
- Gesla uporabniških računov (elektronska pošta, spletni strežniki, osebni računalniki) se spreminjajo po potrebi glede na oceno informacijskega centra in v dogovoru z direktorjem. Prepogosto spreminjanje gesel vodi k temu, da si jih uporabniki ne zapomnijo in si jih zapisujejo na bolj ali manj dostopna mesta. Zamenjava gesel vsak mesec je nepraktična, menjava na daljši čas pa ne rešuje problema z ogroženim geslom. V tem je lahko do vdora že prišlo.
- Gesla v nobenem primeru ne pošiljamo po elektronski pošti ali kateri drugi obliki elektronske komunikacije.
- Vsa uporabniška sistemska gesla morajo biti skladna z zgornjimi določili.

4.2. Smernice

4.2.1. Splošna vodila za kreiranje gesel

V okolju RIC-a se gesla uporabljajo za različne namene. Nekateri izmed teh namenov so uporabniški računi, dostop do elektronske pošte, za ohranjevalnike zaslona in prijavo na lokalne usmerjevalnike. Ker povsod ni mogoče izvesti avtentikacije z enkratnimi gesli (sproti kreirana gesla za enkratno uporabo) se mora vsak spoznati z načini izbiranja močnih gesel.

Slaba gesla imajo sledeče značilnosti:

- Geslo vsebuje manj kot osem znakov
- Geslo je beseda, ki jo lahko najdemo v slovarju
- Geslo je vsakdanja beseda kot so:
 - Imena članov družine, hišnih ljubljencev, prijateljev, sodelavcev, ...
 - Računalniški izrazi in nazivi, ukazi, imena podjetij, strojne in programske opreme
 - Izpeljanke z znanimi predponami (»svetijošt«)
 - Rojstni datumi ali drugi osebni podatki, naslovi, telefonske številke
 - Nizi znakov kot so aaabbb, qwerty, zyxwvuts, 123321
 - Znane besede črkovane nazaj.
 - Znane besede s številčno predpono ali pripono.

Geslo za uporabniške račune zaposlenih na RIC-u mora biti dolgo vsaj 10 znakov in vsebovati male in velike črke ter številke. Opomba: uporabniški računi so dostopni samo iz notranje mreže RIC-a in niso dostopni iz spleta. Za dostop iz zunanjih omrežij je potreben VPN dostop, ki se dodeli uporabnikom le izjemoma z dovoljenjem direktorja. Za VPN dostop uporabnik dobi dodatno uporabniško ime in geslo.

Gesel si nikoli ne zapisujemo ali jih hranimo na lahko dostopnih mestih. Izmislimo si gesla, ki si jih lahko zapomnimo. Eden izmed načinov je da uporabimo kot osnovo naslov svoje priljubljene popevke ali podobne fraze. Če vzamemo stavek »To je način, da si zapomnimo geslo.« nam lahko da geslo »Tjn,dsZg« ali kaj podobnega.

Načeloma gesla uporabnikom določi informacijski center, lahko pa si ga uporabnik spremeni.

4.2.2. Standardi varovanja gesel

Ne uporabljajte istih gesel za uporabniške račune v službi in zasebne uporabniške račune (zasebni Internet dostop, elektronsko bančništvo in podobno). Kjer je mogoče ne uporabljajte isto geslo za dostope do različnih sistemov v podjetju (geslo za dostop do razvojnega sistema naj bo drugačno kot tisto za dostop do elektronske pošte).

Ne razkrivajte svojih gesel nikomur, vključno sistemskim administratorjem ali bližnjim sodelavcem. Vsa gesla se v okviru RIC-a obravnavajo kot zaupna informacija.

Seznam stvari, ki jih z gesli ne počnemo:

- Nikomur ne razkrivamo gesel po telefonu
- Gesel ne pošiljamo po elektronski pošti
- Ne razkrivamo gesel svojim predpostavljenim
- Svojih gesel ne omenjamo med razgovori
- Ne razkrivamo namigov o vsebini in obliki gesel
- Gesel ne zapisujemo na nobeno anketo ali kak drug dokument
- Gesel ne razkrivamo članom svoje družine
- Ne razkrivamo svojih gesel v primeru daljše odsotnosti

Če kdo od vas zahteva, da razkrijete svoja gesla ga usmerite na ta dokument ali na službo za varovanje informacij.

Še enkrat poudarjamo, ne zapisujte si gesla in jih ne shranjujte v pisarni. Ne shranjujte gesel na katerem koli sistemu (vključujoč GSM, osebne asistente in podobno) v datoteke, ki niso s šifriranjem zaščitene pred branjem.

Če sumite, da sta bila uporabniško ime in geslo zlorabljeni, to takoj javite v službo za varovanje informacij.

4.2.3. Standardi za razvoj aplikacij

Razvijalci aplikacij morajo zagotoviti, da njihova programska oprema vsebuje ustrezne varnostne mehanizme.

Programska oprema naj bi:

- omogočala avtentikacijo uporabnika in ne skupine uporabnikov
- omogočala shranjevanje gesla v obliki, da le ta niso čitljiva oz. jih ni mogoče z enostavno operacijo pretvoriti v čitljivo geslo
- omogočala dodelitev vlog, tako da lahko izbrani uporabnik enostavno prevzame vlogo drugega uporabnika brez poznavanja njegovega gesla

4.2.4. Daljša gesla

Daljša gesla se v splošnem uporabljajo za avtentikacijo z javnimi/zasebnimi ključi. Sistem javnih/zasebnih ključev določa matematično relacijo med javnim ključem, ki je javen in dostopen vsem, in zasebnim ključem, ki je znan in dostopen samo lastniku ključa. Uporaba zasebnega ključa je možna samo ob poznavanju daljšega gesla.

Daljša gesla niso isto kot gesla. Daljše geslo je daljša inačica gesla in zaradi svoje dolžine bolj varno. Daljše geslo je ponavadi sestavljeno iz več besed in je tako bolj varno in odporno na t.i. napad z uporabo slovarja.

Dobro daljše geslo je relativno dolgo in vsebuje kombinacije velikih in malih črk, števil in posebnih znakov.

Vsa pravila, ki so bila omenjena v zgornjem besedilu in se nanašajo na gesla, se morajo upoštevati tudi pri daljših geslih.

Pripravil: Matjaž Urank

Številka: 071-3/2020-5

Datum: 9. 1. 2020



Dr. Darko Zupanc,
Direktor Rica