ARBONIA

IT SECURITY

Politika sigurnosti informacija

Smernice za lozinke

Verzija:	1.0
Doneta dana:	08.07.2021. godine
Status:	RELEASED
Klasifikacija:	RESTRICTED
Sastavljena od strane:	ICT Security Officer
Doneta od strane:	Arbonia IT Board
Smernice:	IS-ISP-GROUP-001-PASSWORD-POLICY
Revizija:	n/a

Informacije o smernicama

Svrha	Smernice o lozinkama opisuju i definišu osnove za kreiranje, postupanje i upotrebu lozinki u Arbonia grupi.
Korisnici / primaoci	▪ Svi zaposleni Arbonia grupe ▪ Eksterni nalogoprimci / pružaoci usluga / klijenti i partneri koji imaju pristup IKT sistemima Arbonia grupe
Elektronsko odlaganje dokumenata	https://security.arbonia.com

Napomena o promenama

Verzija	Datum	Status	Promena	od strane
0.1	2021-06-14	Draft	Draft of the policy	ICT Security Officer
0.9	2021-07-07	Draft	Draft for adoption	ICT Security Officer
0.9	2021-07-07	Review		Arbonia IT Board
1.0	2021-07-08	Adoption		Arbonia IT Board

Sadržaj

Skraćenice

Pojam	Opis
IKT	Informations and Communications Technology (informacione i komunikacione tehnologije)
OS	Operating System (operativni sistem)
ISMS	Sistem za upravljanje sigurnošću informacija

Glosar

Pojam	Opis
Napad grubom silom	Kod napada grubom silom radi se o pokušaju da se otkrije lozinka ili korisničko ime isprobavanjem svih mogućnosti.
Sistem za upravljanje sigurnošću informacija	Sistem za upravljanje sigurnošću informacija je niz uspostavljanjenih procedura i pravila unutar organizacije koji služe tome da se trajno definiše, upravlja, kontroliše, održava i kontinuirano poboljšava sigurnost informacija.

1 Svrha, oblast primene i korisnici

Smernice opisuju zahteve za lozinke i zahteve za pristup IKT sistemima Arbonia grupe. Određuju pravila za sigurno upravljanje, upotrebu i kreiranje lozinki.

Smernice važe za sve oblasti primene sistema za upravljanje sigurnošću informacija (ISMS), tj. za sve IKT sisteme Arbonia grupe.

Korisnici i primaoci ovih smernica su svi zaposleni Arbonia grupe kao i eksterni nalogoprimci / pružaoci usluga / klijenti / partneri i dr. kojima je potreban pristup IKT sistemima Arbonia grupe.

2 Načela upravljanja

2.1 Značaj lozinki

Sigurnost IKT sistema Arbonia grupe se, između ostalog, zasniva na tome koliko se pažljivo postupa sa lozinkama, i, pre svega kako se poštuju osnovni principi za upotrebu lozinki.

Glavni cilj napadača je krađa pristupnih podataka nekog korisnika, kako bi sebi obezbedili pristup IKT sistemima Arbonia grupe i zatim pronašli i iskoristili potencijalne slabosti sistema. Pokušavaju da prisvoje privilegovana prava sistemskog administratora, čime u najgorem slučaju mogu neprimećeno izvršiti razne aktivnosti poput krađe podataka, špijunaže ili instalacije malicioznog softvera (malver). Iz tog razloga slabe lozinke kao i nepravilno postupanje sa njima predstavljaju značajan rizik. Ovaj rizik dodatno je povećan zbog neophodnog korišćenja privilegovanih prava, koja su često potrebna za obavljanje radnih aktivnosti.

Zbog toga je obavezno da se spreči krađa pristupnih podataka i da se poštuju sledeće obaveze.

2.2 Obaveze korisnika / vlasnika naloga

Svi korisnici prilikom odabira i upotrebe lozinki moraju koristiti proverene i sigurne procedure (više detalja u poglavlju 3):

- Mora se uvek izabrati „jaka" lozinka. Izbor dužine i formata lozinke mora biti takav da napad grubom silom iziskuje mnogo vremena i ne dovodi do uspeha
- Lozinke se ne smeju otkriti drugim osobama. Ni nadređenima, direktorima ili sistemskim administratorima
- Lozinke se ne smeju zapisati ili čuvati na nepravilan način (npr. u Excelu), osim ako IT odeljenje nije odobrio siguran metod (npr. alat za lozinke)
- Lozinka se mora menjati u redovnim intervalima
- Lozinke se moraju promeniti kada postoje naznake da su postale dostupne javnosti, tj. trećim licima
- Naznake zloupotrebe lozinki moraju se odmah javiti odgovornom IT odeljenju
- Ako korisnik/ca ima namenski korisnički nalog sa administratorskim pravima, ne sme se koristiti ista lozinka kao za standardni nalog
- Vlasnik naloga je u svakom slučaju odgovoran za poštovanje smernica za lozinke, čak i ne bude tehnički prisiljen da ih primeni. Ni u kom slučaju se ne smeju koristiti standardne, prazne ili slabe lozinke

3 Smernice za lozinke

3.1 Definicija

Da bi se postigao primereni nivo sigurnosti informacija, koriste se različite smernice za lozinke u skladu sa potrebnim privilegijama. Razlikuje se između:

- Opšte upotrebe tipa „Korisnik", bez administrativnih privilegija na IKT sistemima
- Specifične upotrebe tipa „Administrator", sa administrativnim privilegijama na jednom ili više IKT sistema. Korisnički nalozi tipa „Administrator" razlikuju se po:
    - Nalogu za uslugu / sistem / servis (koristi se za automatizovane funkcije, instalaciju ili upravljanje komponentama u IKT sistemima, kao što su OS, baze podataka, aplikacije ili mrežni nalozi i dr.)
    - Administratorskom nalogu (koristi se za pojedince da bi im se omogućila privilegovana prava za IKT sisteme)

3.2 Upravljanje lozinkama

1. Lozinka je je dodeljena jedinstvenom ID-u naloga (korisnik ili administrator)
2. I ID i lozinka su lične prirode. Lozinka je poznata samo odgovarajućoj osobi.
3. Lozinka ne sme biti sačuvana u običnom tekstu
4. Trajanje lozinke ne sme nikada biti duže od 360 dana odn. 540 dana (vidi poglavlje 3.3)
5. Nova lozinka biće odbijena ako se nalazi u 5 poslednjih korišćenih lozinki
6. Broj neuspelih pokušaja unosa lozinke ograničen je na 6. Nalog će biti blokiran nakon šestog neuspelog pokušaja, sve dok ga ponovo ne odblokira administrator.
7. Brojač neuspelih pokušaja prijave ne sme se resetovati za manje od 60 minuta
8. Privremene lozinke smeju trajatati najduže 72 sata, a od korisnika se prilikom prve prijave mora zahtevati da promeni privremenu lozinku. To važi ukoliko je tehnički izvodljivo. Ako nije, svaki vlasnik naloga je sam odgovoran za ovu promenu lozinke
9. Prilikom otvaranja korisničkog naloga, lozinka se automatski dodeljuje prema istim zahtevima

Specijalna pravila za naloge za usluge / sistem / servise:

- Izuzetak od pravila br. 2: lozinke koje su povezane sa ovom vrstom naloga mogu se čuvati u sigurnom (šifrovanom) alatu za lozinke sa pristupom zaštićenim lozinkom i podeliti sa više osoba preko definisanih grupa za uloge i prava, ukoliko je to neophodno za obavljanje njihovih aktivnosti
- Izuzetak od pravila br. 4: lozinke koje su povezane sa ovom vrstom naloga smeju, ako je potrebno, imati aktiviranu opciju lozinke koja nikad ne ističe
- Izuzetak od pravila br. 6: lozinke koje su povezane sa ovom vrstom naloga ne moraju se automatski blokirati

Postupanje u izuzetnim slučajevima može se videti u poglavlju 3.5.

3.3 Zahtevi za lozinke

Lozinka za nalog tipa **„Korisnik" bez** administrativnih privilegija na IKT sistemima mora ispuniti sledeće zahteve:

- Sadrži najmanje 12 znakova da bi lozinka trajala 360 dana odn. najmanje 16 znakova da bi lozinka trajala 540 dana
- Ima kompleksnost od 4 od 4, što znači da se sledeći znakovi moraju koristiti najmanje jednom:
    - Velika slova
    - Mala slova
    - Brojevi 0–9
    - Znakovi interpunkcije ili posebni znakovi (ne prihvataju se svi IKT sistemi sve znakove)
- Ne sme sadržati ime naloga
- Ne sme sadržati brojeve na prvom i poslednjem mestu
- Ne sme sadržati 3 identična znaka jedan za drugim

Za lozinke za nalog tipa **„Administrator" sa** administrativnim privilegijama na IKT sistemima dodatno važe sledeća posebna pravila:

Specijalna pravila za naloge za usluge / sistem / servise:

- Sadrži najmanje 32 znaka
- Lozinka mora biti generisata nasumično i dokumentovana pomoću prikladnog alata za lozinke (vidi izuzetak od pravila br. 2, poglavlje 3.2)

Posebna pravila za administratorske naloge:

- Sadrži najmanje 15 znakova

Posebna pravila za sisteme trećih lica (B2C / B2B i drugi) kojima upravlja Arbonia grupa:

Zahtevi za lozinke važe u suštini i za sisteme trećih lica, ali u zavisnosti od situacije i ako je potrebno mogu biti prilagođeni odgovarajućem slučaju poslovne upotrebe. Posebna pravila moraju u svakom slučaju biti tretirana prema poglavlju 3.5.

Posebni zahtevi za naloge za Windows – u Arbonia grupi se sprovode interno i automatski:

- Novopostavljena lozinka ne sme postojati u bazi podataka sa kompromitovanim lozinkama. To će biti sprečeno pomoću tehničke provere prilikom postavljanja lozinke
- Novopostavljena lozinka ne sme se pojavljivati u rečniku definisanom od strane korisnika. Taj rečnik se uređuje centralno i sadrži, između ostalog, ime kompanije. Nedozvoljene reči biće odmah prikazane ako su izabrane u lozinci
- Lozinka se mora promeniti ako pojavi u bazi podataka sa kompromitovanim lozinkama

3.4 Strategija za lozinke

Istorija lozinki	5
Maksimalno trajanje lozinke	360 dana (12–15 znakova) odn. 540 dana (≥16 znakova)
Minimalno trajanje lozinke	0
Kompleksnost	4/4 (velika slova / mala slova / brojevi 0–9 / znakovi interpunkcije ili posebni znakovi)
Minimalna dužina lozinke o Korisnik o Nalozi za usluge / sistem / servise: o Administratorski nalozi	 12 znakova 32 znaka (generisana nasumično) 15 znakova
Obrnuto šifrovanje (Windows domen)	deaktivirano
Broj neuspelih pokušaja prijavljivanja dok se ne blokira nalog	6
Trajanje blokiranja naloga	Dok administrator ne odblokira nalog
Trajanje dok se ne resetuje brojač neuspelih pokušaja prijavljivanja	≥ 60 minuta
Posebno (Windows domen)	Lozinka ne sme sadržati brojeve na prvom i poslednjem mestu Lozinka ne sme sadržati 3 identična znaka jedan za drugim

3.5 Izuzeci / posebno

Sve procedure za autentifikaciju zasnovane na računarima treba u najvećoj mogućoj meri da se pridržavaju zahteva ovih smernica i da provere njihovo poštovanje. Kada nedostaju tehnički uslovi za implementaciju, uslovi se moraju osigurati pomoću manuelnog procesa od strane odgovarajućeg vlasnika naloga, a i mora se koristiti jaka lozinka u granicama mogućnosti sistema.

Lokalni službenik za IT sigurnost može dodeliti izuzetna odobrenja koja odstupaju od ovih smernica, ukoliko su ispoštovana načela sigurnosti informacija i ne postoji opasnost za IKT siteme Arbonia grupe. Ako je potrebno, on će nakon konsultacija sa službnikom za IKT sigurnost doneti odluku o dodeljivanju izuzetnog odobrenja ili definisati druge mere u cilju minimizacije rizika. Svi izuzeci moraju biti zapisani u pisanoj firmi u registru.

4 Kreiranje jakih lozinki

Postoje razne tehnike za kreiranje jake lozinke i za pamćenje iste:

Primer 1: Kreiranje jake lozinke koja se zasniva na rečenici

Izaberite rečenicu koju možete lako zapamtiti i pretvorite je u lozinku.

Primer: „Nije uopšte teško izabrati jaku lozinku.".

Koristite prvo slovo ili više slova svake pojedinačne reči i obogatite lozinku brojevima i posebnim znakovima.

Npr.: „Niuote1izjalo."

Primer 2: Kreiranje jake lozinke zamenom znakova

Izaberite neku reč koju možete lako zapamtiti, npr. „automobile" i definišite poseban niz znakova, npr. „1$1". Definisane delove / slova te reči sada zamenite izabranim nizom posebnih znakova da biste dobili jaku lozinku.

Npr. aut1$1m1$1bile

Vodite računa da za kreiranje vaše lozinke nikada ne koristite informacije koje su slobodno dostupne na društvenim mrežama. Dodatne savete na temu sigurnosti lozinke možete dobiti na našim obukama na temu svesti o IT sigurnosti.

5 Referentni dokumenti

- IS-ISS-GROUP-001-INFORMATION-SECURITY-STRATEGY
- IS-GISP-GROUP-001-GENERAL-INFORMATION-SECURITY-POLICY
- IS-SISD-GROUP-001-PSSS-SPECOPS
- Smernice za korišćenje IT sistema u Arbonia grupi

6 Stupanje na snagu

Ime	Poslovna jedinica	Funkcija	Datum	Potpis
Patrick Langenegger	Corporate IT	CIO Arbonia Group / CIO Division Doors	2021-07-08	n/a
Michael Kreter	Division HVAC / Sanitary	CIO Division HVAC / Sanitary	2021-07-08	n/a
Tobias Shibli	Division Windows	CIO Division Windows	2021-07-08	n/a
Reto Knechtle	Corporate IT	Head of IT Infrastructure	2021-07-08	n/a

7 Relevantni prilozi

Br.	Opis	Ime datoteke
1	IS-ISP-GROUP-001-COM001-EMPLOYEE-INFORMATION	