PROCEDURA

UPRAVLJANJA ZAPORKAMA

Općina Topusko

ODOBRIO
Ivica Kuzmić, općinski načelnik

Topusko, 26. rujna 2019.

Uvod

Zaporke su najčešće upotrebljavan mehanizam autentifikacije korisnika. Međutim, zbog neprimjerenih navika korisnika informacijskog sustava (primjerice dijeljenja zaporka i njihove neadekvatne pohrane te upotrebe neprimjerenih zaporka) one su i jedan od najslabijih mehanizama autentifikacije. Primjereno upravljanje zaporkama (koje uključuje uklanjanje poznatih ranjivosti i prevenciju uobičajenih napada) može uvelike unaprijediti sigurnost informacijskog sustava.

Napadi na zaporke odnosno pokušaji njihova otkrivanja ili zaobilaženja jedna su od najčešćih vrsta napada na informacijske sustave. Neke od najčešćih podvrsta napada na zaporke jesu:

- pokušaj pogađanja zaporka isprobavanjem svih kombinacija dopuštenih simbola (engl. dictionary attack)
- pokušaj pogađanja zaporka pomoću specifičnih informacija o osobi koja rabi tu zaporku (primjerice ime supružnika, imena djece, ime kućnog ljubimca i slično)
- pokušaj neautorizirane autentifikacije pomoću standardnih zaporka koje inicijalno definiraju proizvođači hardvera, softvera i telekomunikacijske opreme
- pokušaj neautorizirane autentifikacije pomoću zaporka čija je povjerljivost narušena zbog neadekvatne pohrane.

Zbog mnogobrojnih ranjivosti koje proizlaze iz neadekvatnog korištenja zaporki, te velikog broja prijetnja koje pokušavaju iskoristiti te ranjivosti, Općina Topusko (u daljnjem tekstu: Općina) ovom procedurom propisuje restriktivne postupke upravljanja zaporkama, kako bi se osjetljivost na tu vrstu napada svela na najmanju moguću mjeru.

Pravila kreiranja i upravljanja zaporkama

U cilju podizanja nivoa sigurnosti informacijskog sustava Općine propisane su slijedeće karakteristike zaporki obavezne za sve korisnike informacijskog sustava Općine:

1. Minimalna dužina zaporke

Propisuje se minimalna dužina zaporke od šest (6) znakova.

2. Ne koristiti riječi iz rječnika

S obzirom da hackeri posjeduju zbirke rječnika, što im olakšava probijanje zaporki (tzv. dictionary attack) zabranjeno je koristiti riječi iz rječnika.

3. Izmiješati mala i velika slova s brojevima

Obavezno treba izmiješati i mala i velika slova s brojevima.

4. Ne koristiti imena bliskih osoba, ljubimaca, datume

Ne smiju se koristiti zaporke koje predstavljaju imena osoba ili ljubimaca, značajne osobne ili porodične datume.

6. Tajnost zaporke

Korisnici su odgovorni za svoju zaporku i ni u kom je slučaju ne smiju otkriti, čak ni administratorima sustava.

Korisnik mora promijeniti zaporku ako postoji sumnja ili je utvrđeno da je zaporku neovlašteno otkrila druga osoba u Općini ili izvan Općine.

7. Čuvanje zaporke

Zaporke se ne smiju ostavljati na papirićima koji su zalijepljeni na ekran ili ostavljeni na stolovima, u nezaključanim ladicama itd. Korisnik je odgovoran za tajnost svoje zaporke, te mora naći način da je sakrije. Ukoliko korisnik zaboravi zaporku, administrator će mu omogućiti da unese novu.

8. Administriranje zaporki

Na računalima koja spadaju u zonu visokog rizika administratori su dužni konfigurirati sustav na taj način da se korisnički račun zaključa nakon tri neuspjela pokušaja prijave.

Prilikom provjere sustava referent za IT sigurnost može ispitati da li su korisničke zaporke u skladu s navedenim pravilima.

Dodjela inicijalne zaporke

Administrator sustava, kod otvaranja novog korisnika, kreira inicijalnu zaporku evidentirajući pri tome slijedeće podatke:

- Korisnik – ime i prezime
- Informacijski sustav za koji se dodjeljuje zaporka
- Korisničko ime (username)
- Inicijalna zaporka

Obaveza korisnika je promjena inicijalne zaporke kod prve prijave na sustav.

Kod preuzimanja inicijalne zaporke korisnik potpisuje Izjavu o preuzimanju zaporke – *Dodatak 1* ovoj proceduri.

Dodatak 1

Izjava o preuzimanju zaporke

Korisnik: Ime i prezime
Aplikacija / IT sustav:
Korisničko ime (username):
Inicijalna zaporka:

Obaveza je promjena inicijalne zaporke kod prve prijave na sustav.

U kreiranju nove zaporke svi korisnici su dužni poštivati slijedeća pravila:

- minimalna duljina zaporke je 6 znakova,
- zaporka mora biti kombinacija velikih i malih slova i znamenki,
- u zaporkama su dozvoljeni i znakovi interpunkcije,
- kao zaporku obavezno izbjegavati
    - korištenje riječi iz javno dostupnih rječnika,
    - korištenja imena bliskih osoba, ljubimaca, karakterističnih datuma i njihovih kombinacija

Zaporke se ne smiju ostavljati na papirićima koji su zalijepljeni na ekran ili ostavljeni na stolovima, u nezaključanim ladicama itd. Korisnik je odgovoran za tajnost svoje zaporke, te mora naći način da je sakrije. Ukoliko korisnik zaboravi zaporku, administrator će mu omogućiti da unese novu.

Preuzimanjem ovog dokumenta korisnik je svjestan da

- Davanje podataka o vlastitom identitetu (korisničko ime, lozinka) drugima u Općini i / ili izvan Općine
- Preuzimanje tuđeg identiteta (korištenje opreme s tuđim korisničkim računom, slanje elektroničke pošte pod tuđim imenom, kupovanje preko interneta s tuđom kreditnom karticom itd.),

predstavljaju teži oblik nedozvoljenog korištenja računala te će kao takvi biti sankcionirani.

U Topuskom, Korisnik (ime i prezime)

_____
Potpis

Ovaj dokument je sačinjen u 2 (dva) istovjetna primjerka od kojih 1 (jedan) zadržava Općina Topusko a 1 (jedan) dobiva Korisnik.