Prilog 1: Pravilnik o rukovanju zaporkama

Svrha

Prosječan korisnik nerijetko smatra kako ne mora brinuti o sigurnosti jer njegovo računalo ne sadrži vrijedne informacije. No kompromitiranjem jednog osobnog računala u lokalnoj mreži ili jednog korisničkog računa na poslužitelju napadač je probio obrambenu liniju i otvorio prolaz za napade na važnije sustave i informacije. Lanac puca na najslabijoj karici. Stoga je svaki korisnik dužan izborom zaporke i njezinom povremenom promjenom doprinositi zaštiti ukupnog sustava.

Dok snaga računala neprestano raste, ljudske sposobnosti stagniraju. Današnja računala mogu brzo dekriptirati jednostavne zaporke, dok u isto vrijeme većina ljudi ne može pamtiti složene zaporke dugačke osam znakova.

Doseg

Svi zaposlenici KBF-a, suradnici i studenti koji u svome radu koriste računala dužni su pridržavati se ovih pravila korištenja zaporki, dok su ih administratori dužni tehnički ugraditi u sve sustave koji to omogućavaju.

Pravila za korištenje zaporki

1. Minimalna dužina zaporke

   Kratku zaporku lakše je probiti. Stoga neka minimalna dužina zaporke bude osam znakova, ali preporučuje se korištenje još dužih zaporki.

2. Ne koristiti riječi iz rječnika

   Hackeri posjeduju zbirke rječnika, što im olakšava probijanje ovakvih zaporki (tzv. dictionary attack).

3. Izmiješati mala i velika slova s brojevima

   Na primjer: h0bo3niCa. Na prvi pogled besmislena i teška za pamćenje, ova je zaporka izvedena iz riječi hobotnica. Polazište je pojam koji lako pamtimo, ali onda po nekom algoritmu vršimo zamjenu znakova.

4. Ne koristiti imena bliskih osoba, ljubimaca, datume

   Takve se zaporke lako otkriju socijalnim inženjeringom.

5. Trajanje zaporke

   Promjena zaporke smanjuje vjerojatnost njezina otkrivanja. Preporuka je mijenjati zaporku barem jednom godišnje.

6. Tajnost zaporke

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

Hackeri nastoje izmamiti zaporke lažno se predstavljajući kao administratori. Pravi administratori imaju mogućnost rješavanja probleme i bez poznavanja korisničkih zaporki.

7. Čuvanje zaporke

Zaporke se ne ostavljaju 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 ili više neuspjelih pokušaja prijave.

Prilikom provjere sustava sigurnosni tim može ispitati da li su korisničke zaporke u skladu s navedenim pravilima.

Nepridržavanje

Korisnici koji se ne pridržavaju navedenih pravila ugrožavaju sigurnost informacijskog sustava. KBF je obavezan odgojno djelovati i obrazovati korisnike u kreiranju sigurnih zaporki.

U slučaju ponovljenog ignoriranja ovih pravila, KBF može stegovno djelovati ili postaviti zaposlenika na radno mjesto na kojem je manja mogućnost ugrožavanja integriteta i sigurnosti sustava i podataka.