AMRES

AMRES projekat, 2008

Rezultat:

D12.b. Pravilnik zaštite i korišćenja lozinki

Aktivnost:

A2.5. CSIRT - *Computer Security Incident Response Team*

Autori: Dušan Pajin (RCUB), Ratko Bučić (JUNIS), Vladimir Ilić (ARMUNS)

Apstrakt:

Lozinke predstavljaju važan aspekt zaštite računara i računarskih mreža. One predstavljaju osnovnu zaštitu korisničkih naloga u različitim servisima (e-mail, pristup računaru, mreži, itd). Cilj ovog Pravilnika je da uspostavi preporuke za izbor lozinki, njihovu zaštitu i frekvenciju njihovih promena.

© Copyright AMRES, 2009

Izvršioci AMRES projekta:


Univerzitet u Beogradu

Računarski centar Univerziteta u Beogradu (RCUB)


Univerzitet u Nišu

Jedinstveni univerzitetski nastavno naučni informacioni sistem (JUNIS)

Univerzitet u Novom Sadu

Centar za informacione tehnologije (CIT-UNS)


Univerzitet u Kragujevcu

Univerzitetski računski centar (UNIC)

Sadržaj

Uvod

Lozinke predstavljaju važan aspekt zaštite računara i računarskih mreža. One predstavljaju osnovnu zaštitu korisničkih naloga u različitim servisima (e-mail, pristup računaru, mreži, itd). Loše izabrana lozinka može predstavljati bezbednosnu pretnju celokupnom funkcionisanju Akademske mreže ili mreže korisnika AMRES-a.

Iz navedenog razloga, svi zaposleni na održavanju i upravljanju AMRES mrežom, uključujući AMRES timove i zaposlene u AMRES servisnim centrima, kao i krajnje korisnike AMRES servisa, moraju se pridržavati pravila navedenih u Pravilniku zaštite i korišćenja lozinki kako bi izabrali svoju lozinku koja će ujedno biti dovoljno sigurna.

Takođe, AMRES CSIRT preporučuje da ovaj Pravilnik usvoje i AMRES korisničke organizacije i predstave ga svojim korisnicima, kako bi prema navedenim pravilima podigli nivo bezbednosti u svojima mrežama i računarskim sistemima.

Pravilnik zaštite i korišćenja lozinki

Cilj ovog Pravilnika je da uspostavi preporuke za izbor lozinki, njihovu zaštitu i frekvenciju njihovih promena. Pravilnik se odnosi na sve korisnike koji imaju bilo kakav nalog koji zahteva lozinku na bilo kom uređaju ili sistemu koji se nalazi u okviru AMRES-a, odnosno AMRES servisnih centara.

Ovim Pravilnikom su postavljene i definisane:

- preporuke za konstruisanje lozinki
- pravila korišćenja lozinki za krajnje korisnike AMRES servisa
- pravila korišćenja lozinki ne mrežnim uređajima i serverima od strane AMRES servisnih centara

Preporuke za kreiranje lozinki

Karakteristike nedovoljno sigurnih lozinki koje se ne smeju koristiti su:

- Nedovoljan broj karaktera u sklopu lozinke
- Lozinka koja se može naći u rečniku srpskog ili stranog jezika
- Lozinka koja se sastoji od porodičnih imena, imena kućnih ljubimaca, poznatih ličnosti ili filmskih junaka
- Lozinka koja se sastoji od kompjuterski termina, komandi, imena web sajtova ili proizvođača računarskog hardvera ili softvera
- Lozinka koja se sastoji od datuma, telefonskih brojeva ili adrese
- Lozinka koja se sastoji od sklopova slova ili brojeva kao što su aaabbb, qwerty, abcdefg, 123321 i slično
- Bilo koji slučaj prethodno navedene lozinke napisan unazad ili kombinovan sa jednim brojem

Karakteristike dovoljno sigurnih lozinki koje se mogu koristiti sledeće:

- Sastoji se iz velikih i malih slova, brojeva i drugih alfanumeričkih karaktera
- Ima dužinu od minimalno 8 karaktera

Pravilnik zaštite i korišćenja lozinki

- Nije konkretna reč nijednog jezika ili slenga
- Nije konstruisana na osnovu nekih ličnih informacija

Pravila bezbednosti lozinki krajnjih korisnika AMRES servisa

Navedena pravila u nastavku su obavezna za sve krajnje korisnike AMRES servisa (npr. Email, web, dial-up...)

- Lozinka koju AMRES krajnji korisnik koristi mora biti konstruisana prema preporukama za kreiranje lozinki navedenih u ovom Pravilniku
- Lozinka koju AMRES korisnik koristi na bilo kojem AMRES servisu ne sme biti ista sa lozinkom koju koristi na bilo kom drugom servisu privatne svrhe.
- Zabranjeno je deliti svoj korisnički nalog AMRES servisa i lozinku sa bilo kojom drugom osobom, kolegom ili korisnikom AMRES-a.
- Ne saopštavati nikome svoju lozinku. U slučaju da vam neko od nadređenih, administratora AMRES-a ili zaposlenih traži da mu saopštite vašu lozinku, pozvati se na ovaj dokument i uputiti ga da kontaktira AMRES servisni centar.
- Lozinke se ne smeju slati elektronskom poštom niti bilo kojim drugim vidom elektronske komunikacije.
- Menjati lozinku u vremenskom intervalu od godinu dana.

U nastavku su navedene preporuke bezbednosti lozinki koje nisu obavezne za krajnje korisnike AMRES servisa, ali su navedene kao preporučeno ponašanje, čime će AMRES krajnji korisnik povećati bezbednost svojih lozinki.

- Ne koristiti opciju čuvanja lozinke u bilo kom računarskom programu (na primer, MS Outlook, Eudora, Internet Explorer, Mozilla Firefox i sl.)
- Ne čuvati lozinku na papiru niti na bilo kom elektronskom uređaju (na primer, prenosnom računaru, mobilnom telefonu, računaru unutar nekog fajla i sl.)
- U slučaju sumnje da je lozinka otkrivena, prijaviti slučaj AMRES servisnom centru kroz Helpdesk službu i promeniti sve lozinke.

Pravila zaštite lozinki na mrežnim uređajima i serverima

Pravila koja se navode u nastavku odnose se na lozinke koje se koriste za korisničke ili administratorske naloge na mrežnim uređajima i serverima, kao i za lozinke ili ključeve koji se koriste kao način autentifikacije različitih mrežnih protokola i uređaja.

- Sve sistemske lozinke se moraju menjati u vremenskom intervalu od šest meseci. Sistemske lozinke se odnose na lozinke administratorskog ili *root* naloga na serverima i "*enable*" lozinke na mrežnim uređajima.
- Lozinke svih administratorskih naloga na mrežnim uređajima moraju se menjati u vremenskom intervalu od šest meseci.
- Lozinke svih administratorskih naloga na mrežnim uređajima i serverima moraju biti jedinstvene u odnosu na bilo koje druge korisničke naloge na bilo kojim drugim sistemima.
- Sve lozinke moraju imati minimalnu dužinu od 12 alfanumeričkih karaktera.
- Sve lozinke moraju sadržati mala slova, velika slova, brojeve i alfanumeričke karaktere.

Pravilnik zaštite i korišćenja lozinki

- Sve lozinke koje se čuvaju na mrežnim uređajima ili serverima moraju se čuvati u kriptovanom obliku.
- Sve lozinke ukoliko se prikazuju, moraju biti prikazane u kriptovanom ili zaštićenom obliku.
- Lozinke se ne smeju slati elektronskom poštom niti bilo kojim pisanim oblikom. Lozinke se korisnicima mogu saopštiti lično ili putem telefona uz prethodno utvrđeni identitet korisnika.
- Ne čuvati lozinku na papiru niti na bilo kom elektronskom uređaju (na primer, prenosnom računaru, mobilnom telefonu, računaru unutar nekog fajla i sl.)
- Sve lozinke moraju biti u skladu sa daljim preporukama u ovom pravilniku i pravilima koja se odnose i na AMRES krajnje korisnike.

Završne napomene

Provera lozinki i pokušaj njihovog otkrivanja može biti sproveden od strane CSIRT tima i u slučaju da je lozinka otkrivena, korisnik će morati da je promeni.

U slučaju da lozinka nije konstruisana u skladu sa preporukama koje su navedene u ovom dokumentu, korisnik može snositi određene kaznene mere u vidu privremenog zamrzavanja pristupa AMRES servisima.

Implementacija tehnika za sprečavanje napada i upravljanje lozinkama

U ovom poglavlju biće opisani primeri implementacije zaštite lozinki na mrežnim uređajima u AMRES servisnim centrima. Kako se pravila koja definiše Pravilnik korišćenja lozinki odnose generalno na ponašanje korisnika, ova pravila nije moguće implementirati na mrežnim uređajima. Ipak, na mrežnim uređajima moguće je implementirati određene tehnike kako bi se zaštitio pristup uređajima i same lozinke od napada.

AMRES CSIRT tim poziva administratore AMRES korisničkih organizacija da primene navedena pravila i na svojim uređajima.

Zaštita od napada i neautorizovanog pristupa mrežnim uređajima

Zaštita od napada i neautorizovanog pristupa mrežnim uređajima se osim dobro smišljenog načina autentifikacije i dobro zaštićenih lozinki, zasniva i na pripremljenosti za napade. Većina napada koji imaju za cilj dobijanje pristupa mrežnim uređajima, izvode se pokušajem pogađanja lozinki. Ovi napadi mogu biti takozvani *brute-force* i *dictionary* napadi. *Brute-force* napadi pokušavaju da pogode lozinku, iz velikog broja pokušaja, koristeći sve moguće kombinacije karaktera koji čine lozinku. Uspešnost ovakvog napada zavisi od vremena koje je potrebno za njegovo izvršenje, što zavisi od broja kombinacija i vremena koje je potrebno za isprobavanje jedne od mogućih kombinacija. *Dictionary* napad pokušava da smanji ukupan broj kombinacija korišćenjem skupa "često korišćenih" lozinki i varijacije ovog skupa kako bi se smanjilo ukupno vreme potrebno za uspešno izvršenje napada.

Iz tog razloga, uspešna odbrana od ovih napada jeste korišćenje lozinki sa velikim brojem karaktera i korišćenje što većeg skupa karaktera (mala i velika slova, brojevi i specijalni dozvoljeni znaci) čime se povećava broj različitih kombinacija koje napad mora da isproba. Odbrana od *dictionary* napada jeste lozinka koja ne koristi poznate reči, već nasumičan skup karaktera. Još jedna odbrana od ovih napada jeste usporavanje njihovog izvršavanja, koje se uglavnom zasniva na usporenju procesa unošenja lozinke u slučaju pogrešnog unosa. Na ovaj način se produžava i ukupno vreme koje je potrebno za eventualno uspešno izvršenje napada.

Kombinacija ovih metoda je vrlo uspešna protiv navedenih *brute-force* i *dictionary* napada jer vreme potrebno za njihovo uspešno izvršenje postaje besmisleno veliko.

U nastavku je navedena konfiguracija koja se koristi za sprečavanje navedenih napada na lozinke. Na uređajima se konfiguriše minimalna prihvatljiva dužina lozinki od 12 karaktera što je u skladu sa Pravilnikom zaštite i korišćenja lozinki. Uređaji se konfigurišu tako da nakon svakog pogrešnog unosa lozinke, ponovni unos je moguć tek posle 5 sekundi. U slučaju tri neuspešna unosa lozinke u vremenskom intervalu od jednog minuta, uređaj blokira terminalski i Web pristup na 60 sekundi. Svaki uspešan i neuspešan pokušaj pristupa mrežnom uređaju se loguje.

```
security passwords min-length 12
!
login block-for 60 attempts 3 within 60
login delay 5
login on failure
login on success
```

Konfiguracija lozinki na mrežnim uređajima

Glavna zaštita Cisco uređaja od menjanja njihove konfiguracije je takozvana "*Enable*" lozinka. "*Enable*" lozinka predstavlja zaštitu za pristup u "*enable*" mod iz koga je moguća promena konfiguracije uređaja. Ovu lozinku je moguće konfigurisati kroz dve komande koje se prikazane ispod. Prva komanda će kasnije u prikazu konfiguracije imati zaštićeni oblik prikaza unesene lozinke (neće se prikazati u izvornom obliku) dok će druga imati nezaštićeni prikaz. Za zaštitu *enable* moda obavezno treba koristiti "*enable secret*" lozinku, dok "*enable password*" lozinku ne treba koristiti obzirom da ona postoji samo iz istorijskih razloga podrške starim verzijama rutera.

```
Router(config)#enable secret lozinka1
Router(config)#enable password lozinka2

Router#show running-config
...
enable secret 5 $sf1dFuYi34%oa3Gfu#zdq8&7
enable password 0 lozinka2
```

Sličan princip treba primeniti i pri konfiguraciji korisničkih naloga na ruteru. Lokalne korisničke naloge na ruteru moguće je konfigurisati sa "*secret*" i "*password*" lozinkama.

```
Router(config)#username korisnik1 secret lozinka1
Router(config)#username korisnik2 password lozinka2

Router#show running-config
...
username korisnik1 secret 5 $HJ1dFuYi78%sp5Gkl#zTR/&3
username korisnik2 password 0 lozinka2
```

Dodatni način zaštite lozinki koje se nalaze u konfiguraciji uređaja je preko servisa za enkripciju lozinki. Ovaj servis obavezno uključiti na svim mrežnim uređajima koji ga podržavaju, nakon čega će prikaz lozinki koje inače nisu kriptovane, biti u kriptovanom obliku. Ovaj servis predstavlja zaštitu od čitanja lozinke pri prikazu konfiguracije, ali ne i dovoljnu zaštitu, pošto se ovako prikazane lozinke mogu dekriptovati.

Ispod je prikazan način korišćenja servisa enkripcije lozinki. Lozinka konfigurisana za korisnik2 je prikazana u kriptovanom obliku, međutim ovaj način enkripcije je poznat i prikazana lozinka se može dekriptovati. Iz tog razloga, obavezno je korišćenje "*secret*" varijante komande obzirom da prikaz lozinke u ovoj komadi predstavlja *md5* funkciju koja nije reverzibilna, pa se originalna lozinka ne može rekonstruisati.

```
Router(config)#service password-encryption

Router#show running-config
...
username korisnik1 secret 5 $HJ1dFuYi78%sp5Gkl#zTR/&3
username korisnik2 password 7 81902348091220219
```

Zaštita od napada i neautorizovanog pristupa serverima

Za zaštitu servera od *brute-force* i *dictionary* napada postoje različiti softveri koji nude sličnu vrstu pomoći. Konkretno, za zaštitu pristupa preko SSH, AMRES CSIRT tim predlaže korišćenje besplatnog softvera za Linux operativne sisteme koji se zove *DenyHosts* (http://denyhosts.sourceforge.net/). Ovaj softver omogućava blokiranje IP adresa u slučaju određenog broja neuspešnih pokušaja logovanja preko SSH, na postojeći ili nepostojeći korisnički nalog. Na taj način, moguće je blokirati IP adresu potencijalnog napadača nakon definisanog broja neuspešnih pokušaja logovanja, čime se sprečava uspešno izvođenje *dictionary* ili *brute-force* napada.