AMPEC
Академска мрежа Србије

Препоруке за заштиту и коришћење лозинки

Историја верзија документа

Верзија	Датум	Иницијали аутора	Опис промене
1.0	2009. год	Душан Пајин (РЦУБ), Ратко Бучић (ЈУНИС), Владимир Илић (АРМУНС)	Прва верзија документа у оквиру AMPEC пројекта
2.0	05.08.2015.	Милош Куколеча (AMPEC)	Друга верзија документа

Садржај

1 Увод

Лозинке представљају важан аспект заштите рачунара и рачунарских мрежа. Оне представљају основну заштиту корисничких налога у различитим сервисима (имејл, приступ рачунару, мрежи, итд). Лоше изабрана лозинка може представљати безбедносну претњу целокупном функционисању Академске мреже или мреже AMPEC корисника.

Из наведеног разлога, сви запослени на одржавању и управљању AMPEC мрежом и мрежом AMPEC корисника, као и крајњи корисници треба да се придржавају правила наведених у Препорукама заштите и коришћења лозинки како би креирали довољно сигурну лозинку.

Такође, AMPEC CSIRT препоручује да ове Препоруке усвоје и AMPEC корисници и представе га својим крајњим корисницима, како би према наведеним правилима подигли ниво безбедности у својим мрежама и рачунарским системима.

Препоруке за заштиту и коришћење лозинки

2 Препоруке за заштиту и коришћење лозинки

Циљ ових Препорука је пружање помоћи за избор лозинки, њихову заштиту и фреквенцију њихових промена. Препоруке се односе на све кориснике који имају било какав налог који захтева лозинку на било ком уређају или систему који се налази у оквиру AMPEC-а, односно AMPEC корисника.

Овим Препорукама су постављене и дефинисане:

- препоруке за конструисање лозинки
- препоруке коришћења лозинки за крајње кориснике AMPEC сервиса
- препоруке коришћења лозинки не мрежним уређајима и серверима AMPEC корисника

2.1 Препоруке за креирање лозинки

Карактеристике недовољно сигурних лозинки које се не смеју користити су:

- недовољан број карактера у склопу лозинке
- лозинка која се може наћи у речнику српског или страног језика
- лозинка која се састоји од породичних имена, имена кућних љубимаца, познатих личности или филмских јунака
- лозинка која се састоји од компјутерски термина, команди, имена web сајтова или произвођача рачунарског хардвера или софтвера
- лозинка која се састоји од датума, телефонских бројева или адресе
- лозинка која се састоји од склопова слова или бројева као што су *aaabbb*, *qwerty*, *abcdefg*, *123321* и слично
- било који случај претходно наведене лозинке написан уназад или комбинован са једним бројем

Карактеристике довољно сигурних лозинки које се могу користити следеће:

- састоји се из великих и малих слова, бројева и других алфанумеричких карактера ♦ Има дужину од минимално 8 карактера
- није конкретна реч ниједног језика или сленга
- није конструисана на основу неких личних информација

2.2 Препоруке за безбедност лозинки AMPEC крајњих корисника

Наведене препоруке у наставку се односе на све крајње кориснике AMPEC сервиса (нпр. имејл, VPN, федерација идентитета...):

- Лозинка коју AMPEC крајњи корисник користи треба бити конструисана према препорукама за креирање лозинки наведених у овом документу
- Лозинка коју AMPEC корисник користи на било којем AMPEC сервису не сме бити иста са лозинком коју користи на било ком другом сервису приватне сврхе.
- Забрањено је делити свој кориснички налог и лозинку који се користе у AMPEC сервисима са било којом другом особом, колегом или крајњим корисником AMPEC-а.
- Не саопштавати никоме своју лозинку. У случају да вам неко од надређених, администратора у локалним мрежама или запослених тражи да му саопштите вашу лозинку, позвати се на овај документ и упутити га да контактира AMPEC CSIRT службу.

Препоруке за заштиту и коришћење лозинки

- Лозинке се не смеју слати електронском поштом нити било којим другим видом електронске комуникације.
- Мењати лозинку у временском интервалу од годину дана.

У наставку су наведене препоруке безбедности лозинки које нису обавезне за крајње кориснике AMPEC сервиса, али су наведене као препоручено понашање, чиме ће AMPEC крајњи корисник повећати безбедност својих лозинки.

- Не користити опцију чувања лозинке у било ком рачунарском програму (на пример, MS Outlook, Eudora, Internet Explorer, Mozilla Firefox и сл.)
- Не чувати лозинку на папиру нити на било ком електронском уређају (на пример, преносном рачунару, мобилном телефону, рачунару унутар неког фајла и сл.)
- У случају сумње да је лозинка откривена, пријавити случај AMPEC CSIRT служби користећи AMPEC хелпдеск (mailto:helpdesk@amres.ac.rs) и променити све лозинке.

2.3 Препоруке заштите лозинки на мрежним уређајима и серверима

Правила која се наводе у наставку односе се на лозинке које се користе за корисничке или администраторске налоге на мрежним уређајима и серверима, као и за лозинке или кључеве који се користе као начин аутентификације различитих мрежних протокола и уређаја.

- Све системске лозинке се морају мењати у временском интервалу од шест месеци. Системске лозинке се односе на лозинке администраторског или *root* налога на серверима и "*enable*" лозинке на мрежним уређајима.
- Лозинке свих администраторских налога на мрежним уређајима морају се мењати у временском интервалу од шест месеци.
- Лозинке свих администраторских налога на мрежним уређајима и серверима морају бити јединствене у односу на било које друге корисничке налоге на било којим другим системима.
- Све лозинке морају имати минималну дужину од 12 алфанумеричких карактера.
- Све лозинке морају садржати мала слова, велика слова, бројеве и алфанумеричке карактере.
- Све лозинке које се чувају на мрежним уређајима или серверима морају се чувати у криптованом облику.
- Све лозинке уколико се приказују, морају бити приказане у криптованом или заштићеном облику.
- Лозинке се не смеју слати електронском поштом нити било којим писаним обликом. Лозинке се корисницима могу саопштити лично или путем телефона уз претходно утврђени идентитет корисника.
- Не чувати лозинку на папиру нити на било ком електронском уређају (на пример, преносном рачунару, мобилном телефону, рачунару унутар неког фајла и сл.)
- Све лозинке морају бити у складу са осталим препорукама у овом документу.

2.4 Завршне напомене

Провера лозинки и покушај њиховог откривања може бити спроведен од стране CSIRT тима и у случају да је лозинка откривена, корисник ће морати да је промени.

У случају да лозинка није конструисана у складу са препорукама које су наведене у овом документу, корисник може сносити одређене казнене мере у виду привременог замрзавања приступа AMPEC сервисима.

3 Технике за спречавање напада и управљање лозинкама

У овом поглављу биће описани примери имплементације заштите лозинки на мрежним уређајима AMPEC корисника. Како се препоруке коришћења лозинке односе генерално на понашање корисника, ове препоруке није могуће имплементирати на мрежним уређајима. Ипак, на мрежним уређајима могуће је имплементирати одређене технике како би се заштитио приступ уређајима и саме лозинке од напада.

AMPEC CSIRT тим позива администраторе AMPEC корисника да примене наведена правила и на својим уређајима.

3.1 Заштита од напада и неауторизованог приступа мрежним уређајима

Заштита од напада и неауторизованог приступа мрежним уређајима се осим добро смишљеног начина аутентификације и добро заштићених лозинки, заснива и на припремљености за нападе. Већина напада који имају за циљ добијање приступа мрежним уређајима, изводе се покушајем погађања лозинки. Ови напади могу бити такозвани *brute-force* и *dictionary* напади. *Brute-force* напади покушавају да погоде лозинку, из великог броја покушаја, користећи све могуће комбинације карактера који чине лозинку. Успешност оваквог напада зависи од времена које је потребно за његово извршење, што зависи од броја комбинација и времена које је потребно за испробавање једне од могућих комбинација. *Dictionary* напад покушава да смањи укупан број комбинација коришћењем скупа "често коришћених" лозинки и варијације овог скупа како би се смањило укупно време потребно за успешно извршење напада.

Из тог разлога, успешна одбрана од ових напада јесте коришћење лозинки са великим бројем карактера и коришћење што већег скупа карактера (мала и велика слова, бројеви и специјални дозвољени знаци) чиме се повећава број различитих комбинација које напад мора да испроба. Одбрана од *dictionary* напада јесте лозинка која не користи познате речи, већ насумичан скуп карактера. Још једна одбрана од ових напада јесте успоравање њиховог извршавања, које се углавном заснива на успорењу процеса уношења лозинке у случају погрешног уноса. На овај начин се продужава и укупно време које је потребно за евентуално успешно извршење напада.

Комбинација ових метода је врло успешна против наведених *brute-force* и *dictionary* напада јер време потребно за њихово успешно извршење постаје бесмислено велико.

У наставку је наведена конфигурација која се користи за спречавање наведених напада на лозинке. На уређајима се конфигурише минимална прихватљива дужина лозинки од 12 карактера што је у складу са Препорукама заштите и коришћења лозинки. Уређаји се конфигуришу тако да након сваког погрешног уноса лозинке, поновни унос је могућ тек после 5 секунди. У случају три неуспешна уноса лозинке у временском интервалу од једног минута, уређај блокира терминалски и веб-приступ на 60 секунди. Сваки успешан и неуспешан покушај приступа мрежном уређају се логује.

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

3.2 Конфигурација лозинки на мрежним уређајима

Главна заштита *Cisco* уређаја од мењања њихове конфигурације је такозвана "*Enable*" лозинка. "*Enable*" лозинка представља заштиту за приступ у "*enable*" мод из кога је могућа промена конфигурације уређаја. Ову лозинку је могуће конфигурисати кроз две команде које се приказане испод. Прва команда ће касније у приказу конфигурације имати заштићени облик приказа унесене лозинке (неће се приказати у изворном облику) док ће друга имати незаштићени приказ. За заштиту *enable* мода обавезно треба користити "*enable secret*" лозинку, док "*enable password*" лозинку не треба користити с обзиром да она постоји само из историјских разлога подршке старим верзијама рутера.

```
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
```

Сличан принцип треба применити и при конфигурацији корисничких налога на рутеру. Локалне корисничке налоге на рутеру могуће је конфигурисати са "*secret*" и "*password*" лозинкама.

```
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
```

Додатни начин заштите лозинки које се налазе у конфигурацији уређаја је преко сервиса за енкрипцију лозинки. Овај сервис обавезно укључити на свим мрежним уређајима који га подржавају, након чега ће приказ лозинки, које иначе нису криптоване, бити у криптованом облику. Овај сервис представља заштиту од читања лозинке при приказу конфигурације, али не и довољну заштиту, пошто се овако приказане лозинке могу декриптовати.

Испод је приказан начин коришћења сервиса енкрипције лозинки. Лозинка конфигурисана за "корисник2" је приказана у криптованом облику, међутим овај начин енкрипције је познат и приказана лозинка се може декриптовати. Из тог разлога, обавезно је коришћење "*secret*" варијанте команде обзиром да приказ лозинке у овој комади представља *md5* функцију која није реверзибилна, па се оригинална лозинка не може реконструисати.

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

...

username korisnik1 secret 5 $HJ1dFuYi78%sp5Gkl#zTR/&3
username korisnik2 password 7 81902348091220219
```

3.3 Заштита од напада и неауторизованог приступа серверима

За заштиту сервера од *brute-force* и *dictionary* напада постоје различити софтвери који нуде сличну врсту помоћи. Конкретно, за заштиту приступа преко *SSH*, AMPEC CSIRT тим предлаже коришћење бесплатног софтвера за *Linux* оперативне системе који се зове *DenyHosts* (*http://denyhosts.sourceforge.net/*). Овај софтвер омогућава блокирање *IP* адреса у случају одређеног броја неуспешних покушаја логовања преко *SSH*, на постојећи или непостојећи кориснички налог. На тај начин, могуће је блокирати *IP* адресу потенцијалног нападача након дефинисаног броја

неуспешних покушаја логовања, чиме се спречава успешно извођење *dictionary* или *brute-force* напада.