AMPEC
Академска мрежа Србије

Препоруке безбедности мрежних уређаја

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	06.08.2015.	Милош Куколеча	Друга верзија документа

Садржај

1 Препоруке за безбедност мрежних уређаја

Овај документ дефинише минималне безбедносне захтеве за све мрежне уређаје (рутере и свичеве) који су повезани на AMPEC. Препоруке се односе на све мрежне уређаје који се користе у продукционој мрежи AMPEC корисника.

Препоручује се да сви мрежни уређаји буду конфигурисани према следећим препорукама:

- За аутентификацију корисника користи се специјализовани сервер за аутентификацију корисника преко протокола *TACACS+* или *RADIUS*.
- Постојање једног локалног корисничког налога на уређају који се користи само у случају да не постоји веза ка серверу за аутентификацију.
- Корисничке лозинке дефинисане на уређају чувају се у криптованом облику.
- Аутентификација корисника врши се на свим линијама за приступ уређајима (терминалске линије, веб-приступ, конзолни или *aux* порт)
- На уређајима би требало бити конфигурисана лозинка за улазак у "*enable*" мод и требало би бити снимљена у енкриптованом облику.
- Уређај треба бити евидентиран у корпорацијском систему за надгледање и управљање рачунарском мрежом одмах након инсталације.
- Искључити *HTTP* (веб) приступ уређајима, осим у случају када је експлицитно потребан за конфигурацију уређаја. У случају коришћења, користити заштићени веб-приступ преко *HTTPS* протокола. Ограничити *HTTP* приступ само са одређених *IP* адреса.
- За терминалски приступ мрежним уређајима и коришћење командног мода преферирати приступ преко *SSH* протокола. Само у случају да уређај не подржава *SSH* користити *Telnet* приступ и само у случају да се уређајима приступа у оквиру мреже AMPEC корисника. Ограничити приступ терминалским линијама само са одређених *IP* адреса.
- На уређајима искључити одређене сервисе уколико их уређај подржава:
  - Сервис "*TCP small services*"
  - Сервис "*UDP small services*"
  - Сервис "*IP Source routing*"
  - Сервис "*IP identification*"
  - Сервис "*IP directed broadcast*"
  - Сервис "*BOOTP server*"
  - Сервис "*DHCP server*"
  - Сервис "*Finger*"
  - Сервисе "*ICMP redirect*", "*ICMP unreachable*" и "*ICMP mask reply*"
  - Сервисе "*Gratuitous ARP*" и "*Proxy ARP*"
  - Сервис "*PAD (Packet assembler and disassembler)*"
  - Сервис "*MOP (Maintenance Operation Protocol)*"
- Приступ преко терминалских линија мора имати банер са следећим садржајем:

```
<Naziv AMRES korisnika> <Ime uređaja>
```

```
NEAUTORIZOVANI PRISTUP MREŽNOM UREĐAJU JE ZABRANJEN!


Morate imati eksplicitnu dozvolu za pristup ili konfigurisanje ovog uređaja.
Sve aktivnosti na uređaju se prate i loguju. Kršenje ovih pravila može
dovesti do disciplinskih mera ili sudske tužbe.


--------------------------------------------------------------------------


<Naziv AMRES korisnika> <Ime uređaja>


UNAUTHORISED ACCESS TO THIS DEVICE IS PROHIBITED!


You must have explicit permission to access or configure this device. All
activities on this device are logged. Violations of this policy may result in
disciplinary action, and may be reported to law enforcement. "
```

2 Примери за имплементацију препорука

Имплементација наведених Препорука безбедности мрежних уређаја, се спроводи конфигурацијом конкретних захтева на уређајима AMPEC корисника, првенствено рутерима и свичевима.

У примеру имплементације правилника користиће се синтакса конфигурационих команди за мрежне уређаје компаније *Cisco Systems*.

У наставку би ће наведене конкретне команде за конфигурацију рутера како би се применила све препоруке из овог документа.

2.1 Заштита приступа уређајима

Заштита приступа мрежним уређајима се односи на приступ ради читања података са уређаја и измену конфигурација уређаја.

У Препорукама безбедности мрежних уређаја наведени су одређени начини заштите сваког начина приступа *Cisco* рутерима:

- терминалске линије
- веб-интерфејса
- конзолни порт
- *aux* порт

Приступ преко терминалских линија односи се на приступ преко протокола за емулацију терминала, од којих се најчешће користе *Telnet* и *SSH*. *Telnet* је стандардни протокол за терминалски приступ, који преноси податке у текстуалном облику што значи да се сви подаци у терминалу, па чак и корисничко име и лозинка, преносе без заштите. Из овог разлога, *Telnet* представља несигуран протокол и прислушкивањем пакета на мрежи се лако могу прикупити информације које се преносе овим протоколом. Са друге стране, *SSH* протокол врши енкрипцију података тако да се подаци не могу прислушкивати. Из тог разлога се увек и препоручује коришћење *SSH* уместо *Telnet* протокола.

У наставку је наведен пример конфигурације терминалских (*vty*) линија коју треба применити на мрежним уређајима. На линији терминала прихвата се приступ преко *Telnet* протокола у случају да *SSH* протокол није подржан. Приступ је ограничен и дозвољен само са *IP* адреса које се налазе у листи приступа (*access-list*) под именом "*vty-in*". У овој листи приступа наведен је скуп адреса који се узима као пример скупа адреса администратора мрежних уређаја (на пример, 10.0.1.0/24).

Према наведеној конфигурацији аутентификација корисника на терминалском приступу се врши преко листе "*auth-lista*" која је дефинисана под "*AAA*" секцијом. Детаљи у аутентификацији корисника наведени су у поглављу "Контрола приступа коришћењем *AAA* сервиса".

```
line vty 0 4 access-class vty-in in
transport input ssh telnet
login authentication auth-lista exec-timeout 3
ip access-list standard vty-in permit 10.0.1.0 0.0.0.255
deny any log
!
aaa new-model
aaa authentication list auth-lista group tacacs+ local
```

У наставку је наведена конфигурација *SSH* приступа мрежним уређајима. За конфигурацију *SSH* потребно је претходно конфигурисати име уређаја (*hostname*) и име *DNS* домена. Ови параметри се

користе за генерисање кључева који ће се користити за *SSH* приступ. Пошто је *SSH* приступ подржан на уређају, додатно је на терминалским линијама *Telnet* приступ искључен, док је *SSH* укључен.

```
ip domain-name <domen institucije, npr amres.ac.rs>
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 120
ip ssh authentication-retries 3
line vty 0 4
no transport input telnet transport input ssh
```

Према Препорукама о безбедности мрежних уређаја, веб-приступ мрежним уређајима треба искључити осим уколико је експлицитно потребан за конфигурацију мрежног уређаја. Конкретно веб-приступ је потребан у случају конфигурације рутера преко Cisco *SDM* апликације. У случају да конфигурација уређаја захтева коришћење *Cisco SDM* апликације треба укључити коришћење веб-приступа. Користити *HTTPS* приступ који обезбеђује криптовану везу између Интернет прегледача и уређаја како би подаци били заштићени при преносу. Веб-приступ је ограничен на *IP* адресе администратора. У наставку је наведена конфигурација веб-приступа уређајима.

```
!   Iskljucivanje Web pristupa
no ip http server
!   Ukljucivanje http pristupa ip http server
ip http secure server
ip http access-class http-in in
!
ip access-list standard http-in permit 10.0.1.0 0.0.0.255
deny any log
```

У наставку је наведен пример конфигурације конзолне и *aux* линије. На приступу конзолном порту потребна је аутентификација корисника, док линија мора бити ресетована у случају некоришћења у временском интервалу од 3 минута. Приступ преко *aux* линије је искључен јер се не користи.

```
line con 0
login authentication auth-lista exec-timeout 3 0
!
aaa new-model
aaa authentication list auth-lista group tacacs+ local
line aux 0 no exec
```

2.2 Искључивање непотребних сервиса на мрежним уређајима

Сваки сервис или апликација рачунарског система може представљати безбедносни ризик. У случају када сервис и апликација немају никакав познати ризик, чињеница је да могу постојати и одређени пропусти у самој апликацији и сервису кога ни њихов произвођач није свестан. Из тог разлога, искључивање непотребних и некоришћених сервиса у рачунарским системима представља један од основних начина повећања сигурности. Исти случај је и са мрежним уређајима.

Наведени сервиси у Препорукама безбедности мрежних уређаја за које се препоручује њихово искључивање представљају сервисе који се већином не користе. Одређени сервиси су се некада користили, неки су прављени по угледу на неке сервисе *Unix* система и углавном постоје из

историјских разлога компатибилности са неким старијим уређајима. Већина ових сервиса су на уређајима укључени у основној конфигурацији и из тог разлога је потребна додатна конфигурација за њихово искључивање. У наставку је наведен пример конфигурације *Cisco* рутера, којом се имплементира искључивање сервиса наведених у правилнику. Одређени сервиси се искључују из глобалног конфигурационог мода, док се неки искључују на нивоу интерфејса.

```
!   Svaka linija konfiguracije koja pocinje sa znakom '!'
!   predstavlja komentar i ignorise se od strane uredjaja
!
!   Iskljucivanje nepotrebnih servisa
!
no service tcp-small-servers no service udp-small-servers no service finger
no service pad
!
!   Iskljucivanje odredjenih IP servisa
!
no ip bootp server no ip dhcp server no ip finger
no ip source-route no ip gratuitous-arp no ip identd
no ip domain-lookup
!
!   Iskljucivanje odredjenih servisa na nivou interfejsa
!
interface FastEthernet0/0 no ip redirects
no ip proxy-arp
no ip unreachables
no ip directed-broadcast no ip mask-reply
no mop enabled interface Serial0/0 no ip redirects
no ip proxy-arp
no ip unreachables
no ip directed-broadcast no ip mask-reply
no mop enabled
```

2.3 Конфигурисање банера за приступ мрежним уређајима

Банер или поздравна порука представљају произвољан текст који ће се приказати при терминалском приступу мрежном уређају. Изузетно је важно конфигурисати банер поруку којом ће се особа која приступа мрежном уређају обавестити о правима и последицама њеног приступа. Никада не користити поруке са речима које одобравају приступ, као што је нпр. "Добродошли".

У наставку је наведен пример конфигурације банера који ће се може користити на мрежним уређајима AMPEC корисника.

```
banner motd %
<Ime institucije> $(hostname)
```

```
NEAUTORIZOVANI PRISTUP MREZNOM UREDJAJU JE ZABRANJEN!

Morate imati eksplicitnu dozvolu za pristup i konfigurisanje ovog uredjaja.
Sve aktivnosti na ovom uredjaju se prate i loguju. Krsenje ovih pravila moze
dovesti do disciplinskih mera ili sudske tuzbe.

------------------------------------------------------------------


<Ime institucije> $(hostname)


UNAUTHORISED ACCESS TO THIS DEVICE IS PROHIBITED!

You must have explicit permission to access or configure this device. All
activities on this device are logged. Violations of this policy may result in
disciplinary action, and may be reported to law enforcement.

%
```