MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CSIRT.SK

Odporúčané nasadenie overovacích a autorizačných systémov pre e-mailové servery

SPF, DKIM, DMARC

21.05.2021

Technológia elektronickej pošty, ako ju poznáme dnes - E-mail - nás sprevádza už vyše dve desaťročia. Slúži primárne na výmenu informácii, ale s rozvojom Internetu a Webu ju čoraz častejšie používame aj ako súčasť digitálnej identity napríklad pri zakladaní online účtov. V roku 2019 existovalo na svete 3,9 miliardy aktívnych používateľov tejto technológie a toto číslo stále rastie. S nárastom využívania E-mailovej komunikácie sa však čoraz častejšie objavujú aj rôzne formy útokov , ako sú phishing, pharming, spoofing, spam a iné.

Phishing je forma kybernetického útoku, pri ktorom útočník používa falošný E-mail ako útočný vektor. Zámerom je docieliť, aby príjemca E-mailu uveril, že sa jedná o legitímnu správu a vykonal požadovaný úkon napr. v podobe spustenia škodlivej prílohy alebo návštevy webového sídla obsahujúceho škodlivý kód.

Pharming je forma kybernetického útoku, pri ktorom napríklad škodlivý kód prijatý E-mailom a spustený na zariadení obete zabezpečí v operačnom systéme úpravu subsystému pre preklad doménových mien na IP adresy - čo v konečnom dôsledku spôsobí, že obeť je odklonená na falošnú webovú stránku, potom čo zadala správnu URL vo svojom internetovom prehliadači. Pri tomto type útoku nie je potrebné zameriavať sa na jednotlivca a nie sú potrebné vedomé kroky obete, preto môže byť obeťou útoku aj väčší počet používateľov.

Spoofing znamená podvrhnutie, resp. sfalšovanie E-mailových hlavičiek, napr. adresu odosielateľa, čím sa útočník snaží získať kredibilitu u príjemcu.

Spam je nevyžiadaná pošta, ktorá môže, ale aj nemusí byť nebezpečná, je však obťažujúca.

Trojica nástrojov **SPF, DKIM, DMARC** nám pomáha chrániť sa pred podvrhnutými E-mailami, ale aj zaručuje, aby nami odoslané E-maily nekončili u príjemcu ako nevyžiadaná pošta. Taktiež tieto nástroje dokážu zabrániť útočníkovi, aby nám prostredníctvom E-mailovej komunikácii ukradol identitu, resp. sa za nás vydával.

SPF (Sender Policy Framework)

SPF je TXT DNS záznam, v ktorom je uvedené, ktorý poštový server je oprávnený odosielať E-mailové správy pre určitú doménu. Poštový server príjemcu si tak môže overiť či sa v SPF zázname domény odosielateľa nachádza poštový server, z ktorého bol E-mail odoslaný. V prípade, že sa v ňom nenachádza, E-mail môže byť serverom príjemcu odmietnutý, eventuálne vyhodnotený ako SPAM (záleží to od nastavenia politiky v SPF zázname a od konfigurácie poštového servera). Napríklad oznámenie „**Message rejected because SPF check failed**“ znamená, že poštový server odosielateľa

TLP: White

správy nie je oprávnený odosielať za danú doménu, a preto nebol E-mail prijatý. Ak sa odosielateľovi po odoslaní správy vracia späť takéto oznámenie, poštový server príjemcu odmietol prijať takýto E-mail z dôvodu nevyhovujúceho SPF záznamu – tento scenár platí iba pre legitímne poštové servery.

Nastavenie SPF záznamu pre Postfix na systéme Ubuntu Server:

1. Vytvorte záznam SPF v DNS svojej domény pre odosielateľa

   V prípade, že používate poštový server s doménou "example.com" pre odosielateľa všetkých svojich E-mailov odosielaných prostredníctvom sieťovej služby Postfix, jedná sa o doménu, pre ktorú musíte nastaviť záznam SPF. Záznam SPF je možné nastaviť na Vašom autoritatívnom DNS servery.
   Po prihlásení stačí vytvoriť nový záznam TXT, napr.:

   ```
   TXT @ v=spf1 mx ~all
   ```

   Existuje niekoľko poskytovateľov DNS, ktorí vyžadujú aby ste záznam SPF vložili s úvodzovkami, napr.:

   ```
   TXT @ "v=spf1 mx ~all"
   ```

   Po pridaní SPF záznamu môže trvať jeho celosvetová propagácia v sieti Internet 24 až 48 hodín. Pomocou príkazu "dig" môžete zobraziť aktuálny stav SPF záznamu a overiť, či bol aktualizovaný (príkaz pre získanie odpovede využíva DNS server, ktorý je predvolený v operačnom systéme).

   ```
   dig example.com TXT
   ```

   Môžete tiež použiť online SPF „validátory", ako mxtoolbox.com, https://dmarcian.com/domain-checker/ alebo SPF Query Tool (kitterman.com)

2. Konfigurácia agenta politiky SPF na serveri

   Rovnako, ako v prípade konfigurácie SPF záznamu pre odchádzajúce E-maily, by ste mali urobiť overenie pre prichádzajúce e-maily.

   Najprv nainštalujte požadovaný balík pre agenta politiky SPF

   ```
   # apt install postfix-policyd-spf-python
   ```

   Ďalším krokom je úprava konfiguračného súboru sieťovej služby Postfix, konkrétne súboru "master.cf". Na úpravu môžete použiť ľubovoľný editor „Vim", alebo „Nano".

```
# nano /etc/postfix/master.cf
```

Na konci súboru pridajte nasledujúce riadky, ktoré inštruujú sieťovú službu Postfix, aby spustila "SPF policy daemon" vždy, keď sa služba Postfix spustí.

```
policyd-spf  unix  -       n       n       -       0       spawn
   user=policyd-spf argv=/usr/bin/policyd-spf
```

Nastavenia uložte a zatvorte súbor. Ďalším krokom je úprava hlavného konfiguračného súboru "main.cf" služby Postfix.

```
# nano /etc/postfix/main.cf
```

Na konci súboru "main.cf" pridajte nasledujúce riadky, ktoré hovoria o tom, že službe Postfix dávate inštrukcie kontrolovať SPF záznam prichádzajúcich E-mailov a odmietnuť neoprávnené E-maily.

```
policyd-spf_time_limit = 3600
smtpd_recipient_restrictions =
   permit_mynetworks,
   permit_sasl_authenticated,
   soft_bounce = yes,
   reject_unauth_destination,
   check_policy_service unix:private/policyd-spf
```

Pravidlo **"soft_bounce = yes"** mení akcie odmietnutia SMTP serverom na odložené (skúste to znova neskôr). Pošta, ktorá by sa po odmietnuti vrátila odosielateľovi ostane vo fronte, kým sa server *odosielatela nepokúsi* správu opätovne doručit neskôr.

Pravidlo "**smtpd_delay_reject = yes"** umožňuje Postfix-u, v prípade odmietnutia správy, zaznamenať informácie o adrese príjemcu aj odosielateľa, aby bolo možné následne zistiť, koho pošta bola odmietnutá.

Všetky parametre pre konfiguráciu Postfixu nájdete napríklad tu:
Postfix Configuration Parameters (uma.es)

Nastavenia uložte a zatvorte súbor. SPF politika je nakonfigurovaná. Pre aktivovanie nakonfigurovaných zmien, reštartujte sieťovú službu Postfix.

```
# service postfix restart
```

alebo

```
# systemctl restart postfix
```

Mechanizmy a ich vysvetlenie:

Používajú sa pre stanovenie množiny hostiteľov, ktorí sú oprávnení odosielať elektronické správy pre danú doménu.

“v=spf1**”**	Definuje použitú verziu SPF (aktuálne existuje len spf1)
“a”	Definuje záznam doménového mena nachádzajúceho sa v DNS (A, alebo AAAA záznam), ktorý korešponduje s IP adresou servera odosielajúceho správu.
“ip4”	Definuje rozsah siete IPv4. Je potrebné určit aj masku siete, inak je sa predpokladá 32-bitová .
„ip6“	Definuje rozsah siete IPv6. V prípade, že nie je určená maska siste, predpokladá sa 128-bitová.
“mx ”	slúži na určenie serverov, ktoré môžu spracovávať e-maily pre doménu. MX záznamov pre jednu doménu môžete zadať hneď niekoľko a e-maily budú smerované podľa priority týchto záznamov. Hodnota MX záznamu sa zadáva v textovej podobe („test.example.com.“), nie ako IP adresa. IP adresy uvedené v MX záznamoch pre doménu, ku ktorým pripájame SPF záznam sú akceptované ako validné.
„–all“	znamená, že správy od odosielateľov, ktorí nie sú uvedení v zázname SPF, budú odmietnuté poštovým serverom adresáta. (**„fail“). Primárne odporúčané nastavenie.**
„~all“	znamená, že správy od odosielateľov, ktorí nie sú uvedení v zázname SPF, môžu byť prijaté s informáciou, že neprešli kontrolou SPF. („**softfail”)**
„+all“	toto nastavenie sa neodporúča. Znamená, že správa od akéhokoľvek odosielateľa (IP adresy), ktorý nemusí byť uvedený v SPF zázname, bude prijatá. **(„pass”)**
„?all“	Záznam SPF vyslovene špecifikuje, že o hodnote nie je možné povedať nič. Správa bude v tomto prípade akceptovaná. (**„neutral“**). Toto nastavenie sa rovnako neodporúča.

Rozšírenú syntax pre konfigurovanie SPF záznamu môžete nájsť napríklad tu: https://dmarcian.com/spf-syntax-table/

DKIM (DomainKeys Identified Mail)

DKIM - v preklade „E-mail identifikovaný doménovým kľúčom“ je nástroj, ktorý umožňuje elektronicky podpísať hlavičky odchádzajúcich E-mailov privátnym kľúčom. DKIM umožňuje príjemcovi overiť, či E-mail skutočne pochádza z oprávneného zdroja - domény odosielateľa. Overiť podpis DKIM v prijatej správe je možné pomocou verejného kľúča uvedeného v DNS zázname pre danú doménu. Platný podpis, ktorý zodpovedá verejnému kľúču uloženému v DNS záznamoch domény tak isto garantuje, že niektoré časti E-mailu (vrátane prílohy) neboli upravované. DKIM spolupracuje s nástrojom DMARC. DKIM na rozdiel od Sender ID využíva na potvrdenie odosielateľa E-mailu a celého jeho obsahu kryptografiu v podobe asymetrického elektronického podpisu, zvyčajne pomocou algoritmu RSA a kryptografickej hashovacej funkcie SHA256. Veľkosť kľúča pri RSA algoritme by mala byť aspoň 2048 bitov.

DKIM, ako bolo uvedené vyššie, využíva DNS záznam pre uloženie verejného kľúča, ktorý cieľový poštový server využíva na kontrolu správnosti elektronického podpisu správy, ktorú odosielací poštový server podpísal prostredníctvom spárovaného súkromného kľúča. V prípade jednoduchej implementácie poštového servera zväčša postačuje zverejnenie jedného verejného kľúča, avšak zvlášť v prípade implementácií SMTP serverov, ktoré poskytujú odosielanie správ pre viaceré domény, vstupuje do hry rozšírenie DKIM, ktoré sa nazýva **selektor**. Selektor je špeciálny prefixový reťazec rôznej dĺžky s voliteľným obsahom v názvovej časti DNS záznamu v nasledovnom tvare:

selektor._domainkey.<názov domény>

Primárny význam selektora je umožnenie využitia viacerých verejných (a k nim zodpovedajúcich súkromných) kľúčov, pričom pre každý takýto pár kľúčov je špecifikovaný selektor. Ak teda odosielací poštový server podpisuje správu určitým súkromným kľúčom, „pribalí“ automaticky do správy aj informáciu o selektore, t.j. o verejnom kľúči, ktorý je následne použitý zo strany prijímajúceho poštového servera na overenie správnosti digitálneho podpisu správy. Súčasne platí, že jedna doména môže mať práve jeden selektor, prípadne ich môže mať viacero, eventuálne môže byť ten istý selektor použitý pre validáciu viacerých domén (zväčša prostredníctvom CNAME DNS záznamov).

Sekundárny význam selektora je poskytnutie tzv. rotácie kľúčov, čo je bezpečnostná technika, ktorá umožňuje v pravidelnom časovom intervale obnovu súkromného a verejného kľúča za účelom zvýšenia dôveryhodnosti odosielacieho poštového servera a minimalizácie neoprávneného použitia súkromného kľúča napríklad z dôvodu jeho odcudzenia, resp. kompromitácie. Rotácia sa zabezpečuje publikáciou nového verejného kľúča, kým sa necháva v platnosti aj pôvodný verejný kľúč na určité časové obdobie z hľadiska kompatibility. Následne sa sa pôvodný kľúč odstráni a ponecháva sa len novopublikovaný. Táto procedúra sa pravidelne opakuje.

Nakoľko tento dokument sa zameriava na bezpečnostné aspekty pri nasadzovaní vlastných poštových serverov, je potrebné uviesť, že pravidelná rotácia kľúčov je ním výrazne odporúčaná.

Nastavenie DKIM pre Postfix na systéme Ubuntu Server:

DKIM je možné nastaviť inštaláciou balíčka s otvoreným zdrojovým kódom (OpenDKIM).

```
# apt install opendkim opendkim-tools
```

Po inštalácii je potrebné pridať „postfix“ systémového používateľa do openDKIM skupiny.

```
# gpasswd -a postfix opendkim
```

Ďalším krokom je úprava hlavného konfiguračného súboru OpenDKIM.

```
# nano /etc/opendkim.conf
```

Obsah súboru upravte na ďalej uvedený obsah.

```
# This is a basic configuration that can easily be adapted to suit a standard
# installation. For more advanced options, see opendkim.conf(5) and/or
# /usr/share/doc/opendkim/examples/opendkim.conf.sample.

# Log to syslog
Syslog          yes
# Required to use local socket with MTAs that access the socket as a non-
# privileged user (e.g. Postfix)
UMask           002

# Sign for example.com with key in /etc/mail/dkim.key using
# selector '2007' (e.g. 2007._domainkey.example.com)
#Domain         example.com
#KeyFile        /etc/mail/dkim.key
#Selector       2007

# Commonly-used options; the commented-out versions show the defaults.
Canonicalization  relaxed/simple
Mode            sv
SubDomains      no
#ADSPAction           continue
AutoRestart     yes
AutoRestartRate       10/1M
Background      yes
DNSTimeout      5
SignatureAlgorithm      rsa-sha256

# Always oversign From (sign using actual From and a null From to prevent
# malicious signatures header fields (From and/or others) between the signer
# and the verifier.  From is oversigned by default in the Debian pacakge
# because it is often the identity key used by reputation systems and thus
# somewhat security sensitive.
OversignHeaders     From

# List domains to use for RFC 6541 DKIM Authorized Third-Party Signatures
# (ATPS) (experimental)
```

```
#ATPSDomains       example.com

#OpenDKIM user
# Remember to add user postfix to group opendkim
UserID             opendkim

# Map domains in From addresses to keys used to sign messages
KeyTable           refile:/etc/opendkim/key.table
SigningTable       refile:/etc/opendkim/signing.table

# Hosts to ignore when verifying signatures
ExternalIgnoreList  /etc/opendkim/trusted.hosts

# A set of internal hosts whose mail should be signed
InternalHosts /etc/opendkim/trusted.hosts
```

Súbor uložte a nádledne zatvorte.

Kompletnú konfiguráciu mechanizmu DKIM pre sieťovú službu Postfix na operačnom systéme UBUNTU môžete nájsť napríklad tu.:
How to Set up SPF and DKIM with Postfix on Ubuntu Server? | Pepipost (netcorecloud.com)

DMARC (Domain-based Message Authentication, Reporting and Conformance)

DMARC je vybudovaný na mechanizmoch DKIM a SPF. Umožňuje správcovi DNS definovať podmienky, ako overiť odosielateľa správy za pomoci DKIM a SPF a taktiež ako sa má príjemca vysporiadať s neúspešným overením. DMARC poskytuje možnosť odosielať správu o stave výsledku vyhodnotenia relevancie prijatých správ.

Kroky pre nasadenie DMARC

Aktiváciu DMARC vykonáte pridaním DNS záznamu ku doméne u registrátora.
DNS záznam (typ TXT) pre DMARC vyzerá nasledovne:

Doména	**Typ**	**TTL**	**Data**
_dmarc	TXT	1800	**v=DMARC1; p=quarantine; sp=none; adkim=r; aspf=r; fo=1;…**

Tu je ukážka záznamu DMARC pre web DMARC testovacej domény:
v=DMARC1; p=quarantine; rua=mailto:reports@dmarc.site; ruf=mailto:reports@dmarc.site; adkim=r; aspf=r; rf=afrf

„v“ verzia protokolu

„p“	Definuje požadovanú akciu príjemcu. Má tri možnosti: žiadna akcia, karanténa, alebo odmietnutie, pokiaľ ide o spôsob zaobchádzania s E-mailom, ktorý porušuje pravidlá. **„p=none: žiadna akcia“** **„p=quarantine: karanténa“** **„p=reject: odmietnutie”**
„sp“	Definuje požadovanú akciu príjemcu správ odosielaných napr. zo subdomén. Možné je zvoliť rovnaké hodnoty ako pri parametri „p“
„adkim a aspf“	Definujú, ako striktne sa majú uplatňovať pravidlá DKIM a SPF, pričom „s“ označuje prísne a „r“ označuje uvoľnené.
„RUA“	Označuje adresu, kam sa má posielať súhrnný prehľad DMARC z domén, ktoré obdržali správu z našej domény. Odosielateľ určí cieľovú adresu v nasledujúcom formáte: **rua=mailto:domain@example.com**
„RUF“	Podobne ako pri RUA označuje, kam by sa mali odosielať forenzné správy DMARC. Odosielateľ určí cieľovú adresu v nasledujúcom formáte: **ruf=mailto:domain@example.com**

Zdroje:

https://www.radicati.com/wp/wp-content/uploads/2018/12/Email-Statistics-Report-2019-2023-Executive-Summary.pdf
https://www.smartertools.com/blog/2019/04/09-understanding-spf-dkim-dmarc
What is phishing? How this cyber attack works and how to prevent it | CSO Online
Spam & Phishing | Phishing Scam Threats | Kaspersky
What Are DMARC, DKIM, and SPF? | Trendline Interactive
https://www.akadia.com/services/spf.html
https://www.esecurityplanet.com/applications/how-to-set-up-implement-dmarc-email-security.html#DMARC
https://www.cyber.gov.au/acsc/view-all-content/publications/how-combat-fake-emails
https://dmarcian.com/spf-syntax-table/
https://www.mailhardener.com/kb/spf/
How to Set up SPF and DKIM with Postfix on Ubuntu Server? | Pepipost (netcorecloud.com)