```
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=nic.cz; s=default;
    t=1414663003; bh=qEs+Qt8DFtEuJTHfMVQu3FgWFMMf5TMVdcVS/z3nkOU=;
    h=Message-ID:Date:From:MIME-Version:To:Subject:References:
     In-Reply-To:Content-Type;
    b=DX39MKw8+T7xic4oWp+7VlCTR+XEbdU3vVBwO6f70VrGCKpk7FNVT4lHEFVFAV39Q
     EOZNSxeBuEM7htjYRzHvdeJytaf9ee6BYe6SMUHRFn2DIyJTzCgOvimhlne1q5GrSw
     UQiwSxJf1Xs54VA0KKvrLekOhvJAN4p2dhF+rKEA=
```

V hlavičce zprávy se v případě použití technologie DKIM objeví položka DKIM- Signature.

Do /etc/postfix/master.cf se pak následně přidá:

```
policy-spf unix - n n - - spawn
user=nobody argv=/usr/bin/policyd-spf
```

Pokud jde o Perl, pak se přidá:

```
policy-spf unix - n n - - spawn
user=nobody argv=/usr/sbin/postfix-policyd-spf-perl
```

Poslední, co je třeba nastavit, je smtpd_recipient_restrictions v /etc/postfix/main.cf:

```
smtpd_recipient_restrictions =
…
permit_sasl_authenticated
permit_mynetworks
reject_unauth_destination
check_policy_service unix:private/policy-spf
```

Po restartu postfixu pak zkontrolujte logy, ve kterých byste nyní měli vidět záznamy o odmítnutí či podržení e-mailu v souvislosti s provedenou SPF kontrolou. Doporučujeme vyhledat si na internetu či v odborné literatuře i další možnosti nastavení SPF.

V případě, že používáte e-mailový server od Microsoftu, v nástroji Edge transport server je spuštěná ve výchozím nastavení služba SenderID. Pokud poštovní server přijme zprávu, Edge transport server se zeptá DNS serveru na záznamy o doméně odesílatele a zkontroluje, zda je IP adresa, ze které zpráva přišla, autorizovaná k odesílání zpráv pro danou doménu.

Podle toho, jak tento proces dopadne, se zprávě přiřadí označení pass, fail, none nebo jiné. Více informací o SenderID můžete získat přímo na stránkách Microsoftu. Pokud používáte jiný e-mailový server než výše uvedené, doporučujeme konzultovat nastavení SPF podle manuálu ke konkrétnímu e-mailovému serveru.

DomainKeys Identified Mail

DKIM (DomainKeys Identified Mail), popsaný ve standardu RFC 6376, validuje obsah zprávy. Tato metoda ověření těla zprávy umožňuje ověřit pravost odesílatele. Zajímavé je, že DKIM nebyl původně zamýšlený jako nástroj proti spamu, přesto v boji proti tomuto nešvaru pomáhá.

Možnosti uživatelského nastavení SPF

all	přidává se na konec záznamu
include	definuje další oprávněné domény např. „v=spf1 include:mail.nic.cz include mail.csirt.cz –all“
a	pokud není specifikováno jinak, odpovídá v případě, že doménové jméno má záznam typu A nebo AAAA; tento záznam je stejný jako adresa odesílatele
mx	pokud má doménové jméno MX záznam, který odpovídá adrese odesílatele, pak nastane shoda
ptr	pokud PTR záznam odpovídá aspoň jednomu A záznamu, pak nastane shoda
IPv4	pokud je odesílatel z daného rozsahu IPv4, nastane shoda
IPv6	pokud je odesílatel z daného rozsahu IPv6, nastane shoda
exists	určuje domény, které jsou vybrané jako výjimky. Tento mechanismus je používaný jen zřídka

[DKIM (DomainKeys Identified Mail), popsaný ve standardu RFC 6376, validuje obsah zprávy. Tato metoda ověření těla zprávy umožňuje ověřit pravost odesílatele.]

Pokud by došlo k plošnému nasazení této metody, donutila by odesílatele spamu spojit obsah zprávy se skutečnou zdrojovou doménou. V hlavičce zprávy se v případě použití technologie DKIM objeví položka DKIM – Signature.

Příjemce zprávy se následně dotazuje na doménu odesílatele a ověřuje, zda se podpis ve zprávě shoduje s veřejným klíčem uloženým v DNS záznamu domény odesílatele.

Z toho vyplývají dva procesy, které jsou součástí služby MTA (Mail Transfer Agent). Jde o podepsání zprávy na straně odesílatele a její následující ověření na straně příjemce.

Pro implementaci DKIM je třeba vygenerovat jeden pár klíčů. Soukromý klíč se uloží na e-mailovém serveru odesílatele a bude sloužit k podepisování zpráv. Do DNS záznamů se pak přidají TXT RR záznam obsahující nastavení DKIM a samotný veřejný klíč.

Implementace DKIM

Pokud chcete kontrolovat DKIM záznamy u příchozí pošty, je třeba tuto kontrolu na e-mailovém serveru nastavit.

Jestliže používáte SpamAssasin pro povolení kontroly DKIM záznamů na příchozí poště, stačí v souboru local.pre zrušit zakomentování řádku.

```
loadplugin Mail:SpamAssassin:Plugin:DKIM
```

Zároveň je ale třeba nainstalovat balíček Perl skriptů, které budou sloužit jako DKIMProxy.

```
apt-get install libmail-dkim-perl
```

Dále je u DKIM nutné definovat politiku pro odchozí (DKIMproxy.out) i příchozí (DKIMproxy.in) zprávy.

Výchozí skóre pro označení podepsaných zpráv je poměrně nízké, protože odesílatelé spamu si mohou teoreticky zaregistrovat vlastní doménu a v ní DKIM implementovat.

V praxi však to není zcela běžné, protože v okamžiku, kdy začne odesílatel spamu zprávy podepisovat, víme jistě, že odesílatelem byla daná doména, a můžeme tedy příjem pošty z této domény zablokovat.

DKIM Proxy byl primárně určený pro Postfix, měl by ale fungovat i s jinými e-mailovými servery. Více o fungování a možných nastaveních najdete přímo v manuálu DKIMProxy.

Další možností je OpenDKIM, který implementuje jak službu DKIM, tak aplikaci na bázi „milter“ (mail-filter), jež pracuje jako plug-in ve všech MTA, které jsou schopné ji rozpoznat.

Pokud server příjemce kontrolu DKIM nevykonává, část hlavičky s DKIM podpisem se ignoruje a zpráva se přijme. Implementace DKIM tedy příjemce zpráv nijak neomezí – naopak si může být jist, že se doména odesílatele ověří.

Vzhledem k tomu, že jde o kontrolu DNS záznamů, je vhodné implementovat zároveň i DNSSEC, který zajistí správnost záznamů získaných z DNS, čímž zvyšuje důvěryhodnost celého systému. ■

Autorka pracuje jako bezpečnostní analytička ve sdružení CZ.NIC a je členkou národního bezpečnostního týmu CSIRT.CZ.