Zatočte se spamem

Není žádnou novinkou, že velkou část e-mailových zpráv, které se v dnešní době rozesílají, tvoří spam. Samotný protokol SMTP totiž umožňuje nastavit libovolnou e-mailovou adresu odesílatele. To se často zneužívá nejen v případě spamu a phishingu, ale například také při podvodech, při nichž se pachatel vydává za někoho, kým není.

ZUZANA DURAČINSKÁ

Z informací od společností a jednotlivců, jejichž doménové jméno bylo zneužité k rozesílání spamu, je zjevné, že takovéto použití domény je velmi nepříjemné a její držitel, kterého většina adresátů považuje za skutečného odesílatele spamu, pak dostává doslova moře e-mailů. Naštěstí se lze proti zneužití domény k tomuto účelu efektivně bránit.

Existují dva základní přístupy. Jedním je kontrola původu zprávy (SPF, Sender Policy Framework), druhým potom kontrola na základě obsahu zprávy (DomainKeys Identified Mail). Obrana se však vždy musí implementovat jak na straně držitele domény, tak u příjemce.

[V linuxových distribucích lze vykonávat kontrolu SPF v postfixu pomocí skriptů napsaných v Pythonu nebo Perlu.]

Sender Policy Framework

V téměř všech falešných e-mailových zprávách je adresa odesílatele podvržená. Aby součástí podvržených e-mailových adres nebylo také vámi používané doménové jméno, je třeba zahrnout SPF (Sender Policy Framework) do DNS záznamů dané domény.

SPF je otevřený standard definovaný IETF v RFC 4408, umožňující určit, která zařízení budou autorizována pro odesílání e-mailové pošty s adresou obsahující danou doménu.

Pokud se tato informace vloží do DNS záznamů domény, může si ji příjemce snadno ověřit a v případě neshody zprávu odmítnout ještě před přijetím těla zprávy. Záznam SPF je jednoduchý textový řetězec, který má následující strukturu:

```
"v=spf1 +mx a:mail.nic.cz –all"
```

V tomto příkladu přijme server poštu z dané domény pouze v případě, pokud se odeslala z některého ze serverů uvedených v rámci MX záznamů (+mx) nebo ze serveru s IP adresou, na kterou je přeložený A záznam pro mail.nic.cz (a:mail.nic.cz). Pošta z dané domény, která by se poslala z jiných IP adres, se odmítne. Nastavení je možné podle vašich potřeb, viz tabulka.

Obvykle má téměř každé omezení i své stinné stránky a nejinak je tomu i v případě SPF. Před jeho nasazením je třeba zhodnotit možné dopady na omezení povolených odesílatelů e-mailové pošty.

SPF záznam sice vhodně omezuje možné zneužití doménového jména k rozesílání nevyžádané pošty, na druhou stranu však také limituje uživatele ohledně použití konkrétních e-mailových serverů, což někdy bývá překážkou při jeho nasazení. Je také vhodné připomenout, že tento mechanismus je závislý na DNS, a v případě podvržení DNS záznamů se tak stane neúčinným.

Implementace SPF kontroly na e-mail serveru

Kromě ošetření SPF záznamů na doméně je také třeba myslet na jejich kontrolu při přijímání pošty na e-mailovém serveru. Pokud neprovozujete vlastní e-mail server, měli byste se informovat u provozovatele e-mailového serveru, zda vykonává kontrolu SPF automaticky či zda je možné ji spustit jako součást antispamové ochrany.

Zda se totiž SPF záznam bude kontrolovat, záleží pouze na provozovateli daného e-mailového serveru. Pokud provozujete vlastní poštovní server, můžete využít základní konfiguraci kontroly SPF pro Postfix a Microsoft Exchange server. Zde je ukázka ohledně *Postfixu*.

V linuxových distribucích lze vykonávat kontrolu SPF v postfixu pomocí skriptů napsaných v Pythonu nebo Perlu. Instalace pak bude v závislosti na preferovaném jazyku vypadat podle jednoho z následujících příkladů:

```
sudo apt-get install postfix-policyd-spf-python
```

nebo

```
sudo apt-get install postfix-policyd-spf-perl
```

Následně je třeba přidat do /etc/postfix/main.cf řádek, který zabrání time-outu během zpracovávání e-mailové zprávy:

```
policy-spf_time_limit = 3600s
```