

E-mailové služby

Důvody nepřijmutí emailu

Antispam ověřuje správné nastavení serveru odesílatele. Každé chybné nastavení serveru, které může znamenat, že se jedná o server spamera, zvyšuje hodnotu skóre antispamu (vysvětleno níže).

Zde je popsán přehled základních správných nastavení poštovního serveru, které zvýší pravděpodobnost doručení emailu a nezachycení emailu na antispamovém filtru:

Poštovní server má platný popředný (A) a zpětný (PTR) záznam v DNS ke svojí IP adrese:

```
$ nslookup testmailserver.vshosting.cz
```

```
Name: testmailserver.vshosting.cz  
Address: 192.168.50.25
```

```
$ nslookup 192.168.50.25
```

```
25.50.168.192.in-addr.arpa    name = testmailserver.vshosting.cz.
```

HELO poštovního serveru je platné FQDN (<https://cs.wikipedia.org/wiki/FQDN>), které se shoduje s popředným (A) záznamem v DNS pro IP adresu serveru:

```
$ telnet testmailserver.vshosting.cz 25  
Trying 192.168.50.25...  
Connected to testmailserver.vshosting.cz.  
Escape character is '^]'.  
220 testmailserver.vshosting.cz ESMTP
```

IP adresa poštovního serveru není uvedena na blacklistu:

Pro ověření, zda není IP adresa na blacklistu lze využít např. webovou službu <http://mxtoolbox.com/blacklists.aspx>

Doména odesílatele (část za znakem @) má nastaven SPF záznam - <https://cs.wikipedia.org/wiki/SPF>

Emaily odesílatele jsou podepisovány pomocí DKIM - https://cs.wikipedia.org/wiki/DomainKeys_Identified_Mail

Doména odesílatele (část za znakem @) se nemusí shodovat FDQN poštovního serveru a také se obvykle neshoduje!

Způsob vyhodnocení emailu antispamovým systémem

Antispamový systém vyhodnocuje, zda je email vyžádanou zprávou HAM (angl. pravá šunka) nebo nevyžádanou zprávou SPAM (angl. namleté zbytky masa a

E-mailové služby

náhražky) na základě výpočtu spamscore.

Do výpočtu score vstupuje řada testů - např. platný DKIM podpis a platný SPF záznam score snižuje, naopak pro SPAM běžná slova jako penis, sex, sleva, výhra a pod. score zvyšují.

Kromě pravidel se do score započítává také výsledek testování statistickým filtrem (bayer), který na základě porovnání s databází vzorků četnosti slov, slovních obrátů a vět určí pravděpodobnost zda je email SPAMem či HAMem a podle toho spamscore zvýší nebo sníží.

Do celkového score se dále započítávají pravidla vyhodnocující technicky korektní chování poštovního serveru odesílatele a v neposlední řadě pravidla kontrolující přítomnost emailové adresy odesílatele a IP adresy poštovního serveru na seznamech známých spamerů (blacklisty).

Dalšími prvky zvyšujícími spamové score jsou blacklistované odkazy (URI blacklisty) v těle emailu, obrázky obsažené v těle emailu nebo odkazované z těla emailu a pro SPAM typické pojmenování a obsah příloh.

Antispamový systém se do jisté míry prolíná s antivirovou ochranou, která buď z emailu odstraní virus/malware nebo email v případě nemožnosti odstranění odmítne.

Unikátní ID: #1000

Autor: Technická podpora

Aktualizováno: 2016-04-16 21:26