# Google, PayPal, Yahoo, Amazon, eBay, Twitter a další používají slabé DKIM klíče

Vložil/a cm3l1k1 [1], 26 Říjen, 2012 - 13:06

- Encryption [2]
- Hacking [3]
- Security [4]

Matematik Zachary Harris objevil souhrou náhod, že Google používá slabý DKIM (512-bit) klíč, který jednoduše cracknul na Amazon Web Services během 72 hodin za $75 a mohl tak posílat důveryhodné emaily z adres @google.com
Poté se podíval na zoubek i dalším populárním službám a zjistil, že podobným problémem trpí i PayPal, Yahoo, Amazon, eBay, Apple, Dell, LinkedIn, Twitter, SBCGlobal, US Bank, HP, Match.com, HSBC a další.

Zachary Google upozornil tím, že jeden takový podvržený email poslal jeho zakladatelům :). Bez reakce ze strany Googlu byli původní klíče revokovány a nyní mají délku 2048-bit.

DKIM [5] je spolu s SPF [6] záznamy další ochranou před podvrhnutým emailům.

## SPF (Sender Policy Framework)

Příklad SPF recordu pro Security-Portal.cz

```
cm3l1k1@deuterius cm3l1k1 $ dig +short txt @ns1.websupport.sk security-portal.cz
"v=spf1 a mx include:_spf.websupport.sk ?all"
"spf2.0/pra a mx include:_sid.websupport.sk ?all"
```

Příklad pro Google:

```
cm3l1k1@deuterius cm3l1k1 $ dig @ns1.google.com google.com txt | grep spf
google.com.             3600    IN      TXT     "v=spf1 include:_netblocks.google.com
ip4:216.73.93.70/31 ip4:216.73.93.72/31 ~all"
```

SPF recordem vlastně definujete z jakých mail serverů může být odeslán email pro danou doménu. Pokud tedy někdo jednoduše podvrhne zdrojovou adresu (From:) a váš mail server ověří, že podle SPF zdrojový server není oprávněný k posílání emailů z dané domény, tak je brán jako spam.
Více o SPF zde: http://www.openspf.org/ [7]

## DKIM (DomainKeys Identified Mail)

DKIM přináší asymetrické šifrování, kdy je veřejný klíč uložen v DNS recordu.

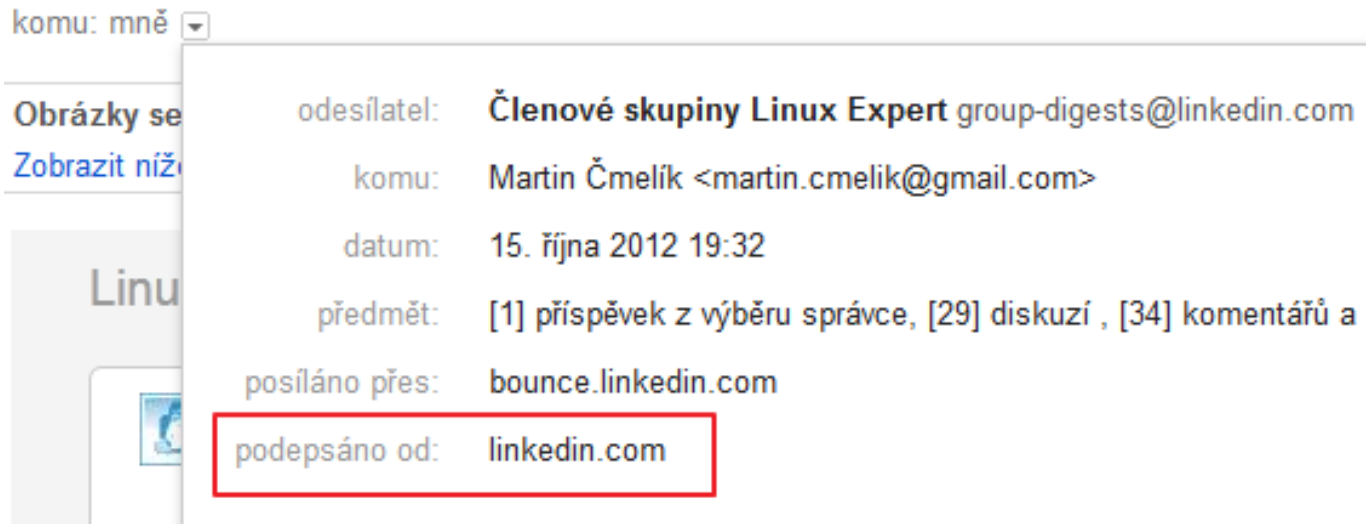
Příklad DKIM pro Twitter:

```
cm3l1k1@deuterius cm3l1k1 $ dig +short txt dkim._domainkey.twitter.com
"v=DKIM1\;" "g=*\;" "k=rsa\;"
"p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCrZ6zwKHLkoNpHNyPGwGd8wZoNZOk5buOf8wJwfkSZsN
llZs4jTNFQLy"
"6v4Ok9qd46NdeRZWnTAY+lmAAV1nfH6ulBjiRHsdymijqKy/VMZ9Njjdy/+FPnJSm3+tG9Id7zgLxacA1Yis
```

```
/18V3TCfvJrHAR/a77Dxd65c96UvqP3QIDAQAB"
```

Při posílání emailů firemní SMTP server podepíše zprávu privátním klíčem a umístí podpis do hlavičky emailu (DKIM-Signature:). Příjemce (mail server, aplikace příjemce) stáhne z DNS veřejný klíč a ověří, že tělo emailu nebylo změněno.

Pěkné a efektivní.
Používáte-li např **Gmail**, můžete ověření podpisu vidět přímo z rozhraní Gmailu:




## Závěr

Dávejte si pozor kdo vám emaily posílá a pokud vám na bezpečnosti opravdu záleží používejte (správně) PGP/GPG [8] klíče a také si rozšiřte všeobecné povědomí o šifrování [9].

Zdroj:
http://www.wired.com/threatlevel/2012/10/dkim-vulnerability-widespread/all/ [10]

**URL článku:**
https://security-portal.cz/blog/google-paypal-yahoo-amazon-ebay-twitter-dal%C5%A1%C3%AD-pou%C5%BEivaj%C3%AD-slab%C3%A9-dkim-kl%C3%AD%C4%8De

**Odkazy:**
[1] https://security-portal.cz/users/cm3l1k1
[2] https://security-portal.cz/category/tagy/encryption
[3] https://security-portal.cz/category/tagy/hacking
[4] https://security-portal.cz/category/tagy/security
[5] http://www.dkim.org/
[6] http://www.openspf.org
[7] http://www.openspf.org/
[8] http://en.wikipedia.org/wiki/Public-key_cryptography
[9] https://security-portal.cz/clanky/praktické-základy-kryptologie-steganografie
[10] http://www.wired.com/threatlevel/2012/10/dkim-vulnerability-widespread/all/