Emaily s garantovaným odesílatelem a obsahem v praxi s využitím DKIM

Ing. Tomáš Hála
ACTIVE 24, s.r.o.
www.active24.cz

Obecně o DKIM

- využívá asymetrické kryptografie
- veřejná část klíče uložena v DNS
- garantuje integritu obsahu emailu
- garantuje odesílatele na úrovni domény
- řeší ho poskytovatel služby, nikoliv koncový uživatel

Jak funguje DKIM na straně odesílatele

- veřejná část klíče v TXT DNS záznamu:

selector._domainkey IN TXT "v=DKIM1; k=rsa; p=MIGfMA0GCS.....frzshgrwIDAQAB"

- SMTP server poskytovatele každý odeslaný email podepíše privátní částí klíče a podpis umístí do hlavičky emailu (DKIM-Signature)

dkim-signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=active24.cz;
s=dkim1; t=1298013027; bh=BpBHK1G9OXl6ZjM4Z7CLR33YamjazhlaeWpODFYPNEg=;
h=Message-ID:Date:From:User-Agent:MIME-Version:To:CC:Subject:
References:In-Reply-To:Content-Type:Content-Transfer-Encoding; b=y
tCoFZaenRThbNg85Q767fIN9D7TPKFVI5ZnQxrigVm4JAv2HbRMscVu19AWXm8qG8hT
Lb4tdvXbmAkfWyZISGdoWr6ejQahksjruB3mgPll6D0tf6lh3XVemnTNYUYMK3/eAL2
L/02+jDgYI89Zf3pJN0VkiXJpTtPmaZCyiBQ=

- přidání DNS záznamu je díky selectoru bez rizika (na rozdíl od SPF)

- snadné testování na ostré doméně bez ohrožení produkčního provozu emailové komunikace

Jak funguje DKIM na straně příjemce

- pokud server/klient příjemce DKIM nezná, hlavičku ignoruje

- pokud DKIM zná, ověří platnost podpisu (pomocí klíče v DNS záznamu) a na základě výsledku může s emailem nějak naložit

- jak se s emailem naloží, záleží na provozovateli, ale typicky se:
  1) email zvýhodní na spamfiltru
  2) zvýrazní, že došlo k ověření integrity a odesílatelovy domény

- při použití parametru „t=y“ se dle specifikace s emailem musí nakládat stejně, jako by podpis vůbec neobsahoval

- výsledek by měl být buď pozitivní nebo stejný jako bez podpisu

Jak pro DKIM definovat podpisovou politiku

- samotné DKIM nijak neřeší, jak s emailem naložit na základě výsledků validace

- k tomuto účelu vzniklo rozšíření ADSP – další TXT DNS záznam:
  _adsp._domainkey (bez selectoru) – “dkim=unknown/all/discardable“

- odesílatel si sám definuje politiku, jak s emaily naložit

- restriktivní politika se používá jako obrana proti phishingu

- příjemce by měl definovanou politiku rozhodně respektovat

Jak jsme DKIM nasadili v ACTIVE 24

- používáme dkim-milter upravený tak, aby zohledňoval SASL login

- implementovali jsme nástroje, které se starají o automatické umístění správného DNS záznamu u domén, splňujících vstupní podmínky

- seznam domén k podepisování se pravidelně aktualizuje podle kontroly existence správného DNS záznamu

- nasazení nijak negativně neovlivnilo odchozí poštu a zákazníci ani nezaznamenali změnu

Jak jsme DKIM nasadili v ACTIVE 24

- jako jediná webhostingová společnost v ČR provozujeme DKIM na zákaznických doménách a to zcela zdarma

- tím jsme tuto technologii zpřístupnili široké veřejnosti k provozování na vlastních doménách

- zajišťujeme automatické umístění TXT záznamu a podepisování

- v případě příjmu emaily výrazně zvýhodňujeme na spamfiltru

- politiku ADSP nedefinujeme (nemůžeme)

Jaké jsou hlavní výhody DKIM

- vše zajišťuje poskytovatel služby, koncový uživatel se o nic nestará

- podepsané emaily s výrazně větší pravděpodobností nebudou označeny za spam

- při dopisování v rámci domény není třeba definovat whitelist, který stejně není účinný (maily poslané „sami sobě“ apod.)

- při důležité komunikaci si obě strany mohou ověřit, že odesílatel emailu není podvržený a obsah emailu se od odeslání nezměnil

Kdo DKIM používá

- gmail.com (Google) – nejen podepisuje, ale i zvýrazňuje ve webmailu

- Seznam.cz (podepisuje)

- Paypal.com a podobní (ADSP)

Jak DKIM souvisí s SPF či DNSSEC

- SPF je odlišná technologie určená pouze k ověřování IP adresy odesílatelova mailového serveru

- nedokáže garantovat integritu, ověření odesílatele je slabší

- nastavení SPF ovlivňuje všechny emaily na doméně

- hrozí penalizace emailů (zejména při automatickém přeposílání)

- DKIM a SFP je možné kombinovat – navzájem se nevylučují

- DNSSEC garantuje integritu samotných DNS záznamů, na kterých je fungování DKIM postaveno

active 24

Je možné dostat spam podepsaný pomocí DKIM?

Je možné dostat spam podepsaný pomocí DKIM?

- samozřejmě je to možné, DKIM není primárně antispamová technika (ačkoliv se tak často označuje)

- v praxi jsme takový případ ještě nezaznamenali (jen nedoručenky)

- pokud bude ale spam validně podepsán, je pevně svázaný s konkrétní doménou a lze ho tedy snadno filtrovat

- výrazně se také zvyšují možnosti dohledání skutečného odesílatele a „zaříznutí“ zdroje spamu

- podepsaný spam by nemohl uvádět falešnou identitu odesílatele, což je jedna z hlavních vlastností spamu

active 24

Typy pro praxi

- ladění přes autorespond+dkim@dk.elandsys.com
  případně přes schránky u active24.cz nebo na gmail.com

- spamassassin:
    - loadplugin Mail::SpamAssassin::Plugin::DKIM
    - pravidla DKIM_SIGNED, DKIM_VERIFIED a další

- rychlý návod na základní zprovoznění např. zde:
  http://www.abclinuxu.cz/clanky/bezpecnost/dkim-podepisujeme-e-maily-na-serveru

- nechcete-li DKIM zprovozňovat svépomocí, stačí mít doménu a emailové schránky (hosting) u toho správného poskytovatele :)

Závěr

- nasazení DKIM nemá v praxi žádné negativní dopady, je tedy bezpečné ho uvést do provozu (díky rozumné implicitní politice)

- DKIM vede ke značnému zdůvěryhodnění emailové komunikace

- rozšiřování této technologie je určitě na místě a do budoucna může velice prospět k omezení anonymního spamu a emailových podvodů, jako je phishing

Prostor pro Vaše dotazy