

Spam védelem

DKIM

A DKIM igazából nem egy spam védelmi technológia, hanem egy kriptográfiai aláírás. A levélküldő szerverünk (tehát nem a saját gépünk) a küldéskor digitálisan aláírja a levelet, így védve az illetéktelen módosítások ellen. Spam védelem akkor lesz ebből, ha a domain TXT rekordjában olyan szabályt adunk meg, hogy a fogadó szerver minden aláíratlan levelet dobjon el, ezzel védekezve a nevükben írt e-mail-ek ellen (hiszen minden aláíratlan levél a szabály szerint hamisítvány). Ez akkor hasznos, ha kevés számú felhasználó kizárólag 1-2 szerveren keresztül levelezik.

SPF

MŰKÖDÉSE

Az SMTP protokoll eredeti működése szerint bármely számítógép bármilyen feladó címmel küldhetett e-mail-t. Ennek következtében egyszerű dolga van a spammereknek, hiszen könnyen hamisíthatják a feladó címeket (Return-Path fejléc). Az SPF ezt lenne hivatott orvosolni azzal, hogy domainenként meghatározható, hogy mely szerverek küldhetnek az adott domain alá tartozó e-mail címről levelet. Ezeket az információkat a domainhez tartozó TXT rekordban kell publikálni.

PROBLÉMÁK

Az SPF egyetlen fontos paramétert hagy figyelmen kívül az SMTP működésében, nevezetesen az átirányítást. Ha egy szerveren be van állítva egy adott címre átirányítás és az a szerver, ahova átirányították a levelet, ellenőríz SPF-et, adott esetben el fog utasítani legitim levelet, hiszen nem az a szerver továbbította, amelyet az SPF bejegyzés engedélyez. Erre a problémára ugyan születtek megoldási próbálkozások, azonban ezek mindegyike csak akkor tud működni, ha az Interneten fellelhető összes szerver implementálja ezeket.

JAVASLAT

Ne használjunk SPF rekordot, több fejfájást tud okozni, mint amennyi előnye van. Helyette inkább használjunk DKIM-et.

További információ:

[Wikipedia](#)

[Why you shouldn't jump on the SPF bandwagon](#)

[Sender Policy Framework project](#)

DCC

A DCC (Distributed Checksum Clearinghouses) minden levélből számol egy ellenőrzőszámot (amely a levél tartalmának változásával más lesz) és számolja az azonos leveleket. Rövid idő alatt érkező sok azonos levélnél (pl spam) figyelmeztet és a spamszűrőben növeli a levél spam pontszámát. (Elég magas pontszám fölött a levelet a rendszer spamnek minősíti.)

A natív Bayes elemző felhasználói visszajelzésből dolgozik. Amennyiben egy levelet megjelölünk, hogy spam vagy nem spam, azt az elemző un. tokenekre bontja és mindegyikhez rendel egy értéket. A teljes levélhalmazból kialakul az egyes szavakra, hogy mennyire valószínű az előfordulásuk a spamekben illetve a valós levelekben.

PYZOR

A Pyzor a Razor spamszűrőből indult ki és hozzá hasonlóan a levelekből számolt ellenőrzőszámmal dolgozik. A közösségi szerveren ezeket az ellenőrzőszámokat gyűjtik és többféle algoritmus szerint elemzik.

RAZOR

A Razor egy zárt forrású közösségi spamszűrő szerver. További információ: [Vipul's Razor](#)

Változat #1

DotRoll Tudásbázis hozta létre 22 szeptember 2023 08:31:18

DotRoll Tudásbázis frissítette 22 szeptember 2023 08:34:06