Deutschlandfunk

Home › computers and communications › spam tackled at its root › **04/08/2007**

packed spam at the root

New signature system to help eliminate email trash

<Strong> Everyone knows it, the unwanted mails sent every day and bring dubious advertising or even bring in viruses and other pests. One method that has the Internet Engineering Task Force now standardized, is intended to remedy. </ Strong>

By Achim Killer

They gave the name, tinned meat in an Australian supermarket. (Stefan lamp)

DomainKeys Identified mails called the process by which the IETF, the Internet Engineering wants to proceed Taskforce against emails with forged senders. "We speak Dikim out. That says more easily. It is a mechanism that uses digital signatures to prove that a mail was actually sent by the sender's domain from. " So Barry Leiba by the IETF. The domains are indeed the problem with spam. The large mail service providers like T-Online and AOL ensured that on accounts with them any bulk mailer is sent, so that you can be reasonably sure that a mail that has been sent via AOL, no spam is. But you can not stop to be sure that a mail has been actually sent via AOL. And for that very reason DKIM is with the operators of mail servers on: "If, Joe At aol dot com 'sent an e-mail, then it is from, Aol Dot com' signed and not from Joe." So the server, the mail the sent, calculates a checksum encrypted with the private key and appended to it. The server that receives the mail, decrypts the checksum with the public key of the sender and automatically calculates a. If they match, it delivers the mail. If not, he throws it away or he delivers them from but warns the recipient but that it is suspicious. Such a complicated process is necessary because the return address of a mail is very easy to falsify. Jim Fenton from the router manufacturer Cisco, the DKIM co-initiated: "The, Simple Mail Transfer Protocol ', is used to transport messages on the Internet, it allows you to use any return address, and which also has its meaning If one example of.. a website an Internet newspaper wants to send an item to a friend, then actually sent the Internet publication this article. but you used the address of the person who has caused the. purpose of DKIM it, something continued to allow is malicious "to prevent deception but. been Iniitiert is DKIM by Yahoo and Cisco. Meanwhile, it is also supported by IBM, Google, AOL, cryptography firm PGP and several others. And also the first implementations already exist. Dave Crocker of the MIPA, the organization to which these companies have come together: "Yes, there are already programs and Internet services that use DKIM to sign messages and those who use it to check mails Since DKIM.. but only recently is a default, the list of supporters is not too long. but it is more. and all indications are that in the course of all the major manufacturers and service providers will join. " the technologies used DKIM how asymmetric encryption, are well known and -bewährt says Crocker. "It now turns only aim is to persuade companies to use software with DKIM functionality. New software is always a challenge. the IT departments must eventually it just are that everything runs smoothly. This is not difficult in the case. But it takes time. " the IETF makes meanwhile already thinking of the time when DKIM will have once established. It's mostly about the question of how to deal with messages that are sent from domains from who refuse to DKIM and not sign. The there will be in any case. Spammers at least put it, and currently register domains that sound similar to those established mail and financial services. The race between IT security people and spammers continues. But with DKIM security people could receive a hefty lead at least once.

[t]