

Trend Micro vs. SPAM

Hardy Viilup
Stallion AS

SPAM

- Algselt Hormel Foods Corporation lihakonservide sarja kaubamärk
- Monty Pythoni 1970 a. toitlustamise teemalises sketšis kasutati sõna SPAM nii ohtralt, et see risustas kõnet. Sealt kandus see edasi ka teistele valdkondadele.
- Spämm IT maailma mõistes - soovimatu e-post



Fakte spämmi kohta

- Üle 50% asutuse sisenevatest meilide hulgast on spämm
- E-Maili saatmine on odav. Tühine hulk spämmereid võib interneti spämmiga üle ujutada.
- Spämmi käitlemiseks kulub palju aega. 3 sek.
* 50 maili * 100 inimest = 250 minutit päevas
= 63,4 päeva aastas

Spämmi hind

Number of employees with email	250	1000	5000	10,000	25,000
Percentage of email that is spam*	40%	40%	40%	40%	40%
Average annual cost of spam per employee**	\$188	\$188	\$188	\$188	\$188
IT maintenance services - hours per month	10	10	10	10	10
Annual total cost of spam per organization	\$51,989	\$192,614	\$942,614	\$1,880,114	\$4,692,614
* typically 30-60%, based on Trend Micro/Postini Email Stat Track Research ** based on spending 3 seconds per spam email for 220 paid workdays per year					

Spämmi hinna kalkulaator:

<http://www.trendmicro.com/form/spam/default.asp?id=calculator>

Trend Micro lahendus

Koosneb mitmest osast:

- RBL+
- Network Anti-Spam Solution
- SPS (Spam Prevention Service)
- Signatuuripõhine filter

} Esimene
kaitseliin

RBL+

- Trend Micro ostis ära Kelkea Inc., IP filtrite ja maine-teenuste osutaja, tundub kui MAPS listi pidaja (vt. <http://www.mail-abuse.com>)
- Trend Micro RBL+ suudab peatada 40–80% kahtlasi e-maile saatvatest ühendustest.
- Sisaldab open-relay, open proxy, real-time black-hole ja dial-up kasutajate IP aadresside nimekirju
- Sisaldab hetkel 1.6 miljardit IP aadressi, vastavuses spämmimistegevusest tuleneva mainehinnanguga

Network Anti-Spam Service

- Sisaldab RBL+ teenust
- Botnet'ide ja zombide IP aadresside nimekiri. Uuendatakse reaalajas.
- Ühildub enamlevinud MTA'dega, ka Postfix, qmail ja Sendmail'iga
- Rünnete tõkestamine (e-posti viirused, phishing, directory harvesting)

Signatuuripõhine filter

- Keskne spämmi-signatuuride andmebaas
- Ei ole efektiivne, kuna spämmi hulk on suur, spämmerid on õppinud seda tüüpi filtreid üle kavaldama.

Spam Prevention Solution (SPS)

- Integreerub Trend Micro toodetega ja ka kolmanda partei MTA-dega
- Heuristiline spämmituvastusmootor
- Paindlik ja skaleeruv
- Edumeelne haldus, End-User Quarantine kaudu kasutajatelt laekuvat tagasisidet arvestatakse spämmifiltri seadistamisel

SPS poolt kirjutatud päise näide

X-imss-version: 2.5

X-imss-result: Default_Triggered

X-imss-scores: Clean:0.00000 C:2 M:14 S:5 R:5

X-imss-settings: Baseline:6 C:4 M:4 S:4 R:4
(2.0000 2.0000)