Spam fiters at CERGE-EI

Incoming emails

Incoming email filtering consists from several steps:

Step 1: Fortimail

Appliance gw.cerge-ei.cz - Fortimail from Fortinet vendor

Fortimail checks for: IP reputation, SPF, DKIM, DMARC, viruses, suspicious content, phishing links, newsletters, executable files, encrypted files etc.

Malicious content - is blocked and is put to system quarantine for further analysis.

Suspicious content - usualy add warning to the subject - warning texts are in lowercase: [Spam], [Newsletter] , [Warning - bad SPF] etc.

Step 2: Ironport

2 appliances iport.cerge-ei.cz and iport2.cerge-ei.cz - Cisco Email Security Appliance

Primary appliance is iport (iport2 is auxiliary)

Filtrace na spam je několikastupňová.
1. První filtr je Fortimail, který kontrolujeme my a pokud by měla být nějaká reklamace na něj, potřebujeme dohledávat podle parametrů zprávy, času, odesílatele a podobně. Pak lze celkem dobře a přesně zjistit v logu, co se stalo, proč a jak se zprávou naložil.
2. Druhý filtr je Ironport, který mimo jiné zprávy značkuje [suspected spam].které propouští ihned dál a [spam], které zařazuje do uživatelské karantény a posílá o tom uživateli zprávu (v současnosti během pracovní doby každou hodinu). Zprávu z karntény lze uvolnit, případně jde i uživatele označit jako čistého pro příští bezproblémové doručení.
3. Poslední serverový filtr je Zimbra, která může přeřadit zprávu do Junk folderu. Jeho filtrace je dohledatelná v hlavičkách zprávy. Viz i výše uvedený text na wiki, poslední ilustrovaný odstavec o hlavičkách zprávy.
4. Úplně poslední filtraci dělá i klient, Thunderbird nebo Outlook.