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)

Ironport checks for: IP reputation, viruses, spam signatures, mass-mail behavior, executable, encrypted files etc.

Malicious content - is rejected

Suspicious content - is put to personal quarantine. Warnings are added to the subject - warning texts are in uppercase: **[SPAM], [SUSPECTED SPAM]** etc.

User gets regular email digest about newly quarantined emails. It is possible to manually release email and even whitelist sender.

Step 3: Zimbra

Zimbra mailserver may put problematic email message to the Junk folder.

It uses Spamassasin for spam detection. User may check message headers for detailed info about spam detection (clasification etc.).

Step 4: Email client

Last step of detection is usualy done in user's client software (Thunderbird, Outlook, ...).

Each email client deals with suspicious content differently. It is necessary to be informed how your specific client works and where to find problematic emails (Junk folder, Spam folder, Newsletter folder etc.)