External Mail Connectivity Impaired 2012-06-25

External mail gateway overloaded due to SPAM attack

A user account on our internal mail system has been compromised and abused to send SPAM mails. The attack started around 2:40 p.m., Sun June 25th.

Symptoms

Due to the huge number of mails to process on the external mail gateway, the cluster software used to provide high-availability for this service was unable to verify the fitness of the provided services and stopped the processing of mails. Thus no mail passes from outside the University to the inside and vice versa.

Impact

Due to the huge number of SPAM mails currently spooled in the mail system it will take a while to clean up the queues. **No regular mail will be lost**, all mail in transit is spooled on either our internal mail server or on the mail servers of the sending side.

At 9 a.m. Monday morning it is not clear, if our mail servers are blacklisted on DNS black lists used for fighting SPAM, see also http://en.wikipedia.org/wiki/DNSBL. If this happened, IRC-IT will act promptly to remove these listings to return the mail connectivity back to normal.

Update 9:20 a.m.

The external mail gateway is back up again, and so far no listings in DNSBLs are visible, although major mail providers like Yahoo or AOL currently block mails from our mail server. This restriction will be lifted in the next few hours.

Update 9:40 a.m.

All mail systems are running clean again.

The cause of the SPAM attack has been identified as a password passed on by a Jacobs user due to a successful phishing attempt, the origin of the attack has been localized to an IP address range assigned to a Nigerian Internet service provider.

Herewith again a reminder to use a secure password - a combination of upper and lower case characters, numbers, punctuation and symbols. Avoid passwords, which are regular words found in dictionaries, also avoid passwords which are shorter than 8 characters. Change the password frequently, and no not - **never** - give the password to a third party!

Update 3:15 p.m.

Unfortunately the external mail gateway is again blacklisted by major mail providers, namely Yahoo, T-Online and AOL. Mail delivery to these addresses will be delayed.