FORSCHUNGSZENTRUM JÜLICH GmbH

Jülich Supercomputing Centre
52425 Jülich, ☎ (02461) 61-6402

Beratung und Betrieb, ☎ (02461) 61-6400

Technical Information

FZJ-JSC-TKI-0415

S. Linner, E.Grünter, M. Meier

31.01.2013

Rules of behavior for dealing with phishing

Introduction

„*Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.*“[1]

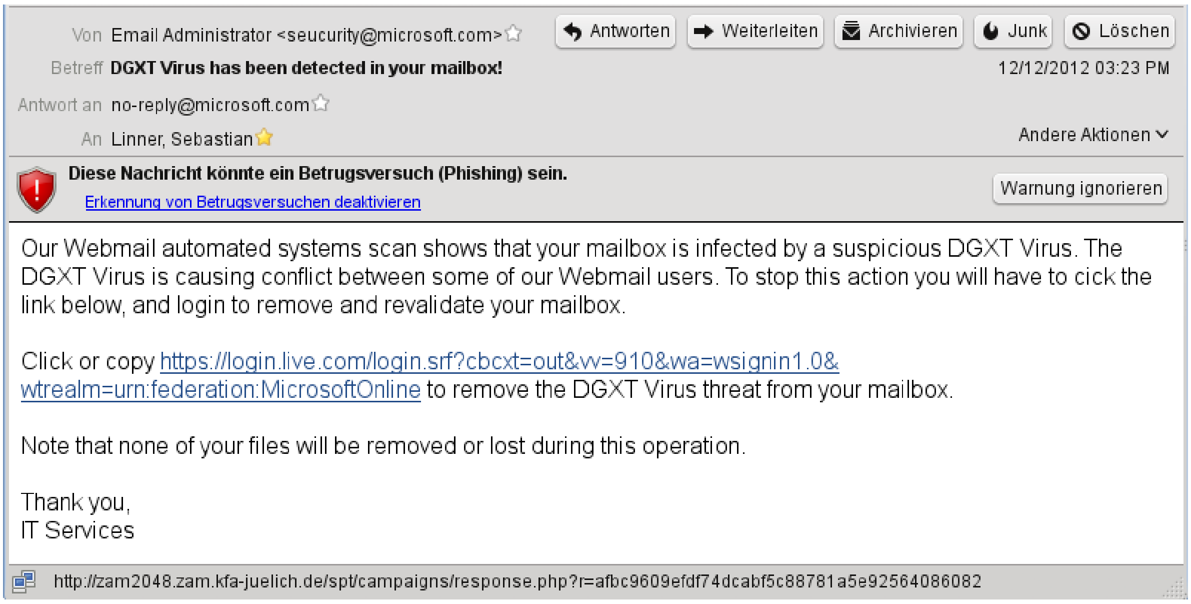
Phishing is a so called *portmanteau* and combines the two words *password* and *fishing*. The basis of a phishing-attack is often an e-mail that tries to lead the user to a website, which is used for identity theft. This can be done directly by a user's input or by malware, which is loaded on the system of the deluded user.

Since phishing attacks also pose a threat to the employees of the Forschungszentrum Jülich, this technical information is to identify characteristics of phishing e-mails and describe the proper handling of these e-mails.

[1] http://en.wikipedia.org/wiki/Phishing

Example of a phishing-mail

The following screenshot shows a typical phishing-mail.



Von Email Administrator <seucurity@microsoft.com>

Betreff **DGXT Virus has been detected in your mailbox!**

12/12/2012 03:23 PM

Antwort an no-reply@microsoft.com

An Linner, Sebastian

Diese Nachricht könnte ein Betrugsversuch (Phishing) sein.

Erkennung von Betrugsversuchen deaktivieren

Our Webmail automated systems scan shows that your mailbox is infected by a suspicious DGXT Virus. The DGXT Virus is causing conflict between some of our Webmail users. To stop this action you will have to cick the link below, and login to remove and revalidate your mailbox.

Click or copy https://login.live.com/login.srf?cbcxt=out&vv=910&wa=wsignin1.0&wtrealm=urn:federation:MicrosoftOnline to remove the DGXT Virus threat from your mailbox.

Note that none of your files will be removed or lost during this operation.

Thank you,
IT Services

http://zam2048.zam.kfa-juelich.de/spt/campaigns/response.php?r=afbc9609efdf74dcabf5c88781a5e92564086082

Characteristics of phishing

On the basis of the foregoing screenshot, one can distinguish the following characteristics:

1. The mail-client (here: Thunderbird) reports a potential fraud attempt.
2. The sender is faked or intentionally misspelled.
3. Phisher often try to hide the actual website by changing the link-text that is being displayed.
4. The e-mail is lacking a personal salutation.
5. The e-mail has not been digitally signed.
6. It is given a website, to be entered in user-name and password.
7. The actual website does not use a secured data transfer via HTTPS.

Rules of behavior

In order not to become victims of a phishing attack, please follow the listed guidelines:

1. Pay attention to correct spelling and grammar.
2. If you never had contact with the sender before, delete the e-mail.
3. Pay attention to the warnings of mail-clients (e.g. Thunderbird or Outlook).
4. Compare the link provided in the e-mail with the actual address of the web page by holding the mouse cursor over the link.
5. Pay attention to the digital signature of the e-mail. Service providers of the Forschungszentrum should generally sign their e-mails.
6. When the sender is trusted, but you have doubts about the content, let the sender verify the e-mail via another communication path.
7. Enter your personal information only on websites that use encrypted data transfer (HTTPS).
8. Report identified phishing-mails to the FZJ-CERT (cert@fz-juelich.de, 6440).
9. For questions, please contact the FZJ-CERT.