FORSCHUNGSZENTRUM JÜLICH GmbH

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

Beratung und Betrieb, ☎ (02461) 61-6400

Technische Kurzinformation

FZJ-JSC-TKI-0414
S. Linner, E.Grünter, M. Meier
31.01.2013

Verhaltensregeln zum Umgang mit Phishing

Einleitung

„*Unter Phishing werden Versuche verstanden, über gefälschte WWW-Adressen, E-Mail oder Kurznachrichten an Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen, um mit den erhaltenen Daten beispielsweise Kontoplünderung zu begehen und den entsprechenden Personen zu schaden.*“[1]

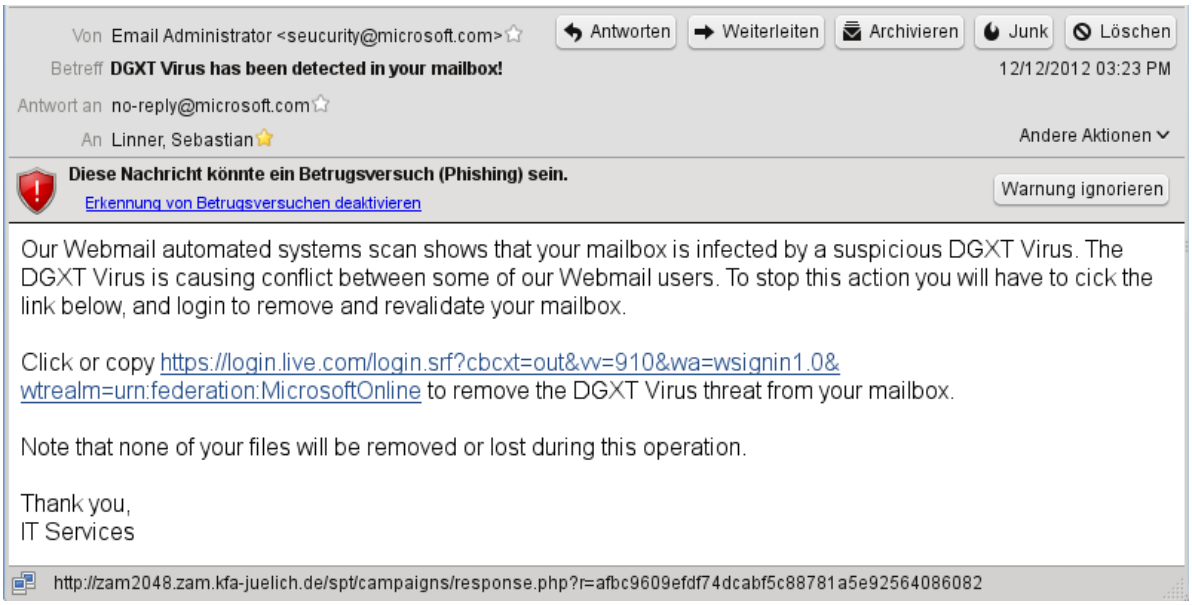
Der Begriff ist ein Kofferwort aus der englischen Sprache und setzt sich zusammen aus *Password* und *Fishing*. Ausgangspunkt eines Phishing-Angriffs ist oftmals eine E-Mail, die den Benutzer auf eine Web-Seite locken soll, die zum Identitätsdiebstahl genutzt wird. Das kann direkt durch die Eingabe eines Benutzers geschehen oder durch Schad-Software, die auf das System des getäuschten Benutzers geladen wird.

Da Phishing-Angriffe auch eine Bedrohung für die Mitarbeiter des Forschungszentrums Jülich darstellen, soll diese technische Kurzinformation Merkmale von Phishing-Mails aufzeigen und den richtigen Umgang mit diesen E-Mails beschreiben. Da insbesondere Nicht-Muttersprachler von schlechter deutscher Grammatik und Rechtschreibung getäuscht werden, steht diese TKI unter der Nummer FZJ-JSC-TKI-0415 auch in englischer Sprache zur Verfügung.

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

Beispiel einer Phishing-Mail

Der folgende Screenshot zeigt eine typische Phishing-Mail.



Merkmale von Phishing

Anhand des obigen Screenshots lassen sich folgende Merkmale erkennen:

1. Der Mail-Client (hier: Thunderbird) meldet einen potenziellen Betrugsversuch.
2. Der Absender ist oft gefälscht oder absichtlich falsch geschrieben.
3. Phisher versuchen oft durch einen anders angezeigten Link-Text die tatsächliche Adresse (unter der E-Mail erkennbar) zu vertuschen.
4. Es fehlt eine persönliche Anrede.
5. Die E-Mail ist nicht digital signiert.
6. Es wird eine Web-Seite angegeben, auf der Benutzername und Passwort eingegeben werden sollen.
7. Auf der tatsächlichen Web-Seite wird keine gesicherte Datenübertragung über HTTPS verwendet.

Verhaltensregeln

Damit Sie nicht Opfer eines Phishing-Angriffs werden, beherzigen Sie bitte die folgenden Verhaltensregeln:

1. Achten Sie auf korrekte Rechtschreibung und Grammatik.
2. Wenn Sie noch niemals Kontakt mit dem Absender der E-Mail hatten, löschen Sie diese.
3. Beachten Sie die Warnhinweise der Mail-Clients, z.B. Thunderbird o. Outlook.
4. Vergleichen Sie den angezeigten Link in der E-Mail mit der tatsächlichen Adresse der Web-Seite indem Sie den Mauszeiger über den Link halten.
5. Achten Sie auf die digitale Signatur der E-Mail. Dienstleister des Forschungszentrums sollten in der Regel ihre Mails digital signieren.
6. Sollte der Absender vertrauenswürdig sein, Sie aber Zweifel wegen des Inhaltes haben, fragen Sie über einen anderen Kommunikationsweg nach, z.B. telefonisch.
7. Geben Sie Ihre persönlichen Informationen nur auf Web-Seiten ein, die eine verschlüsselte Datenübertragung (HTTPS) nutzen.
8. Melden Sie identifizierte Phishing-Mails an das FZJ-CERT (cert@fz-juelich.de, 6440).
9. Bei Fragen wenden Sie sich an das FZJ-CERT.