Benutzerversammlung des CMS 20.3.2013

Phishing - kein Ende in Sicht

Burckhard Schmidt

postmaster@cms.hu-berlin.de

Phishing: Bitte antworten!

Date: Thu, 7 Mar 2013 17:31:05 +0700 (NOVT)

From: "WEB MASTER" <info@webmaster.com>

Subject: Aktualisieren Sie Ihr Konto

Reply-To: Webmaster@accountwebmaster.zzn.com

User-Agent: SquirrelMail/1.4.5

...

Bitte füllen Sie den Raum unten durch Eingabe

der wichtige Informationen zu Ihrem Kontingent zu erhöhen.

Benutzername: .....

Passwort: .....

Gegenwehr

- Reply-To- oder From-Adressen blockieren
- bei Beantwortung:
  - Benachrichtigung des Absenders (HU): „Fehler: Phishing-Verdacht“
- wirksam bei Versand via mailhost.cms.hu-berlin.de
- Auszug aus der Sperrliste (LDAP, ca. 180 Adressen):

  acc.upgrade@tech-center.com

  acc_services_all@admin.in.th

  account-admin@tmail.tv

  account-update@w.cn

  account-upgrade-unit@live.com

Bem.: E-Mail via google.com: kein Spam, via xy-Provider: Spam

Gegenwehr

- Betreff filtern auf typische Phrasen
- E-Mail an den Empfänger: Warnung: Phishing-Verdacht / warning: suspected phishing
  - Zweisprachige Erklärung
  - Original als Anhang
- Auszug aus der Sammlung (31 Phrasen):

  HelpDesk

  Der Zugriff auf Ihr Konto wurde

  URGENT NOTICE!

  Achtung: Ihr Account, Ihr Passwort

  WARNUNG (Kontingent überschritten)

Phishing: Bitte dem Link folgen!

- im Text oder auch im Anhang(!):
  - … kindly visit our admin loGon page HERE to submit your account details for authentication …

  Link dahinter:

  - href=3D"http://www.formpl.us/form/0B3ZNCYkZGKdTOEZMSXAyakgwVUE

Gegenwehr:

- Domain „erden“: nslookup www.formpl.us verweist auf phisher.cms.hu-berlin.de
  - Wettlauf mit der Zeit, jemand muss aktiv werden
  - hilft nur, wenn Nameserver des CMS benutzt werden
  - Seite als Betrugsversuch melden (Google)

Phishing: Bitte dem Link folgen!

- URL zu einem Formular bei docs.google.com
- Ist das ein guter oder ein böser Link?
  - https://docs.google.com/forms/d/1yyObMvp4nG1Iz5Er5CIqjrHUQl17I3sCvSuyPrBYj6k/viewform
- Phisher benutzen docs.google.com sehr gerne als Arbeitsmittel

Gegenwehr

- Filter mittels regulärem Ausdruck auf die E-Mail ansetzen
  - http oder https://docs.google.com und forms
- E-Mail an den Empfänger: Warnung: Phishing-Verdacht / warning: suspected phishing
  - zweisprachige Erklärung
  - Original als Anhang
- permanent aktiv

Nebenwirkungen

- „gute“ E-Mails mit einem Link auf Formular(e) bei docs.google.com werden auch als Phishing-Verdacht eingestuft
- E-Mails aus der HU mit einem entsprechendem Link (Umfrage, Anmeldung) werden zurückgewiesen.
- Umgehung: URL ohne https:// oder http:// angeben
- einen „URL Shortener“ verwenden (bitly)
- oder docs.google.com bestreiken
  - Heise am 19.02.2013 15:59:

    Do it yourself: Oxford blockiert Google Docs

Zusammenfassung

- E-Mail wird nicht als Spam erkannt
- E-Mail wird „klassisch“ als Spam erkannt und gekennzeichnet (X-Spam-Flag: YES, Ordner AutoClenSpam)
  - Haben Sie diesen Filter – wirksam bei Zustellung - aktiviert?
  - Einwilligung unter forward.cms.hu-berlin.de
- zusätzliche Filter
  - typische Formulierungen im Betreff
  - Link auf Formular-Webseiten in der E-Mail
  - Warnung des Empfängers, Original als Anhang
  - Der behördliche Datenschutzbeauftragte wurde informiert.