Schutzmöglichkeiten gegen Phishing

Klaus Plößl
Hannes Federrath
Thomas Nowey

Universität Regensburg

Gliederung

- Einführung
- Bekannte Gegenmaßnahmen
- Neuer Vorschlag
- Bewertung

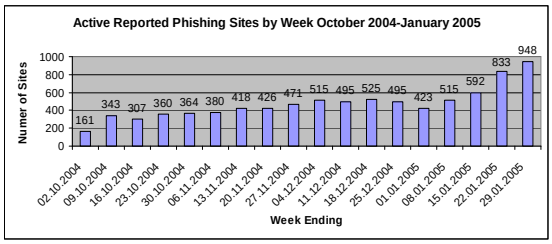
Phishing

"The hottest, and most troubling, new scam on the Internet"

Jana Monroe, Assistant Director der FBI Cyber Division 2003

- Benutzt Methoden des Social Engineering
  - Angriffszenario:
    - Professionell gestaltete E-Mail mit gefälschtem Absender
    - Opfer wird überzeugt seine persönlichen Daten auf einer gefälschten Webseite einzugeben
- Kunstwort aus "Password" und "Fishing"
- Anti-Phishing Working Group (APWG)

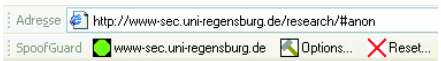
Ausmaß der Bedrohung



- Zahl der Vorfälle steigt stark an
- Schaden von 1,2 Milliarden US-Dollar im Jahr 2003 (Gartner)

Bekannte Gegenmaßnahmen

- Grundsätzliche Ansätze:
  - Minderung des Risikos ohne Verfahrensänderung
    - Nutzerabhängig
      - Schulung der Nutzer, "Leitfäden"
      - Spam-Filter und Filter für ausgehende Daten
      - Browser-Plug-ins



Bekannte Gegenmaßnahmen

- Grundsätzliche Ansätze:
  - Minderung des Risikos ohne Verfahrensänderung
    - Nutzerabhängig
    - Nutzerunabhängig
      - Spam-Trap und Domain-Watch
      - Validierung von Absenderdaten
      - Fraud Detection
      - SANS Internet Storm Center:
        "6 Simple Steps to Beat Phishing"

Bekannte Gegenmaßnahmen

- Grundsätzliche Ansätze:
  - Minderung des Risikos ohne Verfahrensänderung
    - Nutzerabhängig
    - Nutzerunabhängig
  - Änderung des Authentifizierungsverfahrens
    - Hardware-Token
      - Periodisch wechselndes Einmalpasswort
      - Einmalpasswort auf Anforderung
      - Challenge-Response-System
    - Kombination aus Hardware-Token und Browser-Plug-in
    - PKI und Digitale Signatur

Sicher, aber aufwändig, teuer…

Neuer Lösungsvorschlag

- Prinzip:
  - Verknüpfung des PIN/TAN-Verfahrens mit einem papierbasierten Challenge-Response-Verfahren
- Vorgehen:
  - Nutzer erhält Liste mit Challenge-Response-Paaren

Challenge	Response
0374902736	6475823653
1938874629	9928376348
2837492039	2435167989
3459384027	3526778983
4736483729	6573822827
6372891110	8495726334
8364456373	5534251164
8374658902	1727836272
…	…

Neuer Lösungsvorschlag

- Prinzip:
  - Verknüpfung des PIN/TAN-Verfahrens mit einem papierbasierten Challenge-Response-Verfahren
- Vorgehen:
  - Nutzer erhält Liste mit Challenge-Response-Paaren
  - Bei Anmeldung bzw. vor Abschluss einer Transaktion: Anzeigen einer Challenge der Liste

Bitte geben Sie die zur Challenge
6372891110
gehörende Response ein:
[ ]

  - Anmeldung bzw. Durchführung der Transaktion nur bei richtiger Response

Neuer Lösungsvorschlag

- Nebenbedingungen:
  - Jede Challenge wird maximal einmal verwendet
  - Nutzer bekommt neue Liste, wenn die Challenges aufgebraucht sind
  - Sperrung des Accounts und Benachrichtigung des Nutzers nach einer bestimmten Anzahl von Fehlversuchen
  - Begrenzung der Gültigkeit der Challenge
- Usability:
  - Challenge als Zahl, Response als Buchstabenfolge
  - Challenges aufsteigend geordnet
  - Für den Nutzer ähnlich zur TAN-Liste

Challenge	Response
0374902736	ZSJUFS
1938874629	HAGTUH
~~2837492039~~	~~BSUNBI~~
3459384027	XNAJSK
~~4736483729~~	~~OKALSZ~~
6372891110	WQNNIV
8364456373	HEUCNP
8374658902	AFSOPN
…	…

Bewertung

- Schutz vor Phishing mit Passwort und PIN/TAN-Verfahren nicht möglich
- Alternativen (1/2):
  - Einsatz digitaler Signaturen
    - Sicherheitstechnisch beste Lösung
    - Nachteil: sehr hohe Kosten für zusätzliche Hardware, Benutzerschulungen, Support, Betrieb der PKI…
  - Hardware-Token mit zeitlich begrenzten Einmal-Passwörtern
    - Schützt relativ zuverlässig vor Phishing
    - Nachteil: hohe Kosten für zusätzliche Hardware, Benutzerschulungen

Bewertung

- Alternativen (2/2):
  - Neu vorgeschlagenes Verfahren
    - Schützt annähernd so zuverlässig wie Hardware-Token
    - Vorteil: nahezu keine zusätzlichen Kosten für Betreiber
    - Guter Kompromiss, bis digitale Signatur flächendeckend verfügbar
- Weitere Informationen:
  - www-sec.uni-regensburg.de/phishing
  - www.antiphishing.org
- Kontakt:

Klaus.Ploessl@wiwi.uni-regensburg.de