

Sampo pankin sivut avoinna kalastelijoille

26.3.2008 12:57 — Timo Poropudas
timo.poropudas@sanoma.fi

Sampo pankin tietotekniikan siirtäminen Danske Bankin ympäristöön on osoittautunut vaikeaksi harjoitukseksi. Nyt sähköposteissa kiertää viesti, joka näyttää miten verkkosivu on haavoittuvainen muutoksille ilman että käyttäjä tietää siitä.

Palvelimen *verkkopankki.sampopankki.fi*:n järjestelmä sallii käyttäjän lähettää sivulle url-pyyntöjä joissa on mukana javascript-koodia. Tuo koodi päättyy suoritettavaksi sivun kontekstissa.

Sähköpostissa kiertävä ajettava koodi on "alert('fail')", joka tulostaa varoitusikkunan.

Asiantuntijan mukaan [cross-site scripting](#) koodi voisi tehdä paljon muutakin, melkein mitä tahansa.

- Se voisi ladata näytölle phishing-sivuston, joka kyselisi käyttäjän luottokortin numeroa ja lähettäisi sen vorolle.

Tilanteessa on erittäin ongelmallista se, että käyttäjälle se näyttäisi ssl-suojatulta sivulta, jonka verkko-osoite eli url alkaisi "verkkopankki.sampopankki.fi". Käyttäjälle sivu siis näyttäisi luotetulta.

<http://www.digitoday.fi/tietoturva/2008/03/26/sampo-pankin-sivut-avoinna-kalastelijoille/20088576/66>