COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/googles-safe-browsing-laesst-sich-von-tinyurl-taeuschen,1885649

Ausgehebelt

Googles Safe Browsing lässt sich von TinyURL täuschen

Datum: 30.01.2009
Autor(en): Uli Ries

Googles Safe Browsing soll Nutzer von Google Chrome und Mozilla Firefox vor dem Besuch von Phishing-Sites bewahren. IT-Sicherheitsexperten haben jedoch heraus gefunden, dass sich die Schutzfunktion durch einen simplen Trick umgehen lässt. Als alleiniger Phishing-Schutz ist Safe Browsing daher nicht zu empfehlen.

Plakativ: Googles Safe Browsing warnt den Web-Surfer vor potentiell gefährlichen Websites.

Wie die IT-Sicherheitsfachleute von Finjan in ihrem **Blog**[1] schreiben, lässt sich **Googles Safe Browsing**[2] durch einen simplen Trick übertölpeln: Der **Phishing**[3]-Schutz läuft ins Leere, wenn die Phisher ihre Website hinter einem Domain-Umleitungs-Dienst wie **TinyURL**[4] verstecken.
Dienste wie TinyURL, **bit.ly**[5] oder **w3t.org**[6] werden meist zum Abkürzen von ausufernd langen Internetadressen genutzt. Dies ist insbesondere beim Einfügen der Links in E-Mails nützlich. Extrem beliebt ist insbesondere TinyURL auch bei Nutzern der **Web-2.0**[7]-Seiten **Twitter**[8] und **Facebook**[9]. Da auf diese Seiten auch von Clients aus Unternehmensnetzwerken zugegriffen wird, schwappt die **Phishing**[10]-Gefahr hinter die **Firmenfirewall**[11].

Googles Safe Browsing ist fester Bestandteil von **Google Chrome**[12] und der **Google-Toolbar für Firefox**[13]. An sich soll die Funktion verhindern, dass unbedarfte Anwender durch den Klick auf einen bösartigen Web-Link auf eine Phishing-Site gelotst werden. Anstatt die Seite darzustellen, präsentieren die **Browser**[14] eine prominente Warnmeldung. Den Finjan-Mitarbeitern ist es jedoch gelungen, den Phishing-Schutz zu umgehen, indem sie einfach per TinyURL eine neue Webadresse der Phishing-Site erzeugten.

Wie die Experten weiter schreiben, kann **Google**[15] die Gefahr offenbar nicht erkennen, da die Top-Level-Domain **tinyurl.com**[16] für sich genommen ungefährlich ist. Und auch zehntausende andere Domain-Namen, die per TinyURL erzeugt wurden, sind keine Bedrohung. Daher tut sich der Phishing-Filter schwer, gut von böse zu unterscheiden. Finjan rät daher dazu, neben Safe Browsing noch auf weitere Web-Sicherheitsprodukte zu setzen, die Phishing-Sites durch andere Mechanismen erkennen.

Finjan hat nach eigener Auskunft TinyURL bereits über die entdeckten Redirects auf bösartige Site informiert, so dass diese entfernt wurden. Keine Gefahr droht auch durch seit längerem bekannte Phishing-Seiten, da Safe Browsing vor diesen trotz URL-Verschleierung warnt.

Links im Artikel:

1 **http://www.finjan.com/MCRCblog.aspx?EntryId=2153**
2 **http://www.google.com/tools/firefox/safebrowsing/**
3 **https://www.computerwoche.de/knowledge_center/security/1883917/**
4 **http://www.tinyurl.com/**
5 **http://bit.ly/**
6 **http://w3t.org/**
7 **https://www.computerwoche.de/knowledge_center/security/1883917/**
8 **http://www.twitter.com/**
9 **http://www.facebook.de/**
10 **http://de.wikipedia.org/wiki/Phishing**
11 **https://www.computerwoche.de/job_karriere/freiberufler/1877271/**
12 **http://www.google.com/chrome**
13 **http://www.google.com/tools/firefox/toolbar/FT2/intl/de/**
14 **https://www.computerwoche.de/knowledge_center/security/1874700/**
15 **https://www.computerwoche.de/schwerpunkt/g/Google.html**
16 **http://tinyurl.com/**
