Un(der)cover

Jens Liebchen, Patrick Hof - RedTeam Pentesting GmbH
jens.liebchen@redteam-pentesting.de
patrick.hof@redteam-pentesting.de
http://www.redteam-pentesting.de

Netzwerk Recherche
09./10. Juli 2010, NDR Hamburg

RedTeam Pentesting, Daten & Fakten

- ★ Gegründet 2004 in Aachen
- ★ Spezialisierung ausschließlich auf Penetrationstests
- ★ Weltweite Durchführung von Penetrationstests
- ★ Forschung im Bereich der IT-Sicherheit

Über den Vortrag

- ★ Von der einfachen Online-Recherche hin zur *gezielten Generierung* neuer Informationsflüsse
- ★ Anregung zum selber denken und kreativ sein
- ★ Seien Sie interaktiv ⇒ Workshop

Rechtliches

- ★ Recherche ⇔ Ausspähung
- ★ Zivilrechtliche Konsequenzen
- ★ Strafrechtliche Konsequenzen
  - §202a Ausspähen von Daten
  - §202b Abfangen von Daten
  - §202c Vorbereiten des Ausspähens und Abfangens von Daten

Zweigeteilte Sichtweise

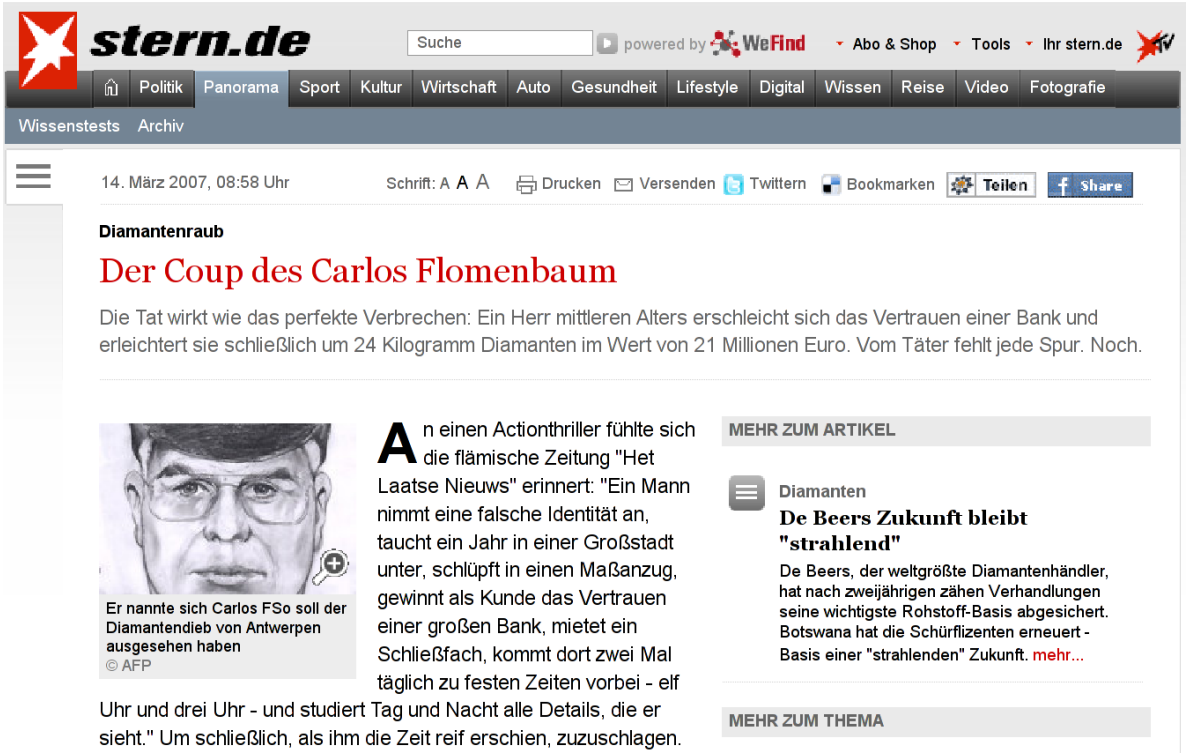
- ★ Journalist ⇔ Gegenseite
- ★ Journalist: Will Sachverhalte aufdecken, Informationen beschaffen
- ★ Gegenseite: Will Informationen unterschieben, manipulieren, ausspähen
- ★ Teilweise gleiche Techniken → Gegenseite hat evtl. weniger ethische Bedenken

Social Engineering - Definition

„Social engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. “

(Kevin D. Mitnick)

Social Engineering



stern.de

Suche | powered by WeFind | Abo & Shop | Tools | Ihr stern.de

Politik | Panorama | Sport | Kultur | Wirtschaft | Auto | Gesundheit | Lifestyle | Digital | Wissen | Reise | Video | Fotografie

Wissenstests | Archiv

14. März 2007, 08:58 Uhr Schrift: A A A Drucken | Versenden | Twittern | Bookmarken | Teilen | Share

Diamantenraub

Der Coup des Carlos Flomenbaum

Die Tat wirkt wie das perfekte Verbrechen: Ein Herr mittleren Alters erschleicht sich das Vertrauen einer Bank und erleichtert sie schließlich um 24 Kilogramm Diamanten im Wert von 21 Millionen Euro. Vom Täter fehlt jede Spur. Noch.

Er nannte sich Carlos FSo soll der Diamantendieb von Antwerpen ausgesehen haben
© AFP

An einen Actionthriller fühlte sich die flämische Zeitung "Het Laatse Nieuws" erinnert: "Ein Mann nimmt eine falsche Identität an, taucht ein Jahr in einer Großstadt unter, schlüpft in einen Maßanzug, gewinnt als Kunde das Vertrauen einer großen Bank, mietet ein Schließfach, kommt dort zwei Mal täglich zu festen Zeiten vorbei - elf Uhr und drei Uhr - und studiert Tag und Nacht alle Details, die er sieht." Um schließlich, als ihm die Zeit reif erschien, zuzuschlagen.

MEHR ZUM ARTIKEL

Diamanten
De Beers Zukunft bleibt "strahlend"
De Beers, der weltgrößte Diamantenhändler, hat nach zweijährigen zähen Verhandlungen seine wichtigste Rohstoff-Basis abgesichert. Botswana hat die Schürflizenten erneuert - Basis einer "strahlenden" Zukunft. mehr...

MEHR ZUM THEMA

Social Engineering

Pressemitteilung des Ministeriums für Wirtschaft und Aussenhandel

Ein Grossteil der Luxemburger gibt ohne Bedenken persönliche Daten preis

Die Gefahr eines Diebstahls persönlicher Daten im Internet ist allseits bekannt. Doch wie reagieren Personen in Luxemburg, die von Unbekannten, also potentiellen Cyberkriminellen, persönlich angesprochen werden? Fast jede fünfte Person gibt bereitwillig ihr Passwort preis. Lockt eine Tafel Schokolade zur Belohnung, so ist sogar jeder Vierte bereit, sein Passwort einem Fremden anzuvertrauen. Insgesamt geben zwei von drei Personen bereitwillig indirekte Hinweise zu ihrem Passwort. Dies ist das Ergebnis eines nachgestellten Social Engineering Angriffs vom Oktober 2008.

[...]

Obwohl die Opfer zu Beginn des gestellten Angriffs darauf aufmerksam gemacht wurden, dass sie an einer anonymen Umfrage teilnehmen, haben 89,1% ihr Geburtsdatum, 79,5% ihren Namen und 57,8% ihre Telefonnummer angegeben.

Faktor Mensch

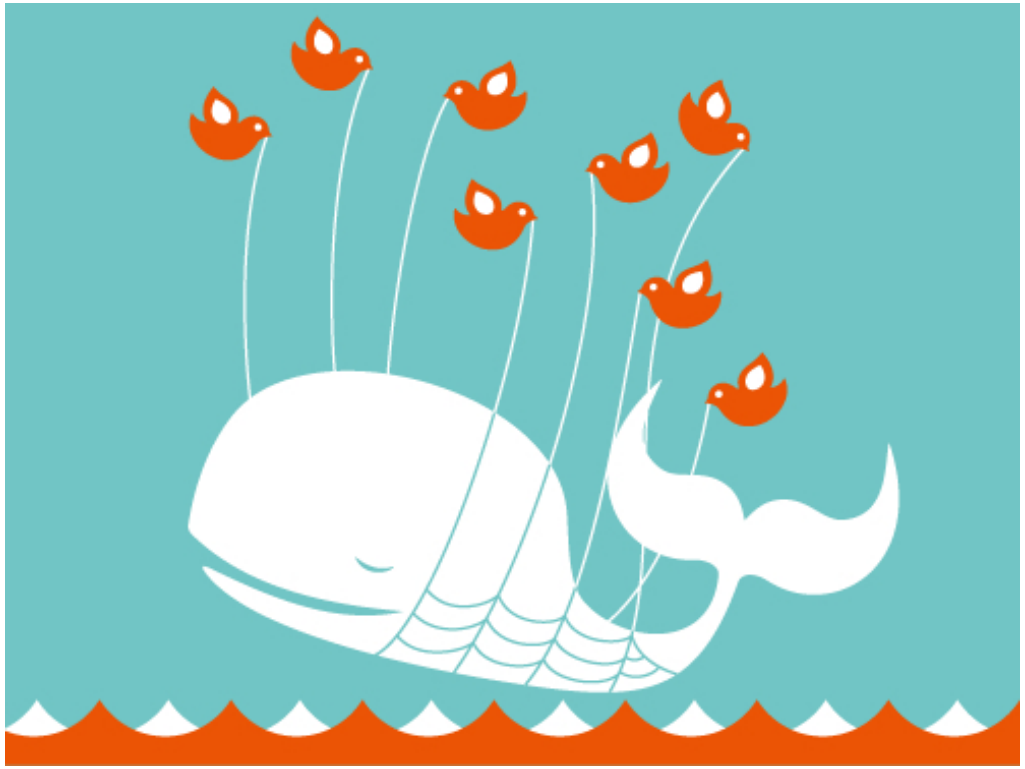
Warum sind Social Engineering-Attacken erfolgreich?

- ★ sensitive Informationen oft nicht intuitiv als solche erkennbar
- ★ spontane Einschätzung von Risiken schwierig
- ★ Stress (evtl. gezielt aufgebaut)
- ★ (anerzogene) Hilfsbereitschaft
- ★ Macht der Gewohnheit
- ★ Egoismus / Egozentrik bei jedem vorhanden

Spezialfall: Reverse Social Engineering

- ★ Social Engineering: Der Angreifer kontaktiert das Opfer
- ★ Reverse Social Engineering: Das Opfer kontaktiert „freiwillig“ den Angreifer

Twitter: Exkursion zum Fail Whale



Twittermeldungen

- ca. 190 Mio. Besucher auf twitter.com am Tag[1]
- Es gibt nichts, was nicht „getwittert“ wird
- Viele kleine Informationsschnipsel, welche sich zu einem Gesamtbild zusammensetzen und/oder als Hintergrundinformationen nutzen lassen

[1] http://techcrunch.com/2010/06/08/twitter-190-million-users/

Twitter ist schneller: Kobil-Hack

April/17/2010

- Der zertifizierte Klasse 3 Smartcard-Reader Kaan Tribank von Kobil wurde geknackt. (Smartcard-Reader-Hack Sektion)

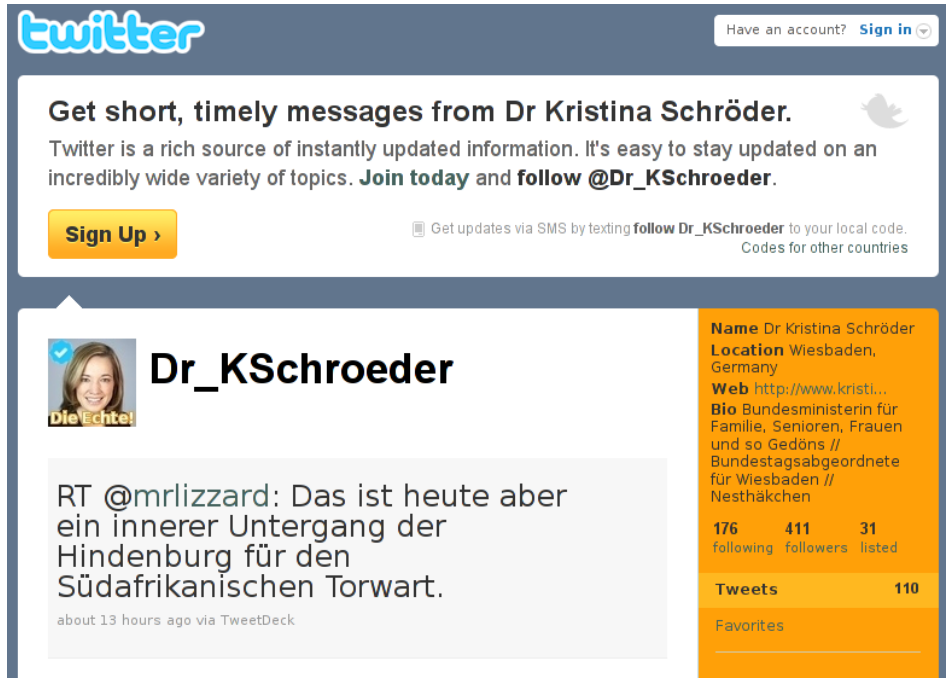
Mar/10/2010

- Kryptoanalyse PowerVu TV-Verschluesselung (PowerVu Sektion)

http://colibri-dvb.info

Twitter ist schneller: Kobil-Hack

Gefälschte Accounts



URL Shortener

Zi.ma
Life Is Short, So Are Your URLs

TiNY where big things fit in tiny packages.

Google url shortener

Compress That Address!
is.gd

TinyURL.com

bit.ly Shorten, share, and track your links

Risiken und Möglichkeiten

Risiken:

- ★ Es ist unklar, was sich hinter den Links verbirgt
  $\Rightarrow$ Malware, illegale Inhalte, Angriffe auf Dritte...
- ★ Menschen sind neugierig und klicken auf fast alles

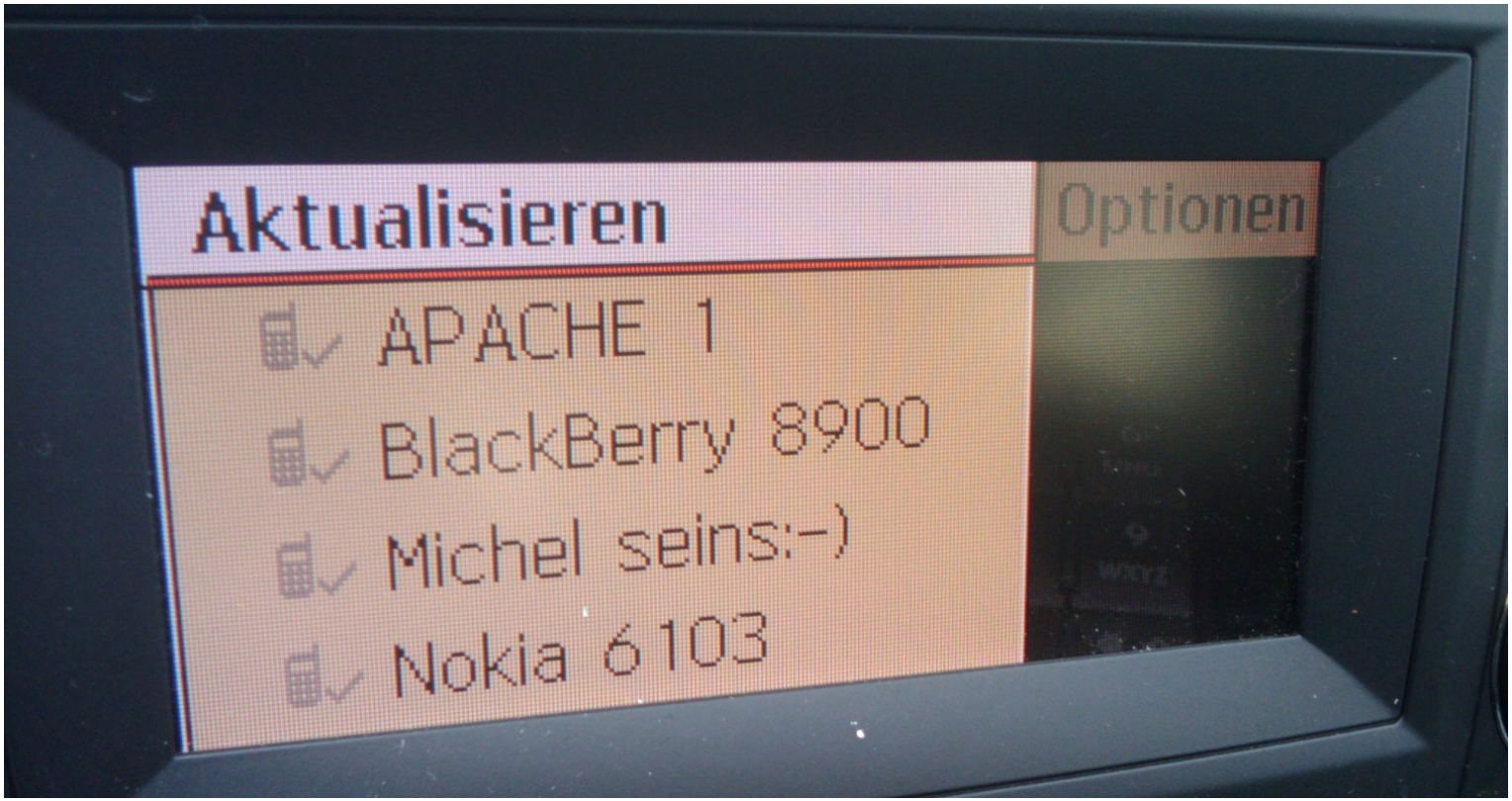
Möglichkeiten:

- ★ Erstellen von Statistiken $\Rightarrow$ z.B. für Recherche

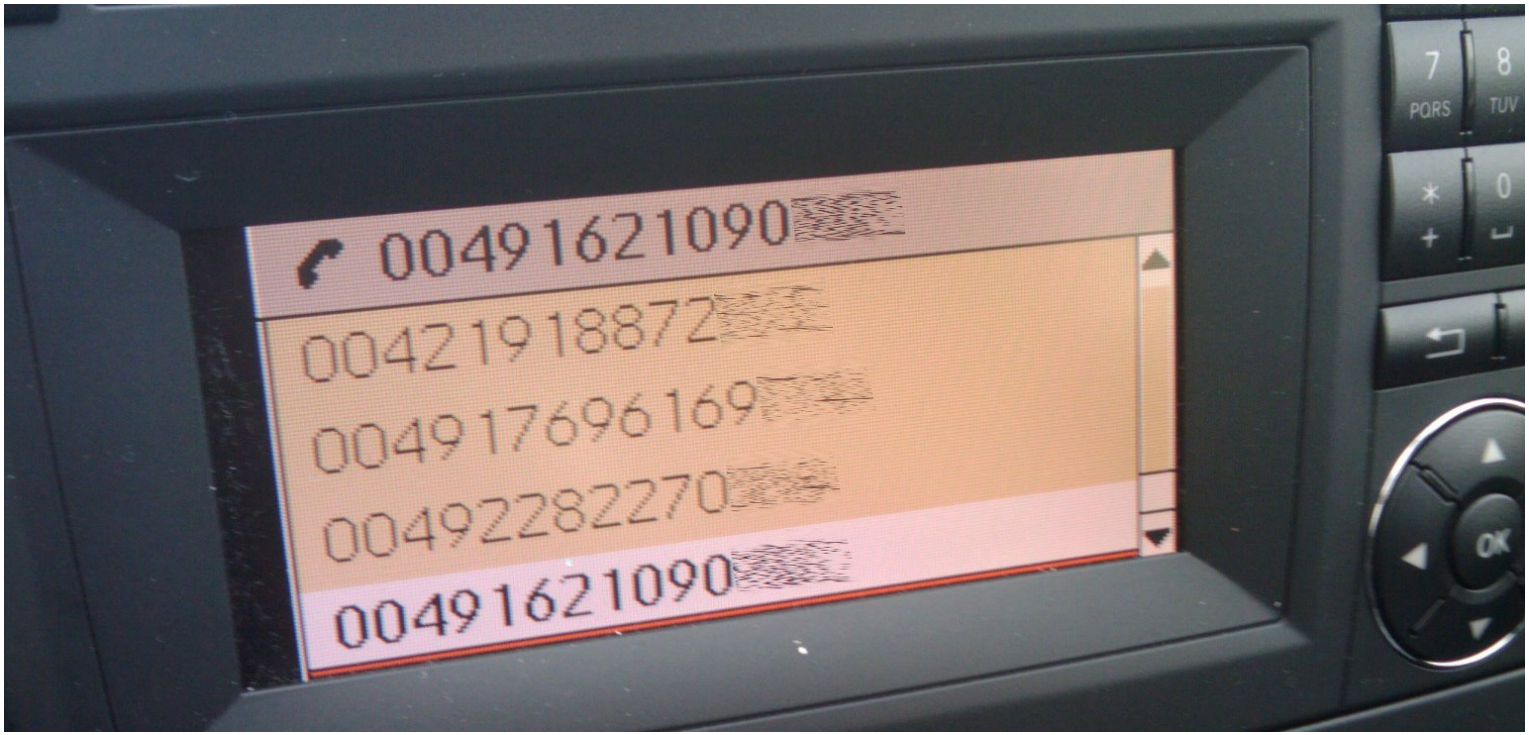
Mietwagen: Navigationsgeräte

Mietwagen: Telefone

Mietwagen: Telefone



Mietwagen: Telefone



Hotel-WLAN


Willkommen im Hotel-WLAN
Bitte geben Sie Ihre Nachnamen als Name und Ihre Zimmernummer als Passwort ein:
Name:
Passwort:

Telefone


SIEMENS
Wahlwiederholung
Nr.1: 02419631300?
Laut
Leise
Mikro aus
Tel.buch
Wahlwdh.
Rückfrage
Lautspr.

Manchmal geht es noch einfacher. . .

Manchmal geht es noch einfacher. . .

Datenspuren: Fazit

- ★ Man hinterlässt überall Datenspuren
- ★ Nutzen Sie die Datenspuren anderer für Ihre Recherche
- ★ Benutzung öffentlicher / verteilter Ressourcen (Hotels, Mietwagen etc.) birgt Risiken und kann ungünstig für Vertrauliches sein
- ★ Achten Sie darauf, welche Datenspuren Sie hinterlassen (Quellenschutz)

Web-Bugging

- ★ Einfügen von (versteckten) Bildern in Nachrichten
- ★ Problem: E-Mail-Programme laden heute meist keine externen Bilder mehr nach
- ★ Stattdessen: URL Shortener-Dienste mit Zugriffsstatistiken
  ⇒ IP-Adressen, Zugriffszeiten, Referrer...
- ★ Aufdecken von Beziehungen zwischen Quellen
  ⇒ Link an eine einzige Quelle weitergeben – greift noch jemand Drittes darauf zu?

Gezielte Streuung von Informationen

Streuung von Informationen erzeugt neue Informationen

- ★ Eigene Webseite, Foren, Social Networks
- ★ USB-Sticks, CDs, Notizen liegen lassen
- ★ Gezielte Anfragen
- ★ Vorgeben, mehr (oder auch weniger) zu wissen, als man eigentlich weiß

Wie kommt ein Angreifer an unsere Daten?

- ★ Sicherheit muss ein Gesamtkonzept sein, denn ein Angreifer sucht sich die schwächste Stelle
- ★ Im Folgenden einige Beispiele...

Emails und andere Accounts...

- ★ Passwörter werden vergessen ⇒ Geheime Fragen
- ★ „Wie ist der Vorname ihrer Oma?“
- ★ „Wie heißt ihr Haustier?“
- ★ „Was ist ihre Lieblingsfarbe?“

⇒ Sicherheitstechnisch katastrophal, wer die Antwort kennt, hat Zugriff auf den Account

Emails und andere Accounts...

„Where did you meet your spouse?“

Emails und andere Accounts...

TIME
IN PARTNERSHIP WITH CNN

SEARCH TIME.COM

Politics

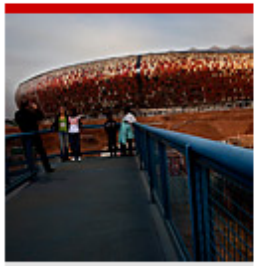
Main • Ted Kennedy 1932-2009 • The Page • Swampland • White House

VIRAL THING

Sarah Palin's E-Mail Hacked

By **M.J. STEPHEY** Wednesday, Sep. 17, 2008

More on TIME.com



World Cup 2010

Republican vice-presidential candidate Sarah Palin speaks at a campaign rally on Sept.13 in Nevada
Max Whittaker / Getty Images

Mobile Telefone. . .

- ★ Ankommende Telefongespräche abfangen
- ★ Onlinebanking! (mTAN)
- ★ Was hindert einen Angreifer daran, eine fremde Telefonnummer zu portieren?

Mobile Telefone. . .

- ★ Ankommende Telefongespräche abfangen
- ★ Onlinebanking! (mTAN)
- ★ Was hindert einen Angreifer daran, eine fremde Telefonnummer zu portieren?

Mobile Telefone. . .

iX > News > 2009 > KW 42 > mTAN in Australien ausgehebelt

14.10.2009 14:09

« Vorige | Nächste »

mTAN in Australien ausgehebelt

vorlesen / MP3-Download

Das auch hierzulande von vielen Banken genutzte mTAN-Verfahren haben sich Betrüger in Australien zunutze gemacht, um ein fremdes Konto abzuräumen. Paul Ducklin von der Sicherheitsfirma Sophos berichtet in seinem Blog vom Auftritt eines Geschädigten namens Dimitri auf einer Konferenz im australischen Bundesstaat Queensland.

Unbekannte hätten dessen Mobilnummer zu einem anderen Betreiber portieren lassen. Dieser konnte dann Transaktionen mit Dimitris Bankkonto ausführen, da er automatisch die von der Bank zur Bestätigung der Aufträge per SMS versandten mTANs erhielt.

Der Vorfall selbst liegt wohl schon einige Zeit zurück, denn der australische Fernsehsender ABC berichtete bereits im August darüber (Abschrift , die 45-minütige Sendung gibt es als Flash-Movie). Dort heißt es, dass Dimitri Glianos zunächst von seiner Bank von ungewöhnlichen Kreditkartentransaktionen erfuhr. Daraufhin stellte sich die Portierung der Mobilnummer heraus, die sich nicht sofort rückgängig machen ließ. Schließlich verschwanden über 80.000 australische Dollar (circa 50.000 Euro) von seinem Bankkonto, die die Bank jedoch ersetzte.

Per Phishing-Mail hatte sich der Angreifer die für den Betrug nötigen persönlichen Daten samt der Mobilnummer verschafft. Ihre Portierung verlief problemlos, da der neue Provider die Identität des Kunden nicht prüfte. (ck)

MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

Einloggen | Ausloggen

Suche

los

News

- 7-Tage-News
- News-Archiv
- News mobil

Heft

- Inhalt 07/2010
- Mailingliste
- Archiv/Suche

Amtliche Dokumente...

- ★ Ausweise
- ★ Geburtsurkunden
- ★ ePass auf fremden Namen aber mit den eigenen Fingerabdrücken?
- ★ ...

Was wäre wenn. . .

. . . jemand Interesse an *Ihren* Daten hätte?

$\Rightarrow$ Demo

Was bedeutet Kompromittierung?

- Der Rechner ist unter der vollständigen Kontrolle des Angreifers
- Der Angreifer kann...
  - alles was Sie sehen vorgeben
  - alles was Sie machen einsehen
  - alle Daten auf dem Rechner einsehen und manipulieren
- Was im Hintergrund passiert, wissen Sie nicht

Was tun nach einer Kompromittierung?

Was nicht hilft:

- ★ Virenscanner
- ★ Personal Firewalls
- ★ Den Sohn des Nachbarn fragen, ob er das beheben kann

Stattdessen:

- ★ Rechner komplett neu installieren
- ★ Genau überlegen, welche (Backup-) Daten auf das neue System übernommen werden

Fazit

- ★ Der Übergang zwischen Recherche und Ausspähen ist fließend
- ★ Scheinbare Anonymität des Netzes sowie die Einfachheit der Informationsbeschaffung / -generierung können dazu führen, dass Legalität und Ethik nicht bedacht werden
- ★ Trotzdem: Nutzen Sie die Chancen!

Fragen?

Vielen Dank für Ihre Aufmerksamkeit

—

Freie Diskussion

Linksammlung

- http://www.social-engineer.org
- http://www.tweetmeme.com
- http://www.tweepsearch.com
- http://www.tweetstats.com
- http://www.xefer.com/twitter
- http://apps.asterisq.com/mentionmap
- http://www.blippy.com
- http://www.paterva.com
- http://bit.ly
- http://zi.ma
- http://nvg8.it