heise Security

News-Meldung vom 18.05.2009 14:10

BKA: iTAN-Verfahren keine Hürde mehr für Kriminelle

Das iTAN-Verfahren stellt für Kriminelle kein Problem mehr dar, erklärte Mirko Manske, Kriminalhauptkommissar im Bundeskriminalamt (BKA) auf dem **11. IT-Sicherheitskongress[1]** des **Bundesamts für Sicherheit in der Informationstechnik[2]** in Bonn. Die indizierten Transaktionsnummern waren eingeführt worden, nachdem sich das herkömmliche TAN-System gegenüber Phishing-Attacken als zu unsicher gezeigt hatte. Zwar seien Phishing-Angriffe mit iTAN schwieriger geworden, so Manske "aber nicht unmöglich".

Bei indizierten TANs fragt die Bank statt nach einer beliebigen TAN auf der Liste nach einer bestimmten TAN, beispielsweise der dreiundzwanzigsten. Allerdings ist für den Kunden nicht vorhersehbar, welche iTAN abgefragt wird. Zudem ist eine iTAN immer an eine bestimmte Transaktion gebunden. Auch wenn die Verbindung unterbrochen wird, kann der Auftrag nur mit dieser TAN zu Ende geführt werden.

Bereits Ende 2005 hatte eine Arbeitsgruppe der Ruhr-Universität Bochum einen Angriff auf das Online-Banking-Verfahren mit indizierten TANs erfolgreich demonstriert. Anfang 2007 tauchten dann erste **Phishing-Kits[3]** auf, die in der Lage waren, per Man-in-the-Middle-Attacke abgephishte iTANs in Echtzeit für eigene Transaktionen zu benutzen. Auch heise Security erreichen immer öfter Meldungen von Lesern über Phishing-Angriffe, die trotz iTAN-Verfahren erfolgreich waren.

Das BKA habe im Jahr 2008 rund 1.800 erfolgreiche Phishing-Aktionen registriert, berichtete Manske. Typischerweise werden diese heute über Trojaner eingefädelt. Ein in einem vorgeblichen PDF-Anhang verstecktes Schadprogramm niste sich auf den Rechner ein, um bei der nächsten Online-Überweisung einen anderen Betrag an einen anderen Empfänger zu überweisen. Der Schaden sei erst über den Kontoauszug bemerkbar.

Sogenannte Finanzagenten ("Money mules"), die bei herkömmlichen Phishing-Aktionen ihre Privatkonten für den Geldtransfer gegen eine Provision zur Verfügung gestellt haben, kämen hingegen kaum noch zum Einsatz. Dies führte Manske auf die Aufklärung seitens der Medien und des Bundeskriminalamts zurück, die die Folgen für die Finanzagenten geschildert hatten: So flogen die Finanzagenten binnen kürzester Zeit auf, ihre Bank kündigte ihr Konto, und eine neue Hausbank zu finden, stellte sich als schwierig heraus. Auf die veränderte Lage habe sich die organisierte Kriminalität binnen drei Monaten mit neuen Social-Engineering-Methoden eingestellt, sagte Manske: "Sie zielen darauf ab Finanzagenten zu finden, die nicht wissen, dass sie überhaupt Finanzagenten sind." Der Rekrutierungsprozess sei damit erheblich aufwendiger geworden und könne sich über mehrere Wochen hinziehen.

Manske schilderte den "typischen" Fall eines geschiedenen 50-jährigen Mannes, der über ein Online-Datingcafé eine E-Mail von einer "Jekaterina" erhalten hatte. Nach gegenseitigen Sympathiebekundungen, die sich über etwa zwei Wochen hinzogen, habe die Frau erklärt, sie wolle gerne nach Deutschland kommen, hätte aber kein Geld zur Verfügung. Gleichwohl habe sie aus einem früheren Aufenthalt in Deutschland Erspartes zurückgelegt. Dieses könne man ihr jedoch nicht direkt überweisen, ohne dass sie Probleme mit den russischen Steuerbehörden bekomme, da sie das Geld aus Schwarzarbeit bezogen habe. Der Mann könne ihr aber das Geld in einer deutschen Filiale der Western Union einzahlen. Dafür müsse er seine Kontodaten zur Verfügung stellen.

Der 50-Jährige nahm ihr die Geschichte ab und stellte seine Kontoverbindungsdaten zur Verfügung. Als "Belohnung" erhielt er daraufhin ein Bild von ihr. Auch auf der russischen Seite wurde ein "Geldesel" organisiert. Jekaterina erklärte, dass ihre "Mutter" das Geld entgegennehmen werde. Dies hätte jedoch einen anderen Nachnamen, da sie wieder geheiratet habe. Der Mann glaubte ihr und zahlte das Geld bei Western Union ein. Nach dem erfolgreichen Transfer nahm Jekaterina erneut Kontakt mit ihm auf, um erneut ein Bild von sich zu schicken, aber auch einen zweiten Transfer

einzufädeln. Begründung: Der erste Transfer habe nicht funktioniert. Doch dazu sollte es nicht mehr kommen. Die Hausbank des Mannes hatte eine Anzeige der von einem Phishing-Angriff betroffenen Bank erhalten. Sie erstattete gegen ihn wegen Geldwäsche Anzeige und schloss sein Konto.

Manske schilderte außerdem die Szene der Online-Kriminalität als hochgradig arbeitsteilig organisiert: Kriminelle könnten die Hehlerei mit geklauter Ware über das Internet mit verschiedenen falschen Identitäten nahtlos über verschiedene Mittelsmänner, die sich über ICQ-Nummer kennen, abwickeln. So seien einige Kriminelle darauf spezialisiert, über bekannt gewordene Schwachstellen oder unzureichende Betrugssicherungsmechanismen in Webshop-Systemen Kundendaten mit Kreditkartendaten abzuziehen. Manske: "Reseller bestellen feste Kreditkarten-Kontingente gegen Vorkasse, die von den Hackern mit einer 3-Monats-Garantie für ihre Frischegüte ausgeliefert werden." Stelle sich heraus, dass eine Kreditkartennummer gesperrt ist, werde sie umgehend gegen eine neue Nummer ausgetauscht. Außerdem würden die Kreditkartennummern nach Postleitzahlenbereichen sortiert ausgegeben. Mit Hilfe dieser Kreditkartennummern werde dann über eBay auf Auftrag geklaute Ware bezahlt, die in dem Online-Auktionshaus über jeweils gehackte eBay-Identitäten angeboten und gekauft werde. Die Ware wiederum werde über "anonymisierte Zugänge" für Post-Pack-Stationen ausgeliefert.

Siehe dazu auch:

- **Packstation-Phishing mit vertrauenserweckender Domain[4]**
- **Betreff: 7858 pro Monat ist vorstellbar[5]**
- **Trojaner verdrängen Phishing[6]**
- **Haftstrafen im Bonner Phishing-Prozess[7]**

- **BKA sieht Deutschland als Experimentierfeld für Internet-Kriminelle[8]**
- **Universelles Phishing-Kit erleichtert Betrügern die Arbeit[9]**

- **Erfolgreicher Angriff auf iTAN-Verfahren[10]**
- **iTAN-Verfahren unsicherer als von Banken behauptet[11]**

(*Christiane Schulzki-Haddouti*) / (**dab[12]**/c't)

URL dieses Artikels:
http://www.heise.de/security/meldung/BKA-iTAN-Verfahren-keine-Huerde-mehr-fuer-Kriminelle-219497.html

Links in diesem Artikel:
[1] http://www.bsi.de/veranst/IT-SiKongress/index.htm
[2] http://www.bsi.de
[3] http://www.heise.de/meldung/Universelles-Phishing-Kit-erleichtert-Betruegern-die-Arbeit-133246.html
[4] http://www.heise.de/meldung/Packstation-Phishing-mit-vertrauenserweckender-Domain-207561.html
[5] http://www.heise.de/meldung/Betreff-7858-pro-Monat-ist-vorstellbar-218063.html
[6] http://www.heise.de/meldung/Trojaner-verdraengen-Phishing-205751.html
[7] http://www.heise.de/meldung/Haftstrafen-im-Bonner-Phishing-Prozess-203186.html
[8] http://www.heise.de/meldung/BKA-sieht-Deutschland-als-Experimentierfeld-fuer-Internet-Kriminelle-202635.html
[9] http://www.heise.de/meldung/Universelles-Phishing-Kit-erleichtert-Betruegern-die-Arbeit-133246.html
[10] http://www.heise.de/meldung/Erfolgreicher-Angriff-auf-iTAN-Verfahren-147177.html
[11] http://www.heise.de/meldung/iTAN-Verfahren-unsicherer-als-von-Banken-behauptet-125776.html
[12] mailto:dab@heise.de
