COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/identitaetsmissbrauch-bedroht-sicherheit,2349033

E-Business

Identitätsmissbrauch bedroht Sicherheit

Datum: 13.07.2010
Autor(en): Johannes Klostermeier

Am Anfang war es Phishing - inzwischen rückt die komplette digitale Identität des Nutzers in den Fokus von Kriminellen. Die Angriffe erfolgen am häufigsten über so genannte "Trojaner".

Hacker

Der US-Kultautor T.C. **Boyle**[1] schrieb 2006 den Roman "**Talk Talk** [2]". Dabei ging es um Identitätsdiebstahl, eine damals neue Verbrechensvariante in den USA. "Im Zeitalter der PINs, Codes und Passwörter verschaffen sich übelwollende Naturen Zugang zu den Konten ihrer Opfer, um sie dann Wirtstieren gleich auszusaugen und sich deren Identität überzustülpen", heißt es dazu bei Amazon. Opfer im Buch wurde die junge, schöne, gehörlose Dana Halter. Aus heiterem Himmel wird sie wegen Autodiebstahls und Drogenmissbrauchs verhaftet.

Jetzt haben sich das deutsche Bundesministerium des Innern (**BMI**[3]) und das Bundesamt für Sicherheit in der Informationstechnik (**BSI**[4]) des Themas aus wissenschaftlicher Sicht und mit deutscher Gründlichkeit angenommen. Auf 415 Seiten haben führende deutsche Experten die interdisziplinäre **Studie**[5] mit dem Titel "Identitätsdiebstahl und Identitätsmissbrauch im Internet - Rechtliche und technische Aspekte" geschrieben.

Im Datenstrudel: die eigene Identität.

Die Autoren der Studie sind deutsche Wissenschaftler, die führende deutsche Experten auf ihrem Gebiet sind: Professor Georg Borges von der Ruhr-Universität **Bochum**[6] und Professor Carl-Friedrich Stuckenberg von der Universität des Saarlandes sowie Professor Jörg Schwenk und Christoph Wegener (beide von der Ruhr-Universität Bochum).

Die beeindruckende Studie führt detailliert aus, inwiefern Identitätsdiebstahl und Identitätsmissbrauch heute die Sicherheit von **E-Government**[7] und **E-Business**[8] bedrohen. Sie nimmt darüber hinaus eine detaillierte Bewertung des geltenden Rechts in Bezug auf Identitätsdiebstahl vor und zeigt die bereits erzielten Erfolge auf und weist auf neue Lösungsansätze und offene Fragen im Kampf gegen Diebstahl und Handel von digitalen Identitäten hin.

Erst Phishing - jetzt wird die komplette digitale Identität bedroht

Die Sichherheit im Netz wird durch Internetkriminelle bedroht.

Der "Diebstahl" und der anschließende Missbrauch der "entwendeten" Identitäten ist ein neues Kriminalitätsphänomen. Bis vor einigen Jahren wurde mittels des sogenannten "**Phishing**[9]" vornehmlich das Abfischen von Online-Banking-Zugangsdaten beschrieben. Mittlerweile rückt die komplette digitale Identität des Nutzers in den Fokus von Kriminellen, etwa die bei **sozialen Netzwerken**[10], **E-Mail**[11]-**Dienstleistern**[12] und Handelsplattformen verwendeten Identitäten.

Das Thema ist jetzt Deutschland angekommen, es war auch das Gesprächsthema der letzten Dialogveranstaltung des Bundesinnenminister Thomas de Maizière bei der **Veranstaltung**[13] "Perspektiven deutscher Netzpolitik" am 1. Juni 2010.

Die wesentlichen Ergebnisse der Studie sind:

- Angriffe mit dem Ziel eines Identitätsdiebstahls werden heute weit überwiegend über Schadprogramme (sogenannte "trojanische Pferde") durchgeführt, die in der Lage sind, auch fortgeschrittene aktualisierte technische Abwehrmaßnahmen zu umgehen.
- In den Mittelpunkt des Interesses von Internetkriminellen rückt die komplette digitale Identität der Internetnutzer. Neben Online-Banking-Zugängen können zum Beispiel auch die bei E-Mail-Dienstleistern, Packstationen, Auktions- und Handelsplattformen sowie bei Social-Network-Plattformen verwendeten Identitäten betroffen sein.

- Die Vorgehensweise der Täter hat sich in den letzten Jahren geändert: Schadprogramme gelangen heute vorwiegend durch Schwachstellen im Betriebssystem bzw. in Softwarepaketen auf die Nutzer-PCs. 2009 wurden die meisten Systeme durch den bloßen Besuch von Internetseiten ("drive-by-infection") und präparierte PDF-Dokumente angegriffen.

Autoren setzten auf Auklärung, Information und Verhaltenskodex

- Als Gegenmaßnahmen schlagen die Verfasser Standardsicherheitsmaßnahmen (Virenschutzprogramme, Firewall sowie regelmäßige Updates des Betriebssystems und der Anwendungen) vor. Notwendig sei zudem eine umfassende Aufklärung der Internetnutzer.

Abhilfe schaffen könne in vielen Fällen der neue elektronische **Personalausweis**[14]: "Die Analyse der rechtlichen Normierung des Personalausweises und seiner rechtlichen Einbettung belegt mit beeindruckender Deutlichkeit, dass der Personalausweis das zentrale Instrument zum Nachweis der Identität natürlicher Personen darstellt", schreiben die Autoren.

Keine guten Aussichten: Für die Zukunft prognostizieren die Autoren, dass Identitätsdiebstahl und -missbrauch noch nicht absehbare Formen annehmen werden, da neue Techniken und Plattformen immer neue Angriffsszenarien ermöglichen.

Die Wissenschaftler setzen in ihren Handlungsempfehlungen vor allem auf Information und Aufklärung. Gesetzliche Maßnahmen halten die Verfasser hingegen nur in Teilbereichen für wünschenswert. Die Autoren schlagen hingegen die Formulierung von Fachnormen vor, um einen Verhaltensstandard zu etablieren. "Zur Formulierung von Anforderungen an Anbieter stellt grundsätzlich ein Kodex, der durch Selbstbindung verbindlich wird, eine geeignete Alternative zur gesetzlichen Regelung dar." Allerdings bedürfe ein solcher Kodex der Akzeptanz durch die **IT-Industrie**[15] und die Anbieter im Internet.

Hinsichtlich der Verhaltensanforderungen an **IT**[16]-Nutzer komme als Alternative oder Ergänzung zu einer gesetzlichen Regelung die Formulierung und Herausgabe von Verhaltensempfehlungen in Betracht, die "mittelbar die rechtlichen Anforderungen erheblich beeinflussen können". Darüber hinaus könnten Verhaltensempfehlungen eine "erhebliche Steuerungswirkung" entfalten; eine Chance, die nach Meinung der Autoren entschlossen genutzt werden sollte.

Das **Bundesinnenministerium**[17] und das **Bundesamt für Sicherheit**[18] in der Informationstechnik stellen die Studie unter www.bmi.bund.de und www.bsi.bund.de für zwei Wochen als kostenlosen **Download**[19] (PDF) zur Verfügung.

Links im Artikel:

[1] **http://www.tcboyle.com/**
[2] **http://www.perlentaucher.de/buch/25165.html**
[3] **http://www.bmi.bund.de/cln_165/DE/Home/startseite_node.html**
[4] **http://www.bsi.de/**
[5] **https://www.bsi.bund.de/cln_165/ContentBSI/Presse/Kurzmitteilungen/Studie_Identitaetsdiebstahl_090610.html**
[6] **https://www.a-i3.org/content/view/924/194/**
[7] **https://www.computerwoche.de/schwerpunkt/e/eGovernment.html**
[8] **https://www.computerwoche.de/schwerpunkt/e/E-Business.html**
[9] **https://www.computerwoche.de/schwerpunkt/p/Phishing.html**
[10] **https://www.computerwoche.de/schwerpunkt/s/Social-Networks.html**
[11] **https://www.computerwoche.de/schwerpunkt/e/E-Mail.html**
[12] **https://www.computerwoche.de/schwerpunkt/i/IT-Dienstleister.html**
[13] **http://www.e-konsultation.de/netzpolitik/**
[14] **http://www.bmi.bund.de/DE/Themen/Sicherheit/PaesseAusweise/ePersonalausweis/ePersonalausweis_node.html**
[15] **https://www.computerwoche.de/schwerpunkt/i/IT-Industrie.html**
[16] **https://www.computerwoche.de/schwerpunkt/i/IT.html**
[17] **https://www.computerwoche.de/rewrite/dmag.cfm?id=N65285**
[18] **https://www.computerwoche.de/rewrite/dmag.cfm?id=P47641**
[19] **https://www.bsi.bund.de/cae/servlet/contentblob/1086544/publicationFile/909**
