

<http://www.taz.de/!80836/>

Hackerangriff in Schweden

Hunderttausende Passwörter öffentlich

Es ist der bisher größte Hackerangriff in Schweden: 57 Webseiten sind betroffen, allein von einem Blogportal wurden 90.000 Passwörter veröffentlicht.

von Reinhard Wolff

STOCKHOLM taz | Auch schwedische Journalisten und Politiker hatten offenbar bislang noch nicht so ganz verstanden, wie einigermaßen "sichere" Passwörter für Internetkonten aussehen sollten. Das dürfte sich jetzt vermutlich ein wenig geändert haben.

Dieser Personenkreis gehört nämlich zu den Hunderttausenden, deren Zugangsdaten für Nutzerkonten seit einigen Tagen im Netz herumschwirren. Und der Name des Haustiers, des Lieblings-Eishockeyvereins oder einer Musikgruppe taugen eben überhaupt nicht, will man verhindern, dass die privaten Mails von anderen mitgelesen werden.

Beim bislang vermutlich grössten Hackerangriff in Schweden sind 57 Webseiten gehackt worden. Allein vom – zwischenzeitlich geschlossenen – Blogportal "Bloggtoppen" waren es 90.000 Passwörter, die der Hacker "Sc3a5j" im Klartext öffentlich machte. Und damit konnten viele Konten bei anderen Internetseiten ebenfalls geknackt werden: Dann, wenn die User nämlich dort das gleiche Passwort benutzten wie bei Bloggtoppen.

Dies war offenbar auch der Fall bei Journalisten der Stockholmer Zeitungen *Aftonbladet* und *Expressen*. Beide Zeitungen stellten Strafanzeige bei der Polizei wegen unerlaubten Eindringens in Konten ihrer Mitarbeiter.

"Nie im Leben" ist kein sicheres Passwort

Nachdem sie sich erst einmal Zugang zu den Datenbanken der fraglichen Webseiten verschafft hatten, war es für den oder die Hacker ein leichtes, die dort mit einem Hash-Algorithmus verschlüsselten Passwörter in Klartext zu übersetzen. "Sc3a5j" liess diese nach eigenen Angaben einfach durch eine mit entsprechendem Hash-Schlüssel codierte Datenbasis von potentiellen 711.772 Passwörtern laufen und konnte sie so dechiffrieren. Nicht einmal Dialekte, Sprichwörter oder ganze Wortfolgen, wie "nie im Leben" oder "bewaffnet bis zu den Zähnen" fielen durch dieses Sieb.

Natürlich sei es blauäugig, wenn man sehe, wie leicht es UserInnen durch ihren Passwortgebrauch Hackern machten, meint David Lindahl, IT-Sicherheitsforscher beim staatlichen schwedischen Verteidigungsforschungsinstitut FOI. Und das sei mehr als ein privates Problem, wenn sie nämlich auch noch auf geschäftlichen Konten das immer gleiche Passwort gebrauchten.

Aber selbst wer nun glaube mit einer wilden Buchstaben- und Ziffernkombination auf der sicheren Seite zu sein, könnte sich täuschen. Lindahl hält das gesamte System des Konten-Zugangs durch Passwörter für veraltet: "Das ist ein völlig unzureichender Schutz, aber für

die Betreiber von Webseiten eben bequem. Allenfalls wenn es noch mehr Vorfälle wie den jetzigen gibt, wird sich daran vielleicht endlich etwas ändern."

Neue Sicherheit durch Gesichtserkennung

Schuld an den scheunentorgrossen Sicherheitslücken hätten auch alle User: "Sie akzeptieren ja die Benutzerbedingungen in denen sich Webseitenbetreiber im Prinzip von jeder Verantwortung freizeichnen."

Er glaubt, dass die Identifizierung per Passwort in wenigen Jahren ganz verschwunden und allenfalls noch in Kombination mit weiteren Sicherheitssystemen üblich sein wird. Beispielsweise ein Passwort zusammen mit einem Kartenleser und dem Ausweis oder der Kreditkarte. Oder in Verbindung mit einer Webkamera mit entsprechender Gesichtserkennungs-Software.

Für recht erfolgversprechend hält Lindahl ein derzeit in Entwicklung befindliches System, in dem der Anwender sich durch seine Stimme identifiziert. Und er fordert ein prinzipielles Umdenken: "Wir müssen einen ganz neuen Ansatz suchen. Ein Autofahrer kann ja bei einer Geschwindigkeit von 120 km/h auch nicht einfach den Rückwärtsgang einlegen. Computer und deren Nutzung müssen so konstruiert werden, dass sie uns von vorneherein daran hindern, dumme Sachen zu machen."

Zugriff am 31.10.2011