Schweiz

Internetkonten von 37 Parlamentariern gehackt

Jedem achten Bundesparlamentarier wurden bereits Nutzername und Passwort eines Internetkontos gestohlen. Nun mahnen die Parlamentsdienste die Ratsmitglieder eindringlich, die Internetsicherheit ernster zu nehmen.

Barnaby Skinner

Wenn am 16. Oktober um 10.15 Uhr der letzte Nationalrat, die letzte Nationalrätin die strengen Sicherheitskontrollen des Bundeshauses passiert und im Sitzungszimmer der Aussenpolitischen Kommission (APK) den Platz eingenommen haben, werden die Türen verriegelt. Und sie werden erst wieder geöffnet, wenn die Sitzung zu Ende ist.

Was in der APK verhandelt wird, ist streng vertraulich. Mitte Oktober stehen heikle Dossiers wie internationale Steuerfragen oder der Bericht zu den Aktivitäten der schweizerischen Migrationsaussenpolitik 2016 auf der Agenda. Es wäre ungünstig, würden Informationen Dritten in die Hände fallen. Gerade in der Aussenpolitik könnte die Verhandlungspositionen der Schweiz geschwächt werden. Doch die Sicherheitsmassnahmen im Bundeshaus mögen noch so gut sein. Die grössten Schwachstellen entstehen nicht während der Sitzungen, sondern während der Kommunikation mit neuen Technologien. Parlamentarier profitieren wie alle andere auch von E-Mail, sozialen Medien oder Dokumenten-Hosting-Systemen. Und je mehr Technologie sie nutzen, desto grösser ist die Gefahr, dass ein Informationsleck entsteht.

Das Passwort nie gewechselt: SVP-Nationalrat Heinz Brand an seinem Computer. Foto: Alessandro della Valle (Keystone)

Betroffene in allen Parteien

Der TA hat Zugriff auf eine Datenbank von Abermillionen geleakten Internetkonten und hat darin nach den beruflichen und privaten E-Mail-Adressen aller National- und Ständeräte gesucht. Die Suche landete insgesamt 37 Treffer: Darunter waren Nutzernamen und Passwörter von E-Mail-Konten, Linkedin-Profilen und Zugängen zu Filehosting-Systemen wie Dropbox. Das heisst: Die Internetkonten von rund jedem achten Parlamentarier waren für Dritte zumindest zwischenzeitlich zugänglich. Darunter Politiker aus allen Parteien, Heinz Brand von der SVP etwa, Christian Levrat von der SP oder Isabelle Chevalley von der GLP.

Die zur Verfügung gestellte Datenbank der geleakten Daten gehört der Zürcher Firma Kaduu. Sie entwickelt ein System, das im sogenannten Darknet und im Deepweb nach geleakten Daten sucht. Geleakte Konten werden in einer Datenbank zusammengefasst, damit Nutzer prüfen können, ob die Zugangsdaten ihrer Konten bereits entblösst wurden. Das passiert zum Beispiel dann, wenn es Hackern gelingt, sich in die Server eines Dienstanbieters zu hacken, zum Beispiel in diejenigen des Swisscom-Mailanbieters Bluewin.

Das Perfide dabei: Oft weiss ein Dienstbetreiber gar nicht, dass er bestohlen wurde, weil die Kriminellen die Daten nicht entwenden, sondern kopieren. Sie verkaufen ihre Beute dann in einschlägigen Foren. Je aktueller ein Datenklau ist, desto mehr Geld können die Cybergangster verlangen; denn je älter ein Leck, desto grösser die Wahrscheinlichkeit, dass Nutzer ihre Passwörter geändert haben. Ältere Datensätze sind oft umsonst zu finden. Diese sammelt die Firma Kaduu automatisch ein. Wenn ein Leak günstig zu haben ist, bezahlt Kaduu auch für Daten. Dafür hat sie Mitarbeiter angestellt, die wochenlang in Foren unter falscher Identität mit Cyberkriminellen in Kontakt treten.

Der Freiburger SP-Ständerat Christian Levrat taucht gleich zweimal in der Datenbank auf. Mit seiner privaten Bluewin-Adresse und mit seiner offiziellen Parl.ch-Adresse, beide Male in Zusammenhang mit einem Dropbox-Konto. «Dieser Datenklau liegt schon eine Weile zurück. Und wenn ich mich richtig erinnere, benutzte ich das Konto damals nur, um Vorlagen für Plakat-Politwerbung auszutauschen», sagt Levrat. Seither hätte er diese Konten nicht mehr verwendet.

«Im Zweifel für die Briefpost»

Doch tote Konten, die mit den Mails von National- und Ständeräten verknüpft sind, sind ebenfalls problematisch. Viele Nutzer verwenden für unterschiedliche Konten das gleiche Passwort. «Bei meiner E-Mail erneuere ich das Passwort regelmässig, bei anderen Konten tue ich das seltener», sagt Levrat. «Das ist jetzt eine gute Gelegenheit, es nachzuholen.»

Andere wechseln ihr E-Mail-Passwort gar nie. SVP-Nationalrat Heinz Brand zum Beispiel. Auch in seinem Fall ist ein Dropbox-Passwort in den geleakten Konten aufgetaucht. Der Bündner betont aber, dass er sich nie auf digitalem Weg über Kommissionsgeheimnisse austauschen würde. Sein Grundsatz lautet: «Im Zweifel für die Briefpost.»

Die Waadtländer GLP-Nationalrätin Isabelle Chevalley stritt zunächst ab, Dropbox zu benutzen. Erst als der TA sie damit konfrontierte, dass man im Besitz ihres Login und möglicherweise ihres aktuellen Passwortes sei, sagte sie: «Ich habe zu privaten Zwecken ein Dropbox-Konto. Nichts, was ich dort speichere, ist vertraulich. Wenn es die Piraten amüsiert, sich Zugang dazu zu verschaffen, nur zu!» Wie Brand würde sie nie via E-Mail vertrauliche Informationen austauschen – um dann einzuräumen: «Höchstens über meine Parl.ch-Adresse.»

Immer wieder ermahnt

Genau auf solche Inkonsistenzen bauen Hacker, wenn sie gezielt die Konten einzelner Personen ausspähen: Im Darknet sammeln sie Nutzerkonten und Passwörter. Mit etwas Glück funktionieren die Passwörter dann auch in anderen Konten der jeweiligen Benutzer. Das Problem haben auch die Parlamentsdienste erkannt. Die Verwaltungsdelegation hat einen Mehrpunkteplan ausgearbeitet, wie sich die eidgenössischen Räte im Internet zu verhalten haben. Dieser bleibt allerdings geheim. Nur so viel verraten die Parlamentsdienste: «Das Problem ist weniger die Verwendung des Rats-E-Mails, sondern die Mehrfachverwendung desselben Passworts.» Ratsmitglieder würden immer und immer wieder dazu ermahnt, unterschiedliche Passwörter zu verwenden.

Um zu unterstreichen, wie ernst die Parlamentsdienste die Cybersicherheit nehmen, schrieben sie nach der TA-Anfrage die 37 gehackten National- und Ständeräte an. Betreff: «Kompromittierte Authentisierungsdaten». Weiter: «Wir wurden gestern von einem Journalisten über eine Liste gehackter Konten informiert.» Nach einer internen Prüfung könnten die Parlamentarier aber versichert sein, dass Integrität und Sicherheit der Infrastruktur der Bundesversammlung nicht betroffen seien.

Das E-Mail bat die Ratsmitglieder eindringlich: «Ändern Sie das Passwort sämtlicher Konten, die mit der betroffenen E-Mail-Adresse verknüpft sind. Verwenden Sie bei jedem Internetdienst ein separates Passwort.» Um dann etwas ohnmächtig zu schliessen: «Leider fehlen uns die Informationen, welche externen Internetdienste kompromittiert sind.» Ob die Botschaft angekommen ist, auch dazu fehlt den Parlamentsdiensten die Information.

Das Darknet im Deepweb

Wo die Daten gehandelt werden

Das Deepweb ist der Teil des Internets, der von Suchmaschinen nicht indexiert wird – weil die Suchmaschine mit der Menge an Information nicht umgehen kann. Die Inhalte werden damit bei Google-Suchen nicht angezeigt. Das Darknet wiederum ist Teil des Deepwebs. Hierbei handelt es sich um Inhalte, die nicht von Suchmaschinen gefunden werden sollen. Darknet-Websites sind nur mit speziellen Browsern abrufbar, dem Tor-Browser zum Beispiel. Der Datenfluss im Darknet ist komplett verschlüsselt, Nutzer surfen hier anonym. Deshalb ist das Darknet, das an sich nicht illegal ist, auch bei Aktivisten und Journalisten beliebt. Es wird allerdings auch von Kriminellen missbraucht, etwa für den Handel von Nutzerdaten, Waffen oder illegaler Pornografie. Die Hackergruppe Anonymous hat im Februar dieses Jahres 20 Prozent des Darknets lahmgelegt. Darunter rund 10 000 Seiten mit kinderpornografischem Inhalt. *(bsk)*