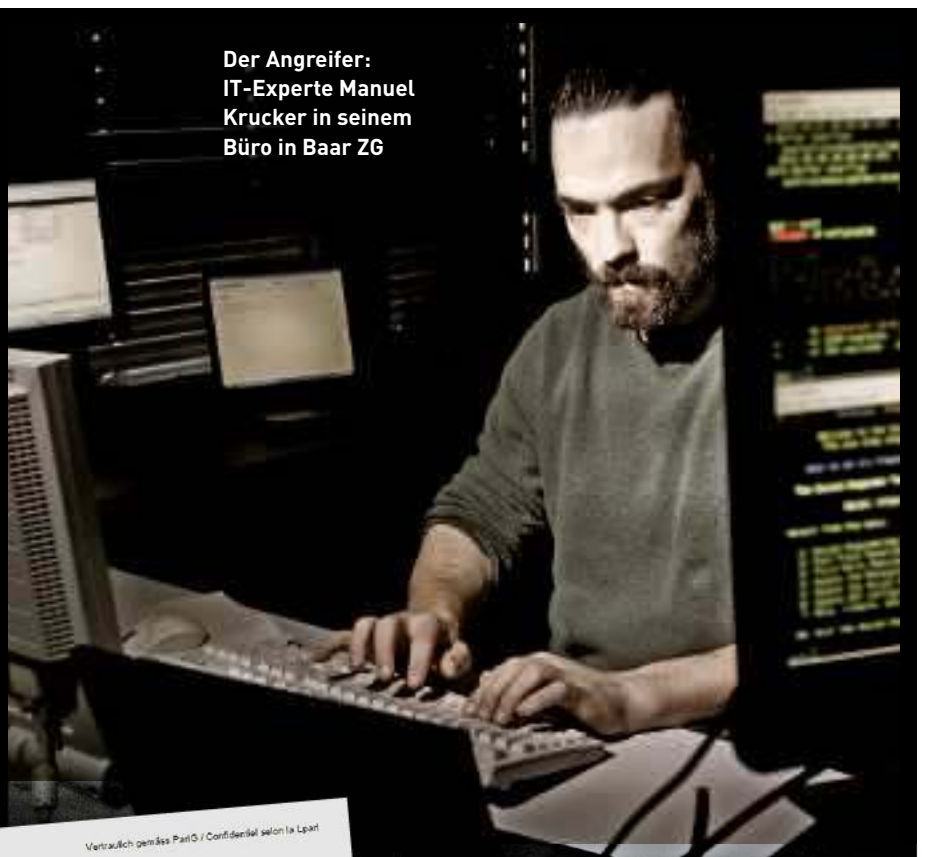
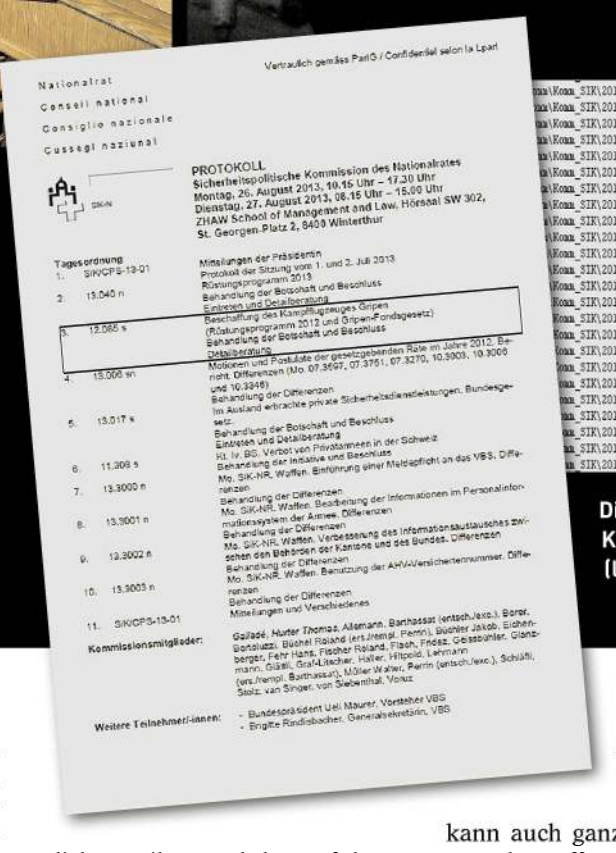
Die Opfer: Die Nationalräte Yannick Buttet, Balthasar Glättli und Jean-Christophe Schwaab (v. l. n. r.)



Der Angreifer: IT-Experte Manuel Krucker in seinem Büro in Baar ZG

Angriff auf den Nationalrat

Ein Test zeigt, wie einfach Hacker unsere Parlamentarier ausspionieren können



Nationalrat
Conseil national
Consiglio nazionale
Cussegl naziunal

Vertraulich gemäss ParlG / Confidentiel selon la Lparl

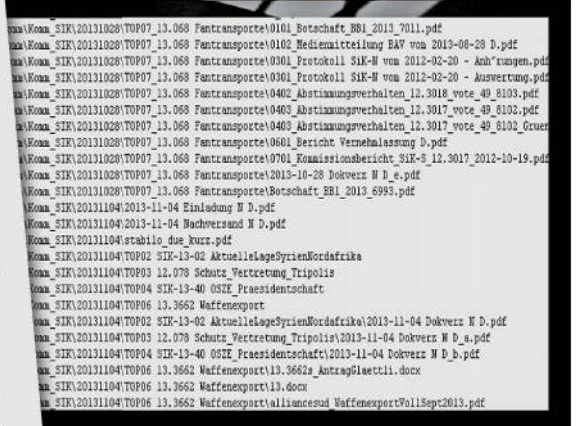
SIK-N

PROTOKOLL
Sicherheitspolitische Kommission des Nationalrates
Montag, 26. August 2013, 10.15 Uhr – 17.30 Uhr
Dienstag, 27. August 2013, 08.15 Uhr – 15.00 Uhr
ZHAW School of Management and Law, Hörsaal SW 302,
St. Georgen-Platz 2, 8400 Winterthur

Tagesordnung
1. SIK/CPS-13-01 — Mitteilungen der Präsidentin
2. 13.040 n — Protokoll der Sitzung vom 1. und 2. Juli 2013
Rüstungsprogramm 2013
Behandlung der Botschaft und Beschluss
Eintreten und Detailberatung
3. 12.085 s — Beschaffung des Kampfflugzeuges Gripen
(Rüstungsprogramm 2012 und Gripen-Fondsgesetz)
Behandlung der Botschaft und Beschluss
Detailberatung
4. 13.006 w — Motionen und Postulate der gesetzgebenden Räte im Jahre 2012. Bericht, Differenzen (Mo. 07.3697, 07.3751, 07.3270, 10.3003, 10.3006 und 10.3346)
Behandlung der Differenzen
5. 13.017 s — Im Ausland erbrachte private Sicherheitsdienstleistungen. Bundesgesetz.
Behandlung der Botschaft und Beschluss
Eintreten und Detailberatung
6. 11.308 s — Kt. Iv. BS. Verbot von Privatarmeen in der Schweiz
Behandlung der Initiative und Beschluss
7. 13.3000 n — Mo. SiK-NR. Waffen. Einführung einer Meldepflicht an das VBS. Differenzen
Behandlung der Differenzen
8. 13.3001 n — Mo. SiK-NR. Waffen. Bearbeitung der Informationen im Personalinformationssystem der Armee. Differenzen
Behandlung der Differenzen
9. 13.3002 n — Mo. SiK-NR. Waffen. Verbesserung des Informationsaustausches zwischen den Behörden der Kantone und des Bundes. Differenzen
Behandlung der Differenzen
10. 13.3003 n — Mo. SiK-NR. Waffen. Benutzung der AHV-Versichertennummer. Differenzen
Behandlung der Differenzen
11. SIK/CPS-13-01 — Mitteilungen und Verschiedenes

Kommissionsmitglieder: Gaillard, Hunter Thomas, Allemann, Barthassat (entsch./exc.), Borer, Bortoluzzi, Büchel Roland (ers./rempl. Perrin), Büchler Jakob, Eichenberger, Fehr Hans, Fischer Roland, Flach, Fridez, Giezendanner, Glanzmann, Glättli, Graf-Litscher, Haller, Hiltpold, Lehmann (ers./rempl. Barthassat), Müller Walter, Perrin (entsch./exc.), Schläfli, Stolz, van Singer, von Siebenthal, Voruz

Weitere Teilnehmer/-innen: - Bundespräsident Ueli Maurer, Vorsteher VBS
- Brigitte Rindlisbacher, Generalsekretärin, VBS



Die Dokumente: Vertrauliches Kommissionsprotokoll von Glättlis Computer (l.), Auszug der Daten auf der Festplatte

VON FLORIAN IMBACH, ALEXANDRE HAEDERLI (TEXT) UND ESTHER MICHEL (FOTOS)

BERN Am 8. Januar, um 14.28 Uhr, beginnt der Angriff. Balthasar Glättli sitzt vor seinem Laptop in seinem kleinen Büro in Zürich Wipkingen. Es ist die heisse Phase des Abstimmungskampfes um die Einwanderungsinitiative. Der Fraktionschef der Grünen hat keine freie Minute, rennt von Podium zu Podium.

Die E-Mails strömen bei Glättli nur so rein. Darunter auch eine von Hans Strittmatter vom Verband Zürcher Handelsfirmen. Glättli weiss, dass Strittmatter das morgige Podium zur Einwanderungsinitiative organisiert, wo auch er auftreten wird. Strittmatter schickt ihm eine Übersicht über die politische und demografische Zusammensetzung des Publikums – nützliche Angaben, die Politiker nur selten erhalten. Das Virenprogramm bleibt ruhig. Es ist 14:30 Uhr, Glättli öffnet das Word-Dokument.

In dieser Sekunde blinkt eine Meldung auf dem Laptop von Manuel Krucker. Der IT-Spezialist der Firma Infoguard sitzt hinter einer Wand aus Bildschirmen im dritten Stock eines grauen Bürokomplexes in Baar bei Zug. Er lächelt. Strittmatters Mail war sein Werk – eine Fälschung. Krucker hat soeben einen Nationalrat gehackt – ein Test im Auftrag der SonntagsZeitung *(siehe Kasten rechts)*.

Der IT-Experte nennt das ein «gezieltes Szenario auf eine exponierte Einzelperson». Hacker nennen es Whaling, Walfang. Dass Glättli bei Strittmatters Podium referiert, hat Krucker eine Woche zuvor auf dem Facebook-Profil des Nationalrats entdeckt. Während Tagen durchleuchtete Krucker den Nationalrat, notierte sich alles, was er über ihn herausfinden konnte. «Glättli ist ein gutes Opfer», sagt Krucker, «weil er sehr viel von sich preisgibt».

Aus seiner Kommandozentrale in Baar schreibt der Informatiker immer wieder Befehle, die das Spionageprogramm bei Glättli gehorsam ausführt. Während der Politiker munter weiterarbeitet, beginnt das Programm im Hintergrund fleissig Daten an Krucker zu schicken.

Krucker erstellt als Erstes einen Auszug aller Ordner und Dokumente, ein sogenanntes Directory Listing. Kruckers Augen wandern über seitenweise sensibles Material: interne Sitzungsprotokolle, Gesprächsnotizen, Gesetzesentwürfe, geplante Anträge, Mitberichte, vertrauliche Berichte, Subkommissionsberatungen und Listen über Abstimmungsverhalten.

Der Angreifer kontrolliert das digitale Leben von Glättli

Krucker kann diese Dokumente stehlen, ohne eine Spur zu hinterlassen. Man stelle sich vor, er wäre kein IT-Sicherheitsexperte, sondern ein Angreifer mit bösen Absichten. Durch Unterlagen auf Glättlis Computer hat der Angreifer Einblick in Milliarden-Rüstungsgeschäfte, die in der sicherheitspolitischen Kommission diskutiert werden. Krucker hat zum Beispiel Zugriff auf die Details des Beschaffungsgeschäfts Gripen. Er kann die Diskussionen in der Kommission verfolgen, die Voten der Parlamentarier einsehen, die technischen Berichte der Luftwaffe studieren.

Hätte Krucker den Nationalrat einige Monate früher gehackt, hätte er schon damals Einblick in die Debatte über die Einsatzfähigkeit der Luftwaffe gehabt. Im Februar war die Schweizer Öffentlichkeit entsetzt darüber, dass die Luftwaffe nur zu Bürozeiten fliegt. Französische Kampfflieger fingen ein entführtes Flugzeug ab. Krucker sieht in den Unterlagen, wie die Kommission die Schwachstelle der Landesverteidigung bereits seit längerer Zeit diskutiert.

Auch im aussenpolitisch brisanten Geschäft um den Steuerstreit mit den USA hat ein Angreifer Pläne und Positionen der Fraktionen, die internen Argumente und Absichten vor sich ausgebreitet. Alles findet sich in E-Mail-Austausch, Gesprächsnotizen und Positionspapieren auf dem Laptop des Nationalrats.

Mit den gestohlenen Daten kontrolliert Krucker das digitale Leben Glättlis. Dank einer Passwortliste hat er Zugriff auf Twitter, Facebook und Linkedin. Ein Klick von ihm, und der Ruf des Politikers wäre ruiniert. Zum Beispiel mit rassistischen Sprüchen auf Twitter oder durch intime Fotos, die ins Internet gelangen.

Auf die Installation eines Trojaners verzichtet Krucker bewusst. Ein Trojaner ist ein mächtiges Spionageprogramm für die komplette Überwachung eines Computers. Trojaner öffnen Hintertüren und können Schaden anrichten. Ein echter Hacker hätte so nach Belieben Mikrofon und Kamera einschalten können und vertrauliche Kommissionssitzungen live mitverfolgt.

Ein Angriff kann auch ganze Computer-Netzwerke treffen. Das zeigt der Angriff auf den zweiten Nationalrat, Yannick Buttet, CVP Wallis. Buttet ist nebst seinem Amt als Nationalrat auch Präsident der Walliser Gemeinde Collombey-Muraz. Ein USB-Stick mit Zugang zu einer Seilbahn-Webcam in der Gegend sollte sein Interesse wecken. Auch dies ein gefälschtes Schreiben von Krucker. Buttet glaubt der Fälschung und lässt den Gemeindeinformatiker am 7. März das «Webcam-Programm» installieren. Die Gemeinde Collombey-Muraz ist gehackt, auch Buttets Laptop ist an diesem Tag im Netzwerk.

Ein weitergehender Angriff aus der Gemeindeinfrastruktur hätte Schaden anrichten können, darum hört Krucker hier auf. Buttet sagt: «Es reicht offenbar nicht, einfach nur vorsichtig zu sein. Wir müssen uns alle besser auf Hackerangriffe vorbereiten.»

Buttet lässt nun in seiner Gemeinde alle USB-Anschlüsse versiegeln. Glättli sagt, er werde nun noch paranoider sein beim Öffnen von E-Mails, zeigt aber auch eine gewisse Hilflosigkeit: «Trotz Virenscanner und Verschlüsselung wurde ich gehackt. Das gibt mir zu denken.»

Einige Parlamentarier benutzen «gehärteten Laptop»

Der Versuch zeigt klar, dass in der Schweiz wichtige Geheimnisträger gehackt werden können. «Es geht um die Interessen der Schweiz», sagt IT-Spezialist Krucker. Er fordert, dass Parlamentarier besser geschützt werden. Damit Hacker keine Dokumente stehlen können, sollen National- und Ständeräte in einer geschützten Umgebung des Bundes arbeiten. Über eine verschlüsselte Internetverbindung könnten sie sich von überall her in das System einwählen und hätten dort einen «virtuellen Desktop», den sie wie ihren eigenen PC nutzen können, in Tat und Wahrheit arbeiten sie aber auf einem geschützten Rechner in Bern.

Ein solches System hätte auch der IT-Sicherheitsbeauftragte der Parlamentarier gerne. Pascal Adam aber sagt, solche verbindliche Schutzmassnahmen müssten sich die National- und Ständeräte selbst auferlegen. Die Parlamentsdienste könnten ein solches System zur Verfügung stellen. Sie seien aber gegenüber den Parlamentariern nicht weisungsbefugt. «Wir haben ein Milizparlament. Die Sicherheit liegt grundsätzlich in der Verantwortung der Parlamentarier», sagt Adam. Er biete bereits einiges, um die National- und Ständeräte zu schützen. Viele Parlamentarier nutzen etwa den «speziell gehärteten» Laptop, der von den Parlamentsdiensten gewartet wird.

Grundsätzlich gilt: Einen 100-prozentigen Schutz gibt es nicht. Wer sich aber in der Öffentlichkeit zurückhaltend verhält, macht es Hackern schwer. Der Angriff auf Jean-Christophe Schwaab zeigt dies deutlich. Über den SP-Nationalrat aus dem Waadtland fand Krucker sehr wenig für einen Angriff. Schwaab war auch misstrauisch genug, eine anonym zugeschickte Whistleblower-Festplatte eines angeblichen Post-Mitarbeiters nicht einzustecken. Schwaab hatte sich in einer Motion über Missstände bei der Post geäussert. Zwar funktionierte die Täuschung, wie Schwaab zugibt: «Ich war sehr neugierig und wollte unbedingt wissen, was da drin ist.» Der Nationalrat steckt aber aus Prinzip keine fremden USB-Sticks ein.

recherchedesk@sonntagszeitung.ch

So schützen Sie sich vor Hackerangriffen

1 Betriebssystem aktuell halten. Installieren Sie Updates mit der automatischen Aktualisierung in den Systemeinstellungen.

2 Internetbrowser aktuell halten. Schwachstellen in Firefox, Chrome oder Internet Explorer sind ein häufiges Einfallstor. Achten Sie auch auf Erweiterungen wie Acrobat Reader und Flash.

3 Vorsicht bei Mails mit Anhang oder Links. Beim Absender nachfragen oder einige Tage warten vor dem Öffnen. Oft wird der Angriffsserver bereits nach einigen Stunden geblockt.

4 Überprüfen Sie Ihren PC mit einem Trojaner-Detektor (z. B. Kaspersky Rescue Disc). Das Programm lässt sich ab CD starten und prüft Ihren Computer.

5 Speichern Sie wichtige Daten auf eine externe Festplatte, die Sie nur bei Bedarf einstecken.

Das steckt hinter dem Parlamentarier-Hack

Für den Versuch stellten sich Nationalräte dreier Bundesparteien zur Verfügung: Balthasar Glättli (Grüne/ZH), Jean-Christophe Schwaab (SP/VD) und Yannick Buttet (CVP/VS). Die Parlamentarier gaben ihr Einverständnis und liessen sich während einer gewissen Zeit angreifen, ohne zu wissen, wann die Angriffe erfolgen würden. Den Versuch organisierte die SonntagsZeitung in Zusammenarbeit mit der IT-Sicherheitsfirma Infoguard in Baar ZG. Die Firma mit 40 Spezialisten ist in der Schweiz und Europa tätig und berät Kunden in Sachen IT-Sicherheit. Dabei prüfen Spezialisten wie Manuel Krucker die Kundensysteme und suchen Schwachstellen. Dazu gehört oft ein inszenierter Hackerangriff. Im Gegensatz zu kriminellen Hackern nutzen «gute» Hacker wie Krucker die gefundenen Schwachstellen nicht aus, sondern helfen den Unternehmen, ihre Sicherheit zu verbessern.