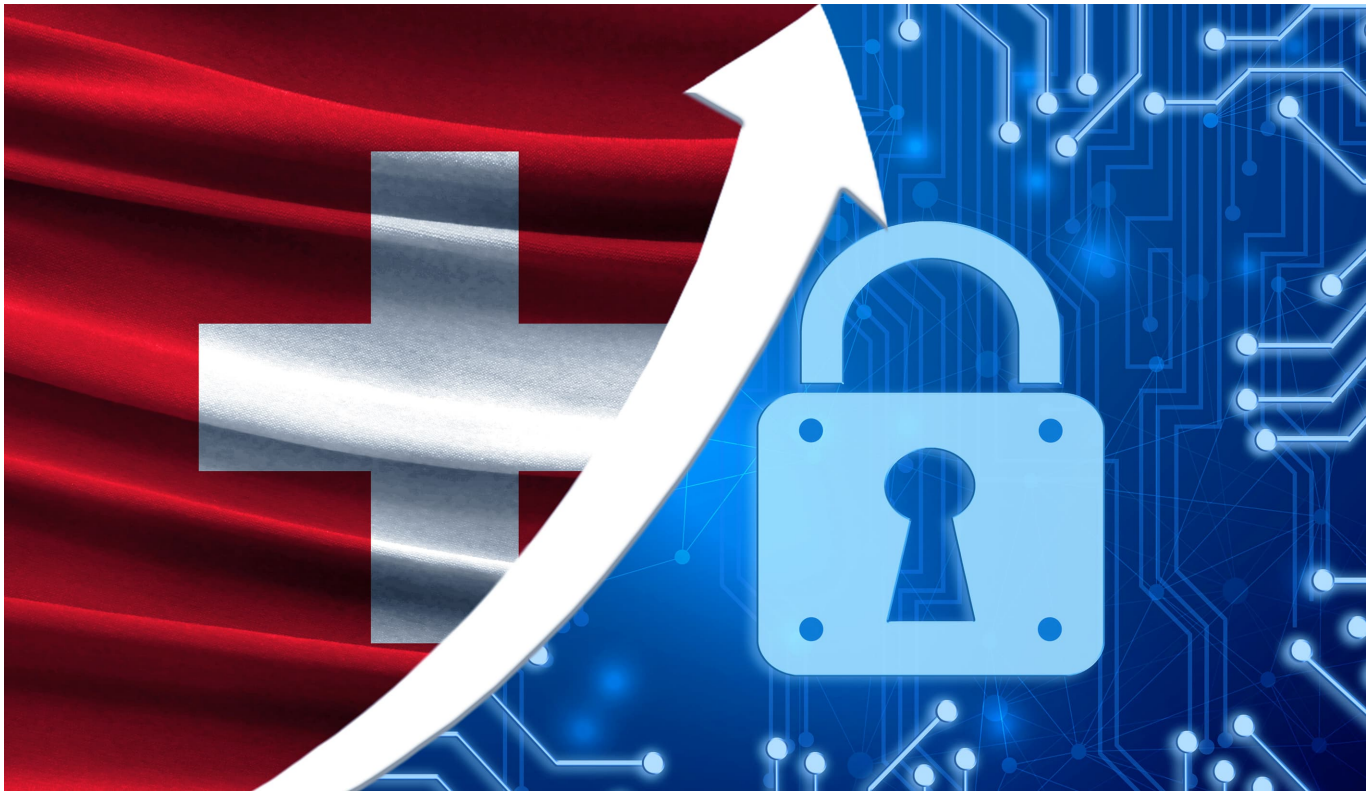
SocietyByte
Wissenschaftsmagazin des BFH-Zentrums Digital Society
https://www.societybyte.swiss

Die angebliche Sicherheitslücke im Genfer E-Voting - eine Kritik an der TV-Berichterstattung

Autor : Christian Folini

Datum : 20. November 2018



Am 2. November behauptete das Schweizer Fernsehen in mehreren News-Sendungen, das Genfer E-Voting-System sei geknackt worden. Dabei recherchierte das Fernsehen unsorgfältig und berücksichtigte die Warnungen von zwei Schweizer Hochschulprofessoren nicht. Es beherzigte auch die Stellungnahme des Kantons Genf nicht gebührend und erlaubte einem Vertreter des Chaos Computer Clubs, offensichtliche Falschaussagen über die SRF Kanäle zu verbreiten. Unser Autor zeigt die Versäumnisse der Medienschaffenden auf und stellt die Ereignisse in ihren Kontext.

Offenbar fahren Vertreter des Schweizer Chaos Computer Clubs CCC eine Kampagne gegen die Pläne, E-Voting in der Schweiz flächendeckend einzuführen. In zahlreichen Zeitungen erschienen im Laufe des Jahres negative Artikel zum Zustand der beiden hiesigen, etablierten E-Systeme. Während die Printmedien inzwischen differenzierter berichten, spitzte das SRF am 2. November den negativen Befund sogar zu.

Inszenierter Angriff unter Laborbedingungen

Volker Birk vom CCC demonstrierte in der Hauptausgabe der Tagesschau vom 2. November

einen Angriff unter Laborbedingungen. Der vorgestellte Angriff erlaubt es unter Umständen, ein einzelnes Opfer beim erstmaligen Aufruf des Genfer E-Voting-Systems auf eine präparierte Seite umzuleiten. Das Opfer hat gute Möglichkeiten, diese Umleitung zu verhindern. Der Angriff funktioniert nämlich nicht, wenn das Opfer die URL vollständig abtippt, die URL nach dem Aufruf nochmals überprüft oder das Sicherheitszertifikat kontrolliert, was in der Anleitung ausdrücklich empfohlen wird.

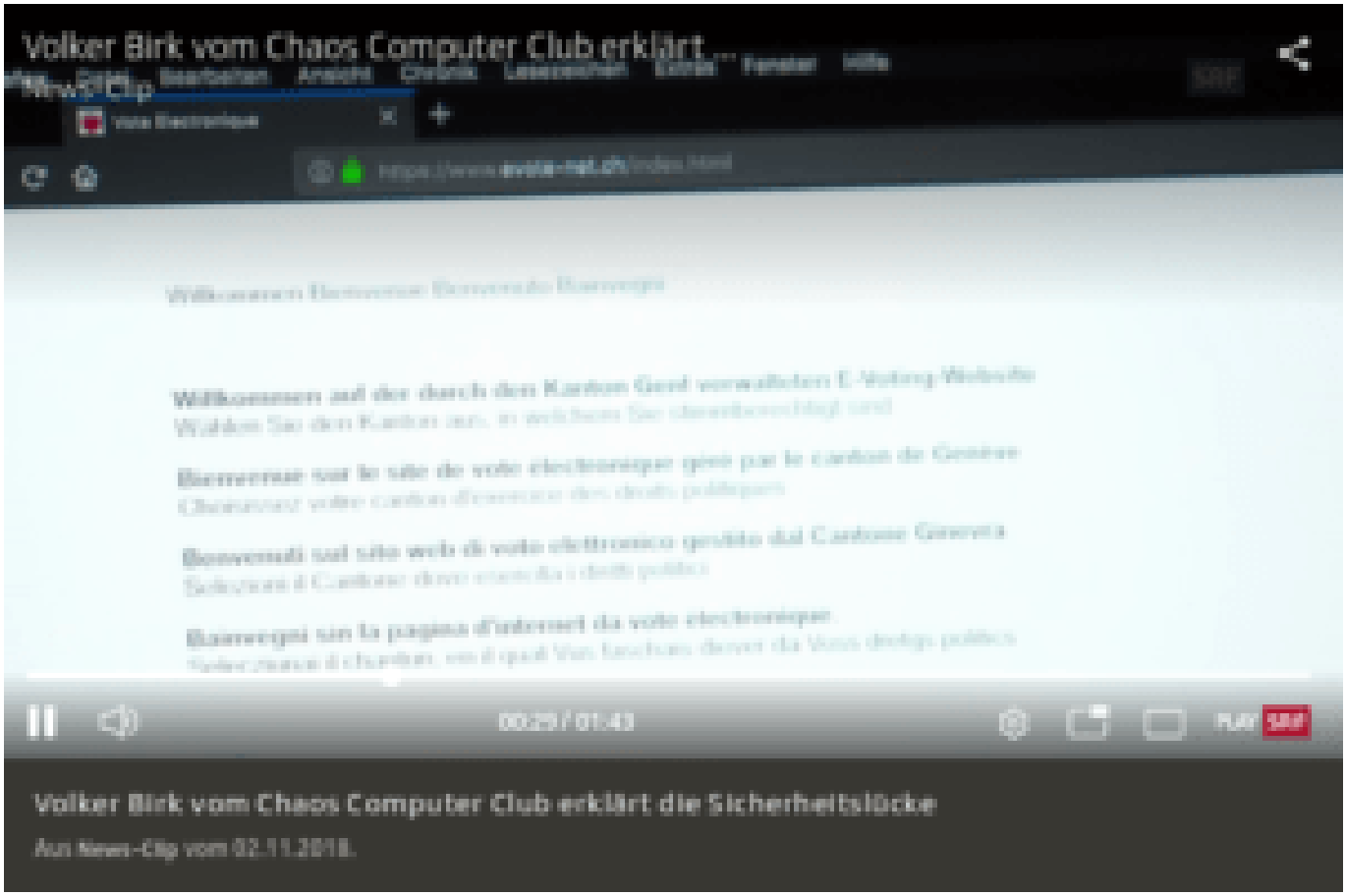


Abbildung 1: Der gefälschte Server ist an der URL leicht zu erkennen (Quelle: SRF)

Auf das briefliche Abstimmen übertragen, hat die Angreifer einen eigenen präparierten Briefkasten an einem öffentlichen Ort platziert. Sie warten nun die gesamte dreissigtägige Stimmperiode lang darauf, die einzelnen StimmbürgerInnen zu diesem falschen Briefkasten umzuleiten: Die StimmbürgerInnen sollen die ausgefüllten Stimmunterlagen in den gefälschten Briefkasten einwerfen. Sofern das Opfer angesichts der Umleitung zu einem gefälschten Briefkasten keinen Verdacht schöpft, erhält der Angreifer so Zugriff auf das Stimmmaterial. Er kann dann das Stimmgeheimnis des Opfers brechen.

Es ist nicht auszuschliessen, dass ein einzelnes Opfer auf diesen Angriff hereinfallen würde. Es ist auch denkbar, dass fünf, zehn, fünfzig oder gar hundert StimmbürgerInnen parallel angegriffen würden und sich von einem gefälschten Briefkasten übertölpeln lassen könnten. Aber je grösser die Zahl, desto wahrscheinlicher wird es, dass jemand Verdacht schöpft –

zumal es nur bei Opfern funktioniert, die zum ersten Mal online abstimmen. Alle anderen würden den gefälschten Briefkasten aufgrund einer Sicherheitswarnung sofort erkennen.

Das alles ändert nichts daran, dass der Angriff technisch funktioniert. Und auch wenn der Angriff nicht skalieren wird, ohne bemerkt zu werden, so könnten die Gegenmassnahmen durch den Kanton Genf doch noch etwas optimiert werden. Dies wird in diesem Artikel erläutert.

Steigerung der Fehlinterpretation

Die gravierenden Fehler in der Berichterstattung passierten während der Recherche und bei der Interpretation im Fernsehstudio: Die Interpretation war unpräzise und schoss über das Ziel hinaus.

1. Im Newsflash

In einem am frühen Abend des 2. Novembers publizierten Newsclips suggeriert das Fernsehen bereits die Möglichkeit zur Manipulation der Abstimmung: "Eine Auslandschweizerin [...] will beim eidgenössischen Urnengang vom 25. November elektronisch abstimmen. Dafür benutzt sie das E-Voting-System des Kantons Genf, der dies anderen Kantonen zur Verfügung stellt. Sobald sie die Adresse evote-ch.ch/lu in ihren Webbrowser eingegeben hat, wird sie auf eine gefälschte Seite umgeleitet. Eine Seite, die Hacker präpariert haben – um an die Stimmabsichten der Frau zu gelangen, oder noch schlimmer: um ihre Stimme zu manipulieren." Aber manipuliert wurde einzig der Aufruf des Browsers. Von der Möglichkeit, die Stimme zu manipulieren, kann keine Rede sein, denn das verhindern weitere Sicherheitsmassnahmen. Diese Unterscheidung macht der Beitrag erst weiter unten im Text. Dort gelingt auch eine Einordnung des Angriffes und ein separater Kasten erklärt den LeserInnen, wie sie sich schützen können.**

2. In der Tagesschau

In der Hauptausgabe der Tagesschau des 2. Novembers nahm der Sprecher die Idee der Manipulation auf und leitete wie folgt ein: "Hacker konnten bei einem Test ein grosses System manipulieren". Und dann weiter "Zu den Recherchen von SRF, dass es Hackern gelungen ist, das Genfer E-Voting-System zu manipulieren..."Während der Newsclip also noch behauptete, es bestehe die Möglichkeit, eine einzelne Stimme zu manipulieren, wurde daraus in der Tagesschau eine Manipulation des Gesamtsystems.

3. In der Sendung 10vor10

Auch 10vor10 machte es nicht besser. Hier sprach man von einem klaffenden Loch und dass es gelungen sei, das E-Voting-System zu knacken: Die Begriffe "klaffendes Loch", "knacken" und "manipulieren" in Bezug auf das E-Voting-System des Kantons Genf lassen ein massives Sicherheitsproblem vermuten. Und für die Masse des Fernsehpublikums ist kaum ein anderer Schluss möglich, als dass Resultate von Abstimmungen manipuliert werden könnten. Dies ist

aber nicht der Fall. Denn wie oben erläutert, würde das flächendeckende Umleiten den StimmbürgerInnen sehr schnell auffallen.

Ferner scheitert die Manipulation der Stimmen an persönlichen Prüfcodes, die man gemäss Benutzerführung während des Abstimmens auf dem E-Voting-System überprüfen soll. Es ist durchaus denkbar, dass einzelne Stimmbürger und Stimmbürgerinnen diesen Schritt unterlassen. Aber die Aufforderung, den Code zu kontrollieren, wird vom E-Voting-System sehr deutlich gemacht. Man muss sich also mit Absicht an dieser Aufforderung vorbeiklicken und früher oder später wird jemand der expliziten Aufforderung nachkommen. Der oder die Erste, die hier einen Fehler entdecken und melden, würden sofort eine weitreichende Untersuchung auslösen und die Wahlkommission käme zum Zuge. Der Fehler könnte natürlich auch darin bestehen, dass ein Angreifer diese Aufforderung verschwinden lässt. Das ist für einen Angreifer technisch gut machbar. Aber hier wiederholt sich das Muster: Ein einzelnes Opfer wird eventuell keinen Verdacht schöpfen, aber der Angriff skaliert nicht, da dann unweigerlich jemand darauf aufmerksam wird und Alarm schlagen wird. Dieser Prozess liefe dann identisch ab, wie es bei Manipulationen von Stimmen beim brieflichen Abstimmen und Wählen üblich ist: Es wird eine formelle Untersuchung eingeleitet und die Wahl gegebenenfalls für ungültig erklärt.*

Fehler bei der Recherche

Wie konnte es zu dieser Fehlleistung durch die FernsehjournalistInnen kommen? Wenden wir uns zunächst der Recherche zu. Hier wurde der Angriff nicht selbst durchgespielt, sondern man liess sich den ersten Teil des Angriffs, die Umleitung, durch die Vertreter des Chaos Computer Clubs demonstrieren. Da Zeit natürlich knapp ist, ist dieses Vorgehen verständlich. Tatsächlich wurden aber die einfach überprüfbaren Behauptungen von Birk nicht kontrolliert, sondern unhinterfragt übernommen und im Wortlaut ausgestrahlt. So etwa die Behauptung, der Kanton Genf habe gar keine Massnahmen zur Abwehr des Angriffes unternommen. Das ist nachweislich falsch. Hätten die Medienschaffenden diese Behauptung selbst zum Beispiel mit Hilfe der bei Sicherheitsforschern beliebten Shodan Datenbank überprüft, wäre ihnen sofort aufgefallen, dass das Genfer E-Voting-System während der Wahlperiode den sogenannten HSTS-Standard unterstützt, der genau diesen gezeigten Angriff erschwert. Und auch die vom Fernsehen auf der Webseite publizierte Stellungnahme der Genfer Staatskanzlei weist darauf hin, dass der Kanton sehr wohl Massnahmen ergriffen hat.

Auch dies veranlasste die JournalistInnen nicht dazu, über die Bücher zu gehen. Das ist nicht die einzige Fehlleistung. Im oben verlinkten Beitrag erklärt Birk den Angriff: "Die Idee ist folgende: Der Wähler möchte sich mit dem Server des Kantons Genf verbinden. Und wir leiten ihn um auf den Server des Angreifers, ohne dass der Wähler eine Möglichkeit hat, das zu bemerken." Die gefälschte URL ist dann aber wenige Sekunden später gut im Bild zu erkennen (Abbildung 1) und auch der Unterschied in der Darstellung des Sicherheitszertifikats sticht ins Auge. Birk bestätigt darin, dass man den erfolgreichen Angriff an der URL sehe. Der offensichtliche Widerspruch zwischen der behaupteten Unmöglichkeit der Unterscheidung und dem Hinweis auf den sichtbaren Unterschied wurde von den Journalisten nicht erkannt, nicht thematisiert und auch nicht aufgelöst. Das heisst, die falsche Behauptung von Volker Birk wurde kommentarlos verbreitet.

Nachgefragt via Twitter

Auf Twitter auf diese Fehlaussage hingewiesen, reagierte Volker Birk so:

Abbildung 2: Chatverlauf, Quelle: Twitter

Volker Birk findet, die gefälschte URL sei für Stimmbürger unauffällig und meint, die Umleitung an sich sei ja nicht verdächtig und antwortete auf Nachfrage mit einem Meme aus der Muppet-Show.

Tatsächlich wäre es möglich, dass zahlreiche unbedarfte Wähler die Umleitung und das Sicherheitszertifikat ignorieren. Aber sobald eines der beiden auch nur einem einzigen Wähler beim Befolgen der Anleitung auffällt, wird er dies dem Kanton mit hoher Wahrscheinlichkeit melden und eine Untersuchung des Betruges würde eingeleitet.

Aussagen zweier Experten verkürzt

Diese beiden Falschaussagen zum Fehlen von Schutzmassnahmen und zur Unmöglichkeit, den

Betrug zu erkennen, hätten den Fernsehredakteuren auffallen und die gesamte Stossrichtung des Berichts in Frage stellen müssen. Denn es mangelte auch nicht an Warnungen, den Befund vorsichtig zu interpretieren.

Neben der Genfer Staatskanzlei befragten die Journalisten in der Sendung auch Professor Eric Dubuis von der Berner Fachhochschule: Er bestätigte, dass der gezeigte Laborangriff technisch funktioniert, weist aber darauf hin, dass die Prüfcodes einer Manipulation der Stimme des Opfers einen Riegel schieben. Dass Dubuis auch darauf hinwies, dass der Angriff nicht flächendeckend skaliere und deshalb nicht überbewertet werden sollte, fand in der Sendung keinen Platz.

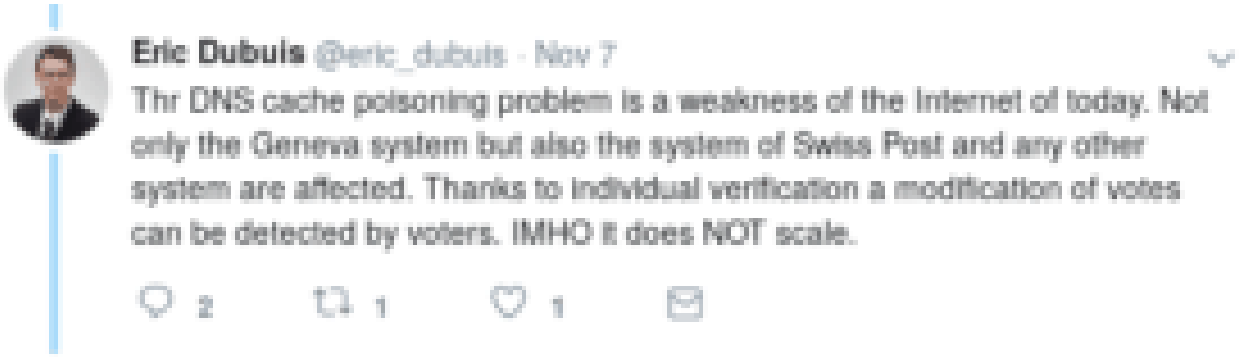


Abbildung 3: Prof. Eric Dubuis der Berner Fachhochschule: der Angriff skaliere nicht in die Breite (Quelle: Twitter)

Auch ein zweiter Fachhochschuldozent, Professor Peter Heinzmann von der Hochschule für Technik Rapperswil, wurde von den JournalistInnen befragt. Seine schriftliche Antwort liegt der Redaktion vor und weist ebenfalls darauf hin, dass es in der Fläche nicht funktionieren könne sowie die behauptete Manipulationsmöglichkeit nicht unter Beweis gestellt worden sei. Diese Warnungen schlug das Fernsehteam aber in den Wind und übernahm die Formulierungen derE-Voting-Kritiker des CCC. Darüber hinaus interpretierte es den erfolgreichen Laborangriff schwerwiegender als der CCC selbst. So wurde die Staatskanzlei des Kantons Genf in ausgesprochen schlechtem Licht dargestellt.

Fazit

Weshalb hier das Genfer E-Voting in seiner Gesamtheit als unsicher und manipulierbar präsentiert wurde, erschliesst sich mir nicht. Vermutlich war die Story "CCC-Hacker machen Beamte lächerlich" so knackig, dass man sie beim SRF nicht mehr aufgeben wollte.

Die NZZ reagierte rasch aber zurückhaltend auf die Enthüllungen des Fernsehens. Weitere Zeitungen brachten kleinere Meldungen. Sie blieben aber weit hinter den vollmundigen Anschuldigungen des Fernsehens zurück. Daher man darf annehmen, dass die Zeitungsredaktionen die Fehler erkannten, oder den vehementen E-Voting-Kritikern des CCC nicht mehr jede Behauptung abnehmen.

Damit ist der Sachverhalt an sich geklärt. Tatsächlich gibt es aber weitere Unstimmigkeiten in den Beiträgen, denn auch technisch ist nicht alles so einfach, wie es im Fernsehen gezeigt wurde. Und dann wären da noch die Optimierungen, von denen das E-Voting-System profitieren könnte. Diese Punkte werden hier detailliert besprochen.

Updates

Wir haben den mit * markierten Abschnitt über die Prüfcodes nach einem Hinweis unseres Lesers Danilo B. präzisiert.

Wir haben den mit ** markierten Satz über den Newsflash nach Massgabe des Autors präzisiert.