… Bundestagwahl 2017 ist sicher! ... Ist sie dass wirklich?

An einem schwülwarmen Donnerstagabend im Juli stellt sich Martin Tschirsich eine Frage, die für die Zukunft Deutschlands entscheidend ist: Kann die Bundestagswahl manipuliert werden? Die Wahlen sind sicher, heißt es, weil die Bürger ihr Kreuz auf einem Zettel machen. Aber den 29-jährigen Informatiker, der gerade seinen Master an der Uni Darmstadt macht, überzeugt das nicht. Tschirsich ist ein leiser Mensch, der schnell denkt und spricht. Abends sitzt er gern an dem Computer in seiner Dachgeschosswohnung und knobelt an Problemen herum.

Tschirsich googelt. So erfährt er, dass aus den Kreuzen auf den Stimmzetteln aus Papier im nächsten Schritt digitale Daten werden. Zwar sind Computer, bei denen das Kreuz an einem Bildschirm eingegeben wird, in Deutschland verboten. Aber das heißt nicht, dass Rechner bei Wahlen keine Rolle spielen. In den rund 70.000 Wahllokalen des Landes werden Wahlhelfer am Abend des 24. September von Hand die Stimmen auszählen und ihre Ergebnisse auf Zettel schreiben. Alles weitere jedoch läuft über Computer.

Tschirsich stößt bei seiner Suche im Internet schnell auf die Software, mit der die Wahldaten gesammelt und weitergeleitet werden. Es handelt sich um ein Programm namens PC-Wahl, nach Angaben des Herstellers "das meistgenutzte Wahlorganisationssystem in deutschen Verwaltungen". Tschirsich zerlegt es, testet die Abläufe – und er erkennt, dass er sie manipulieren kann. Er ist überzeugt: "Die Wahl ist nicht sicher. Sie kann gehackt werden."

Wenn in drei Wochen abgestimmt wird, dann geht es nicht nur um die Frage, wie der nächste Bundeskanzler oder die nächste Bundeskanzlerin heißen wird. Die Demokratie an sich steht auf dem Spiel. Die Bürgerinnen und Bürger bestimmen die Politik der kommenden vier Jahre, sie legitimieren das staatliche Gefüge des Landes. Schon der Verdacht, jemand könne Einfluss auf das Wahlergebnis nehmen, muss ausgeschlossen werden.

… Wahlen in Deutschland ließen sich nicht hacken, sagte der Bundeswahlleiter noch im Januar. ...

Man habe die Bundestagswahl technisch so abgesichert, "dass sie gegen alle Manipulationsversuche geschützt ist". Aber was ist, wenn das deutsche Wahlsystem doch Fehler hat? Wenn Martin Tschirsich Recht behält?

Selten zuvor haben die westlichen Demokratien so unter Druck gestanden wie derzeit – nicht nur von innen. **Auch die Bundesregierung fürchtet Manipulationsversuche**. Immerhin ist der russische Geheimdienst bereits in den Bundestag eingebrochen. Man sei darauf eingestellt, dass Gruppen aus anderen Ländern wie Russland versuchen könnten, sich einzumischen, sagte Bundesinnenminister Thomas de Maizière (CDU) unlängst bei der Vorstellung des Verfassungsschutzberichts. Und in einem internen Papier des Bundesinnenministeriums steht, es müsse "von einem Interesse insbesondere ausländischer staatlicher als auch nichtstaatlicher Akteure ausgegangen werden, Ablauf und Ergebnis in ihrem Sinne zu beeinflussen". Und weiter: "Cyberangriffe könnten darauf abzielen, Wahlergebnisse auf dem Übertragungsweg zu manipulieren, falsche Wahlergebnisse einzuschleusen oder die Übermittlung der vorläufigen Wahlergebnisse technisch zu unterbinden."

Eine manipulierte Wahl – für die Demokratie wäre das ein Desaster. Das findet auch Tschirsich, der erst aus Neugierde und dann aus Besorgnis die Wahlsoftware unter die Lupe nimmt. "Ich hatte ein komisches Gefühl dabei", sagt Tschirsich. Das Ganze erschien ihm nicht ganz so sicher, wie alle Beteiligten es versprechen.

Die Bundestagswahl ist im föderalen Deutschland dezentral organisiert. Die Ergebnisse werden vom Wahlbezirk zum Wahlkreis, dann an den Landeswahlleiter und von dort schließlich an den Bundeswahlleiter übermittelt. Die Verantwortung liegt bei den Ländern und sogar noch weiter unten: bei den Kommunen. Sie haben unterschiedliche Wahlsoftware angeschafft, mit der sie die Ergebnisse verwalten. Aber kein Programm ist so verbreitet wie PC-Wahl.

Tschirsich spielt den Wahlablauf am Beispiel Hessen durch, wo er lebt. Mit Google findet er Teile der Wahlsoftware, die nie hätten öffentlich werden sollen. Das Programm **PC-Wahl**, das es mittlerweile **seit 30 Jahren gibt**, wird normalerweise nicht an Privatpersonen verkauft, sondern nur an Kommunen. Die restriktive Vergabe soll das Programm vor Angriffen schützen.

Ingo Höft von der Piratenpartei in Rheinland-Pfalz klagte im Jahr 2009 sogar dagegen.

Er wollte den Quellcode von **PC-Wahl** sehen, um verstehen zu können, wie das Programm Ergebnisse berechnet. Jeder Wähler, jede Wählerin sollte nachvollziehen können, wie die Mehrheitsverhältnisse zustandegekommen sind.

Doch trotz dieses Transparenzgebotes habe nie eine offizielle Stelle den Quellcode von **PC-Wahl** gesehen oder gar zertifiziert, argumentierte Höft. Aber das Verwaltungsgericht Neustadt entschied, der Landeswahlleiter habe das ordnungsgemäße Funktionieren der Software geprüft, das genüge.

Tatsächlich haben die Wahlleiter landauf, landab nur **überprüft, ob die Software die Stimmen korrekt addiert**. Niemand interessierte sich bislang dafür, ob das Programm an sich angreifbar ist. Bis Tschirsich kam.

Das Passwort stand im Internet

Auf der Website der Herstellerfirma ist der Service-Bereich mit einem Passwort geschützt. Doch Tschirsich findet das Passwort im Internet, denn ein anderes Unternehmen, das PC-Wahl vertreibt, hat es versehentlich veröffentlicht. Die Firma ekom21 ist ein kommunaler IT-Dienstleister in Hessen, der als Vertriebspartner PC-Wahl verkauft. Auf der Webseite der ekom21 entdeckt Tschirsich eine Bedienungsanleitung für das Programm. Und in dieser Bedienungsanleitung stehen auch die Zugangsdaten zum internen Servicebereich des Herstellers von PC-Wahl: "Nutzername: service", "Kennwort: pcwkunde". Damit lädt sich Tschirsich wichtige Teile der Software runter. Nun kann der Informatiker wie ein Chirurg den Code der Software sezieren. Und entdeckt den nächsten gravierenden Fehler.

PC-Wahl ist im Kern eine Art Tabellenkalkulationsprogramm. Die Stimmen für jeden Kandidaten werden in Zeilen und Spalten summiert und die Ergebnisse in eine neue Datei geschrieben. Tschirsich analysiert die Struktur dieser Datei, die die Wählerstimmen enthält. Sie ist zu seiner Überraschung nicht eigens gesichert. Wenn PC-Wahl diese Datei an die Wahlleiter verschickt, gibt es keine Authentifizierung, keine Signatur, keinen einzigartigen Schlüssel. Es gibt kein System, das beweist, dass die korrekten Wahldaten der richtigen Gemeinde beim Wahlleiter ankommen. Somit ist es problemlos möglich, diese Wahldateien zu fälschen.

Gemeinden infizierte Software unterschieben

Tschirsichs nächste Entdeckung ist nicht weniger frappierend. Gemeinden, die das Programm nutzen, müssen es aktualisieren, beispielsweise, um die korrekten Vorlagen für die Bundestagswahl zu erhalten. Die neuen Programmversionen stehen bei der Herstellerfirma auf einer speziellen Seite, wieder ist sie durch ein Passwort geschützt. Und wieder findet Tschirsich dieses Passwort im Netz. Es lautet "ftp,wahl". Damit könnte er auf dieser Seite eine gehackte Version von PC-Wahl verstecken und Gemeinden würden sich diese dann, ohne es zu bemerken, beim Aktualisieren herunterladen. Das wäre kein Angriff auf die Wahlergebnisse eines einzelnen Wahlkreises mehr, es wäre ein Flächenbrand. Hacker könnten den Kommunen bundesweit falsche Ergebnisse unterjubeln.

Und das ist noch nicht das Ende der Probleme. In der Software sind die Vorgaben zur Übertragung der jeweiligen Auszählungen aus den Wahllokalen bereits vorinstalliert. Am Wahlabend werden die Stimmergebnisse in Hessen aus Sicherheitsgründen nicht über das Internet übertragen, sondern über ein internes Netzwerk, das eine Firma den Gemeinden zur Verfügung stellt. Doch der Einwahlpunkt in dieses Netzwerk, das eigentlich niemand kennen soll, ist in PC-Wahl bereits voreingestellt, damit die Beamten am Wahlabend weniger Arbeit haben. Es ist zwar durch ein Passwort geschützt, aber das Passwort für Hessen ist nicht sonderlich schwer zu erraten. Es lautet: "test".

Tschirsich weiß jetzt, wie die Software arbeitet und wie sie die Dateien erstellt, mit denen die Stimmverhältnisse weitergeleitet werden. Er kennt das interne Netzwerk, über welches diese Dateien in Hessen weitergeschickt werden. Und er hat einen Weg gefunden, viele Gemeinden mit einer infizierten Version der Software zu bestücken. Ihm genügt das als Beweis, dass das System gefährliche Lecks hat. Er kontaktiert **Gerhard Bennemann**.

Bennemann ist Gemeindewahlleiter der kleinen Stadt Büdingen im Wetteraukreis in Hessen, ein Mann mit kurzgeschnittenen, grauen Haaren, randloser Brille und aufmerksamen Augen, die derzeit etwas erschrocken blicken. Denn Tschirsich hat ihm an seinem Rechner vorgeführt, dass er die Wahlergebnisse von Büdingen verändern könnte, ohne dass Bennemann es beim Verschicken der Wahldaten merken würde.

"Es gibt bessere Passworte als 'test'"

Zögerlich räumt Bennemann die Fehler ein. "Es gibt bessere Passworte als 'test'", sagt er. "Das ist unangemessen." Und die Manipulation der Software sei "zumindest störend". Aber die Wahlergebnisse könnten jederzeit nachgeprüft werden, sie stünden letztlich noch immer auf Zetteln. "Das Endergebnis ist nichtsdestotrotz gesichert."

Das sagt auch Volker Berninger, der Entwickler von PC-Wahl. "Bei dem schlimmsten Szenario würde jemand damit Verwirrung stiften. Dann würden zwar irgendwelche falschen Ergebnisse im Internet stehen, aber auf dem Papier wären noch immer die richtigen vorhanden. Das gibt Ärger und Verwirrung, hat aber keine Relevanz."

Um das Vertrauen der Bürger in eine demokratische Wahl zu erschüttern, muss jedoch nicht unbedingt das Endergebnis gefälscht werden. Zweifel genügen. Angreifer könnten beispielsweise die verfälschten Ergebnisse übertragen und zugleich die Übertragung der richtigen Ergebnisse blockieren. Was würde etwa passieren, wenn mit dem vorläufigen Ergebnis am Wahlabend verkündet würde, die AfD sei an der Fünfprozenthürde gescheitert – dieses Ergebnis dann aber später korrigiert werden müsste, weil die AfD tatsächlich sieben Prozent der Stimmen bekommen hat? Wie verliefe dann die Diskussion in Deutschland? "Das wäre wahrscheinlich verhängnisvoll", sagt Bennemann, der Gemeindewahlleiter.

ZEIT ONLINE und DIE ZEIT haben Experten vom Chaos Computer Club (CCC) gebeten, die Qualität von PC-Wahl zu prüfen. Das Programm sei so schlecht, dass es "nie hätte eingesetzt werden dürfen", sagt Linus Neumann, einer der Sprecher des CCC. Neumann hat zusammen mit seinem Kollegen Thorsten Schröder das Programm begutachtet. PC-Wahl ignoriere grundlegende Prinzipien von Sicherheit und Verschlüsselung, urteilen sie.

Bundeswahlleiter und BSI sind alarmiert

PC-Wahl habe nicht nur die Zielserver für die Übermittlung der Ergebnisse am Wahlabend voreingestellt. Auch das Passwort, das benötigt wird, um sich auf dem Server der nächsten Ebene einzuloggen, liefere es gleich mit. Damit niemand Unbefugtes an diese Passwörter kommt, sind sie in PC-Wahl verschlüsselt gespeichert. "Ein normaler Mensch kann die nicht auslesen, denn ich habe einen eigenen Kompressionsalgorithmus gebaut, da braucht es schon viel Gehirnschmalz, um den zu knacken", sagt PC-Wahl-Entwickler Berninger. Dem CCC gelang dies mühelos. Berninger hatte nicht damit gerechnet, dass die Hacker eine Vollversion seines Programms finden würden.

"Das ist keine richtige Verschlüsselung, sondern nur eine Maskierung", sagt Linus Neumann vom CCC. Außerdem sei die Formel, nach der die Passwörter maskiert würden, ebenfalls in PC-Wahl enthalten.

Jeder, der Zugriff auf das Programm habe und die Verschlüsselung brechen könne,

bekomme damit auch Zugriff auf die Passwörter und könnte so manipulierte Wahldaten weiterschicken.

Neumann vergleicht die Logik des Programms mit einem Mietshaus, in dem alle Wohnungen das gleiche Schloss hätten. Die Wohnungen seien zwar abgeschlossen, aber da jeder Schlüssel in alle Schlösser passe, sei das nicht wirklich sicher.

Wahlhelfer sollen Ergebnisse von Hand prüfen

Und noch eine Schwachstelle hat der CCC entdeckt: PC-Wahl kann Dateien mit Wahlergebnissen für jedes Bundesland erzeugen, weil es in fast jedem Land irgendwo im Einsatz ist. Dadurch konnten die CCC-Analytiker ermitteln, wie die Dateien mit den Ergebnissen in den einzelnen Bundesländern aussehen müssen, um akzeptiert zu werden. Zusammen mit Tschirsichs Erkenntnissen ergibt sich daraus, dass Angreifer auch dort Wahlergebnisse fälschen könnten, wo PC-Wahl gar nicht im Einsatz ist – indem man die zu übermittelnden Dateien einfach imitiert.

Der Landeswahlleiter von Hessen hat, aufgescheucht durch Tschirsichs Recherche, eine Anordnung an alle Wahlhelfer erlassen. Sie sollen am 24. September sämtliche mit PC-Wahl übermittelten Ergebnisse nach dem Versenden auf der Webseite des Statistischen Landesamtes überprüfen, wo sie aufgelistet werden. Die Helfer sind angehalten, einen Ausdruck zu machen und diesen mit ihren Werten abzugleichen. Bei jeder Auffälligkeit sollen sich die Wahlhelfer telefonisch zu melden.

Auch auf Bundesebene sind die Behörden mittlerweile alarmiert. Am 28. Juli warnte das zuständige Bundesamt für die Sicherheit in der Informationstechnik (BSI) den Bundeswahlleiter. Der informierte alle Landeswahlleiter. "Die Verhinderung von Manipulationsmöglichkeiten der Schnellmeldungen und damit des vorläufigen Wahlergebnisses hat für den Bundeswahlleiter höchste Priorität", so ein Sprecher.

CCC hält Gegenmaßnahmen für wirkungslos

Berninger, der Erfinder von PC-Wahl, sagt, es werde in den nächsten Tagen eine aktualisierte Version des Programms geben. Die enthalte neue Sicherungsmechanismen. Der CCC hat auch diese neuen Sicherungen bereits analysiert. Sie ließen sich problemlos umgehen, heißt es in der schriftlichen Analyse des Clubs (Analyse einer Wahlsoftware, PDF). Angreifern würden sich bei der neuen Version beispielsweise "drei unabhängige triviale Wege" bieten, die nun installierte Verschlüsselung auszuhebeln. Das Fazit der CCC-Autoren: Sämtliche der nun hastig ergriffenen Gegenmaßnahmen "erwiesen sich bereits bei oberflächlicher Überprüfung als ungeeignet zur Beseitigung der gemeldeten Schwachstellen".

Auf die Frage, warum Sicherungsmechanismen nicht schon vor Jahren in die Software eingebaut worden sind, sagt Berninger, dafür sei von seinen Kunden "bisher kein Bedarf angemeldet worden". Auch eine umfassende Analyse und Zertifizierung des Programms habe es nie gegeben, räumt er ein.

Deutschland ist das Thema Wahlen bislang mit einer bemerkenswerten Unschuld angegangen.

Die Stimmauszählung erschien als handwerkliches Problem, kein sicherheitstechnisches,

und schon gar kein politisches.

Aber die Zwischenfälle in den USA und Frankreich, wo im Wahlkampf gehackte interne Dokumente von Hillary Clinton und Emmanuel Macron auftauchten, zeigen, welche Angriffspunkte die digitale Welt bietet. In den Amtsstuben von Gemeinden wie Büdingen hat daran bislang kaum jemand gedacht.

Wenn aber Martin Tschirsich und die Hacker vom CCC in der Lage sind, die in Deutschland eingesetzte Wahlsoftware zu knacken – dann können es Angreifer aus Russland ebenso.

Am Abend des 24. September wird Deutschland wohl wieder etwas analoger werden: Die Wahlleiter von Bund und Ländern haben sich vorsichtshalber auf "Meldeketten" verständigt, um die Ergebnisse persönlich übermitteln zu können. "Auf diese Meldeketten kann zurückgegriffen werden, wenn wider Erwarten die Probleme mit PC-Wahl nicht behoben werden können", heißt es beim Bundeswahlleiter. Meldeketten bedeuten: das gute, alte Telefon. Für den Technologiestandort Deutschland eine Blamage.

Demnächst soll PC-Wahl ausrangiert werden. Allerdings werden Computer damit nicht verbannt, die Software wird nur ersetzt. Tschirsich und die CCC-Hacker haben sich das Nachfolgeprogramm bereits angeschaut.

Sie sind sich sicher, darin jede Menge Sicherheitsprobleme entdeckt zu haben.

Kai Biermann *Redakteur im Ressort Investigativ/Daten, ZEIT ONLINE*

Systemvoraussetzungen nach der Homepage von ***PC-Wahl*:**

Notwendige Hard- und Software:

Betriebssystem	Windows Vista / Windows 7 / 8 / 10 (unter 32 Bit und 64 Bit Versionen nutzbar) Nutzung unter älteren Versionen (ab Windows XP) möglich, aber nicht empfohlen

© Juli 2017, **vote iT GmbH** - Kontakt - Impressum - Datenschutz

Von Syberangriffen am 12. Mai 2017 weltweit auf Windowssysteme noch nichts gehöhrt!!!

Urteil gegen Transparenz bei Wahlen ist gesprochen

Nach der mündlichen Verhandlung am **3. März 2010** gibt es nun das Urteil zur 1. Instanz:

Allein der Verlauf der mündlichen Verhandlung liess erwarten, dass die Klage abgewiesen wurde. Nach meiner natürlich parteiischen Einschätzung war der vorsitzende Richter der Sache gegenüber – als interessanten neuen Aspekt – recht aufgeschlossen.

Es gelang mir aber nicht, das Selbstverständnis der digitalen Generation zu verdeutlichen: ein Klick auf einen Link im Browser und man kann sich das Programm ansehen. Das war für die anwesenden Richter intuitiv völlig undenkbar. Als ich die Frage, wie ich das Quellprogramm denn veröffenlichen wolle, damit beantwortete, es einfach ins Internet zu stellen, war die allgemeine Reaktion ein verhaltenes Murmeln, Kopfschütteln und leichtes Gelächter, so als wäre das ein völlig unrealistischer Vorschlag. Man konnte sich das gar nicht vorstellen.

Auch ein beisitzender Richter hatte mehrfach deutlich und auch recht aggresiv zu verstehen gegeben, was ich denn überhaupt wolle. Durch die Prüfungen und Tests des Programms sei hinreichend sicher gestellt, das es richtig funktioniere.

Da bedürfe es keiner Einsichtnahme durch den Wahlberichtigten mehr. Auch hätte ich mir eine etwas andere Zusammensetzung der beisitzenden Richter gewünscht, denn unglücklicherweise gab es keinen offensichtlichen Vertreter der Internet-Generation. Im Prinzip hat man mein Anliegen gar nicht verstanden und immer darauf abgestellt, ich wolle die Fehlerfreiheit des Programms anzweifeln. Darum geht es mir aber allerhöchstens hilfsweise. Ich bin überzeugt, dass sich jeder Bürger das Programm anschauen darf, mit dem seine Stimmen gezählt werden.

2 A 10620/10.OVG
1 K 943/09.NW

EINGEGANGEN
27. DEZ. 2010
Rechtsanwälte

OBERVERWALTUNGSGERICHT RHEINLAND-PFALZ

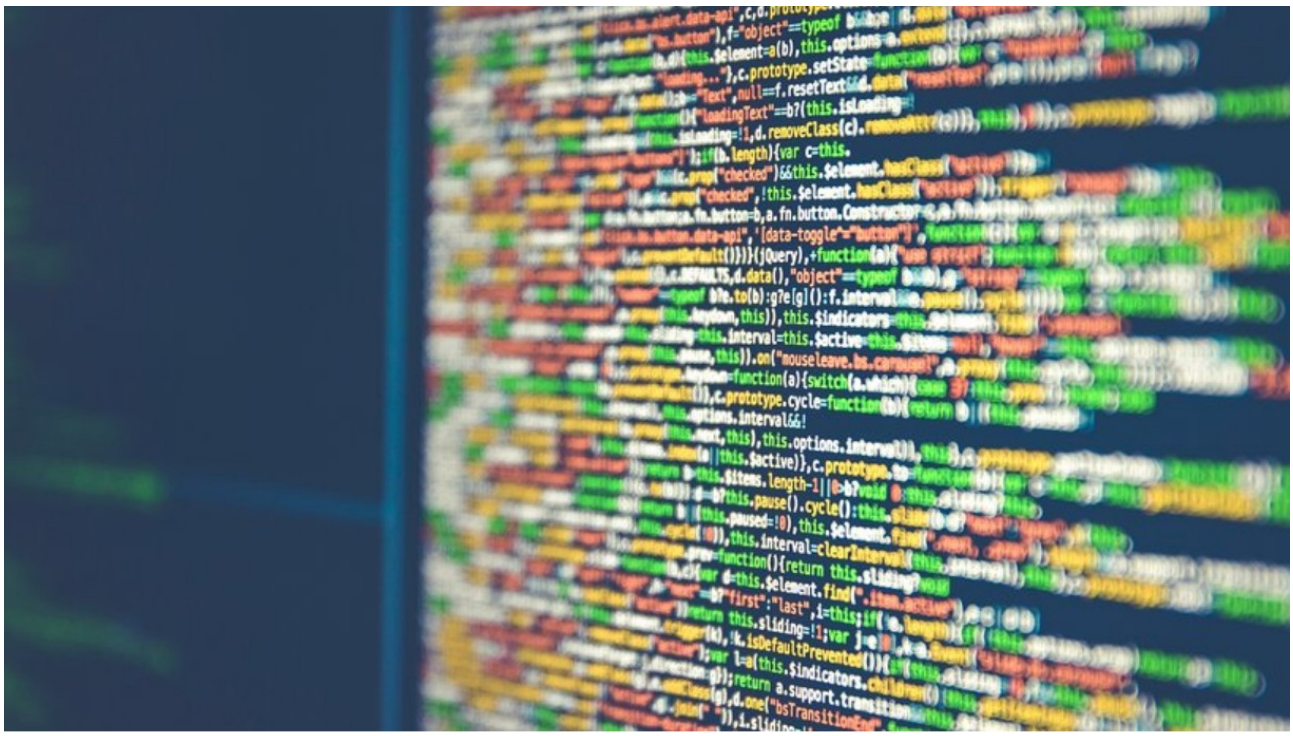
...

hat der 2. Senat des Oberverwaltungsgerichts Rheinland-Pfalz in Koblenz aufgrund der Beratung vom 17. Dezember 2010, an der teilgenommen haben

Präsident des Oberverwaltungsgerichts Prof. Dr. Meyer
Vorsitzender Richter am Oberverwaltungsgericht Stamm
Richter am Oberverwaltungsgericht Dr. Schumacher

beschlossen:

Der Antrag des Klägers auf Zulassung der Berufung gegen das Urteil des Verwaltungsgerichts Neustadt an der Weinstraße vom 3. März 2010 wird abgelehnt.



Die Öffentlichkeit sollte über Hacks und Schwachstellen informiert werden. © Markus Spiske/unsplash.com

PC-Wahl

Warum Hacks in die Öffentlichkeit gehören

Nach der Veröffentlichung von IT-Sicherheitslücken werden Hacker und Medien immer wieder gefragt, ob sie damit nicht Kriminellen helfen. Das Gegenteil ist der Fall.

Von **Patrick Beuth**

8. September 2017, 19:10 Uhr / 77 Kommentare

horsten Schröder vom Chaos Computer Club (CCC) weist auf Twitter darauf hin, dass er drei Werkzeuge veröffentlicht hat, mit denen sich die Schwächen in der Software PC-Wahl ausnutzen lassen, die bei der kommenden Bundestagswahl eingesetzt wird.

Zu den ersten Fragen, die der Sicherheitsforscher in so einem Fall immer zu hören bekommt, gehört diese: Warum machst du das? Bringst du andere damit nicht auf dumme Ideen?
Das ist auch dieses Mal so. Immerhin geht es um eine Software zur Übermittlung von Wahlergebnissen an die Landeswahlleiter, also letztlich um einen Weg, die Bundestagswahl zu stören. Der Informatiker Martin Tschirsich hatte im Juli entdeckt, dass sich PC-Wahl auf verschiedene Weise manipulieren lässt. Zusammen mit Schröder hat er die entsprechenden Anleitungen als Beispielcode geschrieben und ZEIT ONLINE hat darüber berichtet.

Die Wahl ist deshalb nicht an sich gefährdet, auch nicht die korrekte Auszählung der Stimmen. Sollte es jemandem gelingen, die elektronische Übertragung zu manipulieren, würde es Wahlhelfern und Wahlleitern auffallen. Aber im Extremfall könnte es eine Weile dauern, bis die richtigen Ergebnisse feststehen und so lange könnten sich die falschen verbreiten. Was sie angesichts der zahlreichen medialen und sonstigen Kanäle zweifellos tun würden. Das könnte das Vertrauen der Deutschen in die Integrität des Wahlsystems oder gar die Demokratie an sich beschädigen, was schlimm genug wäre.

Notwendiger Druck auf die Anbieter

Hackern wie Schröder und Tschirsich, aber auch Medien wie ZEIT ONLINE, die solche Schwächen offenlegen, wird immer wieder vorgeworfen, sie selbst setzten das Vertrauen der Bürger aufs Spiel. Ihnen wird unterstellt, andere durch ihre Veröffentlichungen zu kriminellen Handlungen anzustiften.

Solchen Vorwürfen tritt der CCC entgegen, aus drei Gründen: "Mit einem sogenannten *proof of concept* heben wir erstens die Problematik von der theoretischen auf eine praktische Ebene", sagt Schröder. "So können wir leichter belegen, dass unsere Behauptungen stimmen."

Das helfe zweitens den Herstellern der betroffenen Produkte, die Lücken nachzuvollziehen und zu schließen, sagt Linus Neumann, einer der Sprecher des CCC. Und drittens "erhöht es den Druck auf sie, endlich aktiv zu werden".

Abwiegeln, negieren, leugnen

Das ist nötig, wenn die Firmen nach der ersten, nicht öffentlichen Konfrontation erst einmal abwiegeln, negieren, leugnen. Wenn sie das Problem kleinreden oder gar nicht reagieren. Schröder kennt das aus Erfahrung: "Manche nehmen erst einmal eine Verteidigungshaltung ein."

Auch **vote iT**, der Hersteller von **PC-Wahl**, hat das versucht. Noch einen Tag vor der Veröffentlichung der ersten Medienberichte hatte die Firma in einer E-Mail an *Spiegel Online* behauptet, in PC-Wahl seien "sicherheitsrelevante Schwachstellen nicht vorhanden" und man habe auch keine entsprechenden Hinweise bekommen.

ZEIT ONLINE hatte den Entwickler und Co-Geschäftsführer Volker Berninger aber bereits am 27. Juli telefonisch auf die Sicherheitslücken angesprochen. Zu diesem Zeitpunkt hatte auch schon das Bundesamt für Sicherheit in der Informationstechnik (BSI) Kontakt zu vote iT aufgenommen.

"Security by obscurity" ist kein zeitgemäßes Konzept

Entscheidend ist, dass es eine solche nicht öffentliche Vorwarnung gibt. Im Bereich der IT-Sicherheit heißt das *responsible disclosure* – verantwortungsvolle Offenlegung. Wer Sicherheitslücken findet, informiert den Hersteller und gibt ihm Zeit, sie zu beheben. Erst danach geht er an die Öffentlichkeit.

Manchmal entscheiden sich die Entdecker von Schwachstellen für die schärfere Variante – *full disclosure* genannt. Sie wenden sich sofort an Medien und damit die Öffentlichkeit und zwingen das Unternehmen zum schnellen Handeln im Sinne der Kunden.

Alternativ verzichten sie auf eine Veröffentlichung und kassieren dafür eine Belohnung vom Hersteller, *bug bounty* genannt. Viele Technikunternehmen bieten so etwas an, wobei die Belohnung aus einer lobenden Erwähnung auf der Website bestehen kann oder aus mehreren Hunderttausend Dollar.

Auch nach den Updates waren nicht alle Schwächen beseitigt

Technik, die bei Wahlen eingesetzt wird, sollte in dieser Hinsicht transparent sein. Vertrauen in sie entsteht nicht durch Geheimhaltung des Quellcodes, das klammheimliche Beseitigen von Schwächen oder dadurch, sie nur zu kaschieren, sondern durch überprüfbare Verbesserungen. *Security by obscurity*, Sicherheit durch Verschleierung, ist kein zeitgemäßes Konzept.

Wie wichtig Transparenz im aktuellen Fall ist, beschreibt der CCC in seinem Untersuchungsbericht. Zwar seien die Schwachstellen auf Servern beseitigt und neue organisatorische Sicherheitsmaßnahmen für den Wahlabend vorgeschrieben worden. Aber "sämtliche durch mehrere Updates vorgenommenen technischen Gegenmaßnahmen in der Software selbst erwiesen sich bereits bei oberflächlicher Überprüfung als ungeeignet zur Beseitigung der gemeldeten Schwachstellen". Wenn der CCC also die entsprechenden Werkzeuge zur Verfügung stellt, können technische versierte Anwender selbst überprüfen, ob der Hersteller angemessen reagiert hat.

Natürlich profitieren Hacker und Medien von der Aufmerksamkeit, die sie für ihre Funde und Berichte erhalten. Den größeren Nutzen aber hat die informierte Öffentlichkeit.

31. März 2017: Brad Smith auf der RSA-Konferenz 2017

Unsere **Daten in den Netzen** sind in Gefahr durch (kriminelle) **Hacker**(gruppen) und durch staatliche **Überwachungsmaßnahmen** von Geheimdiensten. Sie können abgeschöpft und in vielfältiger Weise missbraucht werden.

Gefährdet sind dabei nicht nur die persönlichen Daten, sondern auch Steuerungsdaten in den Infrastrukturnetzwerken, im Internet der Dinge.

Es gab Einbrüche auch in Hochsicherheitsnetzwerke und personenbezogene Daten wurden millionenfach entwendet.

In der **Europäischen Union** gelten vergleichsweise hohe **Sicherheitsstandards**, höher als in den **USA**. Alle Daten, die wir in die Netzwerke der großen US-Internetkonzerne (**Amazon, Apple, Facebook, Google, Microsoft, Yahoo**…) eingeben, werden in den USA gespeichert oder unterliegen zumindest US-amerikanischer Gesetzgebung.

Deshalb musste das **Safe-Harbor-Abkommen** mit den USA, das den Datentransfer in die USA regelte, nachgebessert werden. Auch das neue **EU-US-Privacy-Shield** wurde von Datenschützern gleich als unzureichend charakterisiert. Und seit der Amtsübernahme von Donald Trump in den USA haben die Sicherheitsbedenken weiter zugenommen.
Während allgemein große Ratlosigkeit herrscht, geht der US-IT-Riese Microsoft in die Offensive. Anfang des Jahres wurde die **Microsoft Cloud Deutschland** gestartet. Das Besondere daran: Alle Daten werden in sicheren Rechenzentren in Deutschland und mit Datentreuhänderschaft durch die deutsche Telekom-Tochter **T-Systems** gespeichert. Dadurch soll verhindert werden, dass US-Behörden per Gerichtsbeschluss doch noch Zugriffsrechte auf die Daten erzwingen könnten.

Microsoft war – wie mehrere andere große US-Internetkonzerne – durch die **Snowden**-Enthüllungen des **PRISM-Programms** Mitte 2013 in Verruf gekommen, den US-Geheimdiensten Zugang zu personenbezogenen Daten der Nutzer zu geben. Jetzt legt sich der Konzern auch mit der US-Justiz an und Microsofts Präsident und Chefjurist **Brad Smith** startete weltweit eine Initiative, die unsere Daten und unser Leben sicherer machen soll:


ZEIT ONLINE

Suche

Politik Gesellschaft Wirtschaft Kultur ▾ Wissen **Digital** Campus ▾ Karriere Entdecken Sport ZEITmagazin mehr ▾

Hack der Bundestagswahl

Das Vertrauen in die Demokratie wird fahrlässig gefährdet

Die Bundestagswahl kann gehackt werden. Das liegt an einer Mischung aus Naivität und Ignoranz. Nicht einmal die Wahlsoftware selbst entspricht dem Stand der Technik.

Ein Kommentar von **Kai Biermann**

7. September 2017, 12:52 Uhr / 308 Kommentare

> Um die Bürger im digitalen Zeitalter zu schützen, müssen wir über die Aufgaben der Nationalstaaten hinausschauen.

Kai Biermann *Redakteur im Ressort Investigativ/Daten, ZEIT ONLINE*

Abgestimmt wird auf Papier. Aber danach gibt es ein Problem.

Freie und geheime Wahlen, in denen jede Stimme gilt und transparent gezählt wird – sie sind das Herz der Demokratie.

Wenn Bürger dem Wahlergebnis nicht trauen, dann vertrauen sie auch den Gewählten nicht. Die Wahl zu schützen, muss deshalb das höchste Ziel all derer sein, die für ihren Ablauf verantwortlich sind.

Seit Monaten behaupten alle zuständigen Behörden, die Bundestagswahl sei sicher. Denn anders als in den USA würden Wähler ihr Kreuz hierzulande auf einem Wahlzettel aus Papier machen. Das könne niemand in großem Stil fälschen.

Doch wer so argumentiert, denkt nicht weit genug. Die Kreuze selbst sind sicher. Aber was geschieht, nachdem die Stimmzettel ausgezählt werden?

Die Ergebnisse der Auszählung werden noch im Wahllokal in Computer eingegeben und per Software an die Landeswahlleiter übertragen. Dort werden sie zusammengerechnet und an den Bundeswahlleiter weitergeschickt. So entsteht das Ergebnis, das den Bürgern später als Ausgang der Bundestagswahl präsentiert wird und auf das sie vertrauen. Auf seiner Grundlage werden ein neues Parlament und eine neue Regierung gebildet.

Doch die Übertragungssoftware ist angreifbar. Ein 29 Jahre alter Informatiker aus Darmstadt hat das gerade bewiesen. Hacker hätten sie knacken, hätten Stimmen verändern und so Misstrauen gegen die Wahl säen können. Zwei Analytiker des Chaos Computer Clubs haben diese Ergebnisse bestätigt und weitere Schwachstellen entdeckt. Die in Deutschland am weitesten verbreitete Wahldatensoftware namens **PC-Wahl** ist so leicht zu manipulieren, dass ihr Einsatz geradezu fahrlässig erscheint.

"Gut geschützt" gegen Hacker? Nein

Getestet wurde das Programm oft. Die zuständigen Kommunen und Wahlleiter, die Statistischen Landesämter und Innenministerien haben jedoch nur geprüft, ob es die Stimmen richtig zählt. Die Frage, ob es technisch sicher ist, ob es gehackt werden kann, ob Mehrheiten verändert werden können, hat sie nie interessiert.
Selbst als im vergangenen Jahr bei den Abstimmungen in den USA, in Frankreich und in den Niederlanden aller Welt klar wurde, dass es Kräfte gibt, die versuchen, Wahlen zu manipulieren, wurde die deutsche Wahlsoftware nicht gründlich untersucht.

Noch im Januar 2017 sagte der Bundeswahlleiter, alles sei sicher, die Bundestagswahl sei "gut geschützt" gegen Hackerangriffe.

Erst jetzt, da jemand den Behörden die Unsicherheit ihrer Computersysteme vor Augen führt, rühren sie sich.

Als das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Bundeswahlleiter von den Sicherheitsmängeln erfuhren, entfalteten sie endlich fieberhafte Tätigkeit.

Ob die Wahl nun sicherer ist? Wohl nicht. Denn die Änderungen, die hastig an der Software vorgenommen wurden, lassen sich ebenfalls knacken. Auch das haben der Informatiker aus Darmstadt und die beiden CCC-Analysten bewiesen.

Doch statt den Warnern nun Orden zu verleihen, wurden sie bedroht. Ein Statistisches Landesamt dachte laut darüber nach, sie wegen Eindringens in IT-Systeme anzuzeigen.

Verstoß gegen das IT-Sicherheitsgesetz

Dabei sind es die Betreiber der Computersysteme, die eigentlich angezeigt werden müssten. Haben sie mit ihrem Verhalten doch gegen das IT-Sicherheitsgesetz verstoßen. Das seit 2015 geltende Gesetz schreibt vor: **"Betreiber kritischer Infrastrukturen sind verpflichtet, (…) angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, (…) zu treffen."** Dass die Technik der Bundestagswahl eine kritische Infrastruktur ist, wird niemand bezweifeln.

Das Gesetz fordert, solche Sicherungsmaßnahmen müssten dem Stand der Technik entsprechen. Doch nicht einmal die Wahlsoftware selbst entspricht dem Stand der Technik. "Oldtimer" nennt sie der Chaos Computer Club.

Statt offensiv für die Sicherheit dieser Infrastruktur zu sorgen, überließ man es den einzelnen Städten und Gemeinden, diese Technik zu installieren. Jede Kommune muss für sich entscheiden, welche Software sie anschafft und wie viel Geld sie dafür ausgeben will. In manchen Ländern helfen die Statistikbehörden dabei, eine Lösung zu finden, in anderen nicht. In manchen werden die Wahlprogramme selbst programmiert, in anderen werden sie von landeseigenen Firmen entwickelt oder von externen Unternehmen gekauft. **Es gibt nicht einmal Vorgaben, wie gründlich solche Programme getestet und zertifiziert werden müssen**. Auch keine Vorschrift, die fordert, dass unabhängige Stellen die Programme überprüfen müssen. Am Ende lautet dann das Passwort, dass die Systeme schützen soll, so wie in Hessen **"test"**.

Diese Ignoranz setzt sich immer noch fort. In den Niederlanden gab es 2016 ähnliche Sicherheitsmängel bei der dort verwendeten Wahlsoftware namens IVU.elect. Die niederländische Regierung hatte das Programm daraufhin aus dem Verkehr gezogen und seinen Einsatz bei Wahlen verboten. In Deutschland aber wird IVU.elect bei der Bundestagswahl trotzdem zum Einsatz kommen. Das Land Brandenburg nutzt es, um seine Ergebnisse an den Bundeswahlleiter zu schicken.


ZEIT ONLINE

Suc

Politik Gesellschaft Wirtschaft Kultur ▾ Wissen Digital Campus ▾ Karriere Entdecken Sport ZEITmagazin mehr

Zitis

Bundeshacker im Verzug

Die staatliche Forschungsstelle für Überwachungstechnik, Zitis, wird nicht wie geplant jetzt eröffnet. Für die IT-Sicherheit ist jede Verzögerung ein gute Nachricht.

Ein Kommentar von Patrick Beuth

30. August 2017, 16:12 Uhr / 35 Kommentare

Patrick Beuth
Redakteur im Ressort Digital, ZEIT ONLINE

Die Selbstbeschreibung ist ein Euphemismus: "ein Start-up für Experten" will die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (Zitis) sein, so steht es auf zitis.bund.de – tatsächlich wird sie die Heimat der Bundeshacker. Zitis soll dem Bundeskriminalamt, der Bundespolizei und auch dem Bundesamt für Verfassungsschutz neue Werkzeuge liefern, mit denen die Behörden abhören und überwachen können, was auf klassischem Weg über die Telefonnetzbetreiber nicht länger abhörbar ist: Handygespräche zum Beispiel über Skype, Chats, Kurznachrichten. Eben alles, was verschlüsselt wird, sodass es nur noch auf den Geräten von Sendern und Empfängern entziffert werden kann.
Am heutigen Mittwoch sollte die "Forschungs- und Beratungsinstanz für technische Lösungen mit Cyberbezug" offiziell eröffnet werden. Doch Bundesinnenminister **Thomas de Maizière**, der Zitis per Dekret geschaffen hat, musste seine Teilnahme "aus terminlichen Gründen" kurzfristig absagen, weshalb die Veranstaltung verschoben wird. Der Minister kommt stattdessen am 14. September, kurz vor Ende des Wahlkampfs, in dem Innere Sicherheit ein wichtiges Thema ist.

Erst 17 von 120 Stellen besetzt

Der Verzug passt zur Geschichte von Zitis: Von den für dieses Jahr geplanten 120 Stellen sind laut Bayerischem Rundfunk bisher 17 besetzt, daher auch die vielen Stellenausschreibungen. 400 Stellen sollen es mal werden. Wie viele der dringend gesuchten Experten angesichts des staatlichen, aber eher nicht stattlichen Lohns die Arbeit für Zitis einem Job in der freien Wirtschaft vorziehen werden, ist jedoch fraglich. Ob altbackene Formulierungen wie "Wir suchen Q, nicht 007 (…) Sind Sie aus diesem Holz geschnitzt?" da helfen, ebenfalls. Aber jede noch so kleine Verzögerung ist aus defensiver Sicht eine gute Nachricht.

Denn wenn die Forschungsstelle irgendwann den Regelbetrieb aufnimmt, wird sie eine von vielen Institutionen weltweit sein, die systematisch nach Schwachstellen in jener Technik suchen, die Millionen von Menschen täglich benutzen. Sie sticht nur deshalb hervor, weil sie vom Bund finanziert wird, so wie die Operational Technology Division des FBI in den USA. Die meisten anderen derartigen Einrichtungen sind privatwirtschaftlich organisiert und gewinnorientiert. Sie verdienen mit dem Entdecken und dem Verkauf von Sicherheitslücken ihr Geld, weil das einträglicher ist, als sie dem jeweiligen Hersteller zu melden. Der zahlt im besten Fall eine einmalige Belohnung (*bug bounty* genannt), während jeder einzelne Käufer bezahlen muss, um das Wissen um die Lücke offensiv auszunutzen.

Um welche Summen es geht, hat kürzlich die aktualisierte Liste des Händlers Zerodium offenbart. Das Unternehmen will Hackern für bisher unbekannte Sicherheitslücken sowie Werkzeuge, um diese auszunutzen (*exploits*), bis zu 1,5 Millionen US-Dollar zahlen.

Interessant ist aber vor allem eine andere Zahl: Bis zu 500.000 Dollar bietet Zerodium für Exploits gegen WhatsApp, Telegram, Signal und andere Messenger-Apps mit zumindest optionaler Ende-zu-Ende-Verschlüsselung.

Das ist mehr als für einen Hack gegen Windows 10 und jedes andere Desktop- oder Serverprodukt. Das Eindringen in mobile Geräte ist mittlerweile wichtiger. Zu den Endabnehmern gehören Strafverfolger und Geheimdienste in aller Welt – nicht nur in Demokratien – und möglicherweise organisierte Verbrecher.

Der Bundesinnenminister und seine Länderkollegen sowie die Strafverfolger und Nachrichtendienste argumentieren, es sei notwendig, auf diesem Markt für IT-Unsicherheit mitzumischen. Andernfalls könne man Kriminelle und Terrorverdächtige nicht mehr abhören, denn WhatsApp und andere Verschlüsselungsdienste könnten die schließlich alle problemlos bedienen. Anders gesagt: Die Leitungen transportieren häufig nur noch unbrauchbare Daten, also sind die Endgeräte das neue Ziel.

Sicherheitslücken geheim halten – und das Beste hoffen

Gleichzeitig behaupten die Bundesregierung, das Thema IT-Sicherheit "zur Chefsache" gemacht zu haben. In ihrer Digitalen Agenda steht zum Beispiel, Deutschland solle Verschlüsselungsstandort Nummer eins in der Welt werden und die Verschlüsselung von privater Kommunikation "zum Standard". Im Entwurf zur Cybersicherheitsstrategie der Bundesregierung ist das so zusammengefasst: "Die deutsche Kryptostrategie umfasst Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung."

Auflösen kann diesen Widerspruch niemand. Würden die Bundeshacker ihre Erkenntnisse sofort mit den betroffenen Herstellern und Anbietern teilen, könnten diese ihre Schwachstellen ausbessern und Millionen von Nutzern schützen – vor wem auch immer. Stattdessen sollen sie Angriffswerkzeuge für die deutschen Behörden entwickeln und dabei in Kauf nehmen, dass andere die gleichen Angriffspunkte finden und ebenfalls ausschließlich zur Überwachung von Menschen einsetzen, die man in freiheitlichen Gesellschaften als kriminell bezeichnen würde.

Zitis ist – neben einem inhaltlich vergleichbaren Programm des Bundesnachrichtendienstes – der Beleg dafür, dass die Bundesregierung in letzter Konsequenz Innere Sicherheit und IT-Sicherheit für Gegensätze hält.

Bundesüberwachungsminister Thomas de Maizière © Steffi Loos/Getty Images