Zeitschrift für Datenrecht und Informationssicherheit

digma

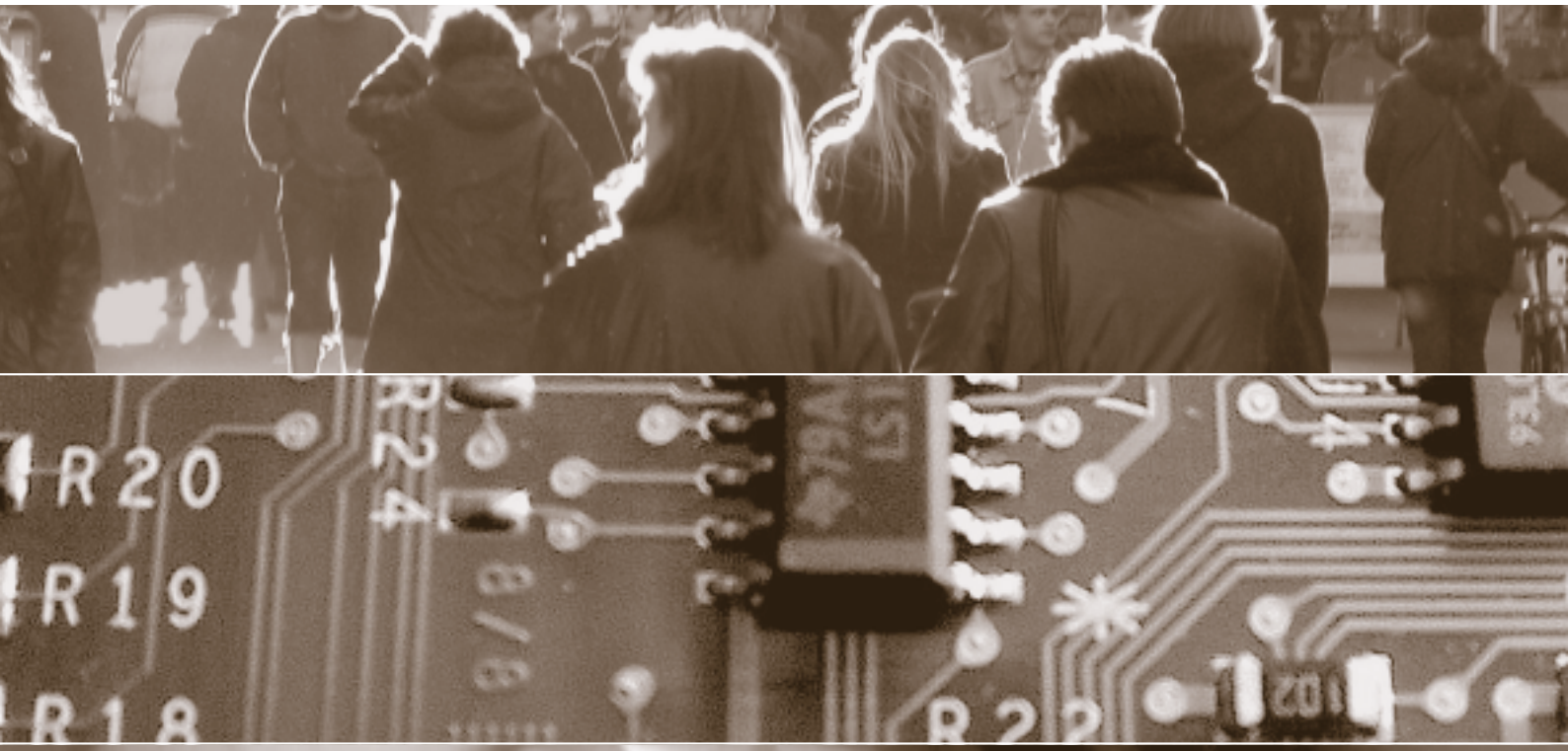
www.digma.info

8. Jahrgang, Heft 2, Juni 2008

Schwerpunkt:

Wirkung und Evaluation

fokus: Die Wirksamkeit von Datenschutzbehörden
report: E-Voting auf unsicheren Client-Plattformen
forum: Handlungsbedarf nach der Schengen-Evaluation



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth

Schulthess §

fokus

Schwerpunkt:
Wirkung und Evaluation

Zur Evaluation von Gesetzen

Dass der Gesetzgeber nicht nur Gesetze erlassen, sondern sich auch mit den erwünschten und erzielten Wirkungen auseinandersetzen soll, tönt banal – und ist doch erst eine jüngere Entwicklung. Der Autor verschafft einen Überblick über die verschiedenen Facetten der Gesetzesevaluation.

Die Wirksamkeit der Datenschutzbehörden

Die Wirksamkeit der Datenschutzbehörden ist ein Schlüsselfaktor zur Verwirklichung der Datenschutzanliegen in unserer Gesellschaft. Ihre Effizienz und Effektivität ist deshalb öffentlich zu thematisieren.

Datenschutzevaluation im Unternehmen

Die Erfahrungen mit dem vor zehn Jahren bei der Deutschen Telekom-Gruppe eingeführten Audit zeigen, dass es mit vertretbarem Aufwand möglich ist, in einem grossen Unternehmen ein Organisations-Datenschutzaudit flächendeckend durchzuführen.

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer, J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Rubrikenredaktor: Dr. iur. Amédéo Wermelinger

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Kirschgartenstrasse 7, CH-4010 Basel
Tel. +41 (0)61 270 17 70, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 112.00 (inkl. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Publicitas Publimag AG, Mürtschenstrasse 39, Postfach, CH-8010 Zürich
Tel. +41 (0)44 250 31 31, Fax +41 (0)44 250 31 32, www.publimag.ch, service.zh@publimag.ch

Herstellung: Schulthess Druck AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 99, Fax +41 (0)44 200 29 98, www.schulthess.com, zs.verlag@schulthess.com

E-Voting auf unsicheren Client-Plattformen

In der Schweiz wird E-Voting im Sinne von «Remote Internet Voting» vorangetrieben. Das Problem der unsicheren Client-Plattformen ist dabei nach wie vor ungelöst. Die Malware-basierten Angriffe, die sich zurzeit gegen Internet-Banking-Lösungen richten, können grundsätzlich auch gegen E-Voting-Lösungen eingesetzt werden.

Le PFPDT et la mise en œuvre de Schengen

Im März 2008 wurde im Hinblick auf die Schengen-Assoziierung der Datenschutz von Bund und Kantonen von einem EU-Evaluationskomitee evaluiert. Angesichts der daraus resultierenden Empfehlungen plant der EDÖB in Zusammenarbeit mit den kantonalen Datenschutzbehörden verschiedene Kontroll- und Informationstätigkeiten.

Sicherheits-Check für Protokolle

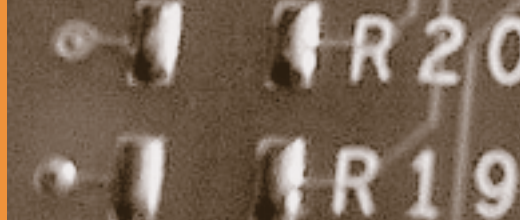
Bei der Programmierung fehlt heute oft die Zeit, die Protokolle gründlich «auf Herz und Nieren» zu prüfen. Kann diese Aufgabe durch andere Programme übernommen werden? Der Autor stellt die laufende Forschung in diesem Bereich vor.

Handlungsbedarf nach Schengen-Evaluation

PRIVATIM, die Vereinigung der schweizerischen Datenschutzbeauftragten, zeigt auf, welcher Handlungsbedarf sich bei den Datenschutzaufsichtsbehörden aus den Empfehlungen des EU-Evaluationskomitees ergibt.

report

forum



Sicherheit beim E-Voting

E-Voting auf unsicheren Client-Plattformen

Prof. Dr. Rolf Oppliger, Informatikstrategieorgan Bund ISB, eSECURITY Technologies und Universität Zürich*
rolf.oppliger@esecurity.ch

Im Artikel «E-Voting sicherheitstechnisch betrachtet» (digma 2002, 184 ff.) hat der Autor verschiedene Sicherheitsfragen und -probleme rund um elektronische Abstimmungsmechanismen, insbesondere im Hinblick auf das «Remote Internet Voting» aufgegriffen und zur Diskussion gestellt. Bei dieser in der Schweiz primär interessierenden Form des E-Voting gibt der stimmberechtigte Bürger seine Stimme auf seinem Personal Computer (PC) ab und die Stimme wird dann über das Internet zum eigentlichen Abstimmungsserver übertragen und dort ausgewertet bzw. verbucht. Die Sicherheitsfragen und -probleme betreffen

- die Autorisation der stimmberechtigten Personen,
- die Authentifikation der Abstimmungsserver,
- die Sicherheit der Kommunikationsbeziehungen,
- die unsicheren Client-seitigen Plattformen,
- das verteilte Auszählen der Ergebnisse, sowie
- die fehlende Nachvollziehbar- und Beweisbarkeit (die sich aus dem Abstimmungsgeheimnis ergibt).

Die Ausführungen haben gezeigt, dass mit unterschiedlicher Dringlichkeit und Kritikalität alle Sicherheitsfragen und -probleme angegangen und beantwortet werden müssen, dass aber das Problem der unsicheren Client-Plattformen – insbesondere in Kombination mit der fehlenden Nachvollziehbar- und Beweisbarkeit – besonders kritisch und politisch brisant ist. An dieser Situation hat sich nichts Grundlegendes geändert. Ganz im Gegenteil: Das Problem hat sich verschärft und hat heute durchaus das Potenzial, sich zu einem «Show Stopper» für das Remote Internet Voting zu entwickeln.

Problem der unsicheren Client-Plattformen

Das Problem der unsicheren Client-Plattformen besteht darin, dass die Client-seitig eingesetzten Plattformen aus handelsüblichen PCs, PC-Betriebssystemen und Web-Browsern bestehen, und dass diese Plattformen «Software-offen» und damit im Prinzip fast beliebig funktional erweiterbar bzw. manipulierbar sind. Manipulationen sind meist durch Malware (Schadsoftware) verursacht, wobei es sich dabei um Software mit verdeckter Funktionalität (im Sinne eines Trojanischen Pferdes) und/oder Autoreproduktionsfähigkeit (im Sinne eines Computervirus oder -wurms[1]) handeln kann. Um einen PC mit Malware zu infizieren, reicht es in der Regel aus, dass ein Benutzer einen Mail-Anhang anklickt und ausführt (z. B. getarnt als PDF-Datei), ein manipulatives Plug-in oder eine andere Browser-Erweiterung installiert oder eine speziell präparierte Web-Seite besucht (sogenannte «Drive-by»-Infektion). Im letzten Fall muss der Angreifer eine Verwundbarkeit oder einen Programm(ier)fehler im Browser ausnutzen, um über aktive Inhalte die Malware zu installieren und zur Ausführung zu bringen. In allen Fällen liegt am Schluss ein Client-System vor, das vom Angreifer manipuliert ist und im Namen des Benutzers beliebige Aktionen vornehmen kann. Zum Beispiel kann es eine bestimmte Stimme abgeben oder die vom Benutzer abgegebene Stimme vor ihrer Übertragung verändern. Der Angreifer hat über die vom Benutzer abgegebene Stimme im Extremfall die volle Kontrolle.

Das Problem der unsicheren Client-Plattformen gilt nach wie vor. Aus einem ganz anderen Bereich haben wir Evidenz für dessen Tragweite erhalten: Gemäss Holderegger (2008) erleben wir im Internet-Banking seit längerer Zeit grossangelegte Malware-Angriffe, die gezielt und in Echtzeit versuchen, Transaktionen von Bankkunden zu manipulieren. Die Angriffe nutzen die unsicheren Client-Plattformen aus, um Internet-Banking-Anwendungen anzugreifen und deren Sicherheitsmechanismen auszuhebeln. Die

gleichen, beim Internet-Banking erfolgreichen Angriffsvektoren können auch genutzt werden, um die Stimmabgabe eines elektronischen Urnenganges zu manipulieren. Keine Benutzerauthentifizierungs- oder Datenverschlüsselungstechnologie kann das verhindern; die Angriffe finden nach der Benutzerauthentifizierung bzw. vor der Datenverschlüsselung statt.

Leider muss man heute davon ausgehen, dass das Manipulieren von Client-Systemen, die für E-Voting genutzt werden, eher noch einfacher ist als das Manipulieren von für das Internet-Banking genutzten Client-Systemen. Dafür gibt es mindestens vier Gründe:

- Aus politischen Inhalten können «Cover Stories» konstruiert werden, auf die tendenziell nur bestimmte Bevölkerungsschichten ansprechen. Damit lassen sich Angriffe besser platzieren und zielgerichteter ausführen.
- Benutzer erleiden bei E-Voting-Manipulationen keinen finanziellen Verlust. Diese Tatsache ist nicht geeignet, die Benutzer zu einem sicherheitsbewussteren Umgang anzuregen.
- Zudem haben im Gegensatz zum Internet-Banking im E-Voting Benutzer in der Regel keine Möglichkeit, ihre Stimme zu überprüfen und damit einen Betrug zu erkennen.
- Schliesslich stellt im Internet-Banking der genügend schnelle Abtransport der Gelder aus der Sicht der Angreifer das hauptsächliche Problem dar (und nicht die Erstellung der Malware). In grosser Zahl müssen «Finanzagenten» rekrutiert werden, die ihre Bankkonti für illegale Transaktionen zur Verfügung stellen. Im E-Voting sind die Angreifer auf keine Finanzagenten angewiesen (weil es keine Gelder abzutransportieren gibt), und diese Tatsache vereinfacht die Situation aus Angreifersicht erheblich.

Vor diesem Hintergrund muss (leider) davon ausgegangen werden, dass Client-seitige Angriffe auf E-Voting-Systeme heute möglich und technisch relativ einfach zu realisieren sind. Das entsprechende Fachwissen ist ebenso verfügbar wie entsprechende Werkzeuge und Tools. Zum Beispiel liesse sich jedes System eines Botnet so manipulieren, dass damit das Abstimmverhalten des jeweiligen Benutzers kontrolliert wird. Diese Erkenntnis hat Ron Rivest anlässlich eines letztjährigen Seminars zum Thema «Frontiers of Electronic Voting» bewogen, von Botnets als der potentiell grössten Wählergruppe zu sprechen. Man bedenke, dass es Botnets gibt, die mehr als eine Million kompromittierter Systeme umfassen, dass es sich bei diesen Systemen meist um Heim-PCs handelt, und dass gerade diese PCs auch für das E-Voting benutzt werden. Insofern ist die Aussage von Ron Rivest berechtigt, auch wenn sie natürlich pointiert formuliert ist und die Botnet-PCs über verschiedene Länder verteilt sind.

Dass Client-seitige Angriffe auf E-Voting-Systeme (wenigstens in der Schweiz) noch nicht stattgefunden haben, ist wohl weniger darauf zurückzuführen, dass sie nicht möglich sind als vielmehr darauf, dass das E-Voting – im Gegensatz zum Internet Banking – kein finanziell attraktives Angriffsziel darstellt. Dies gilt namentlich auch für die Schweiz mit ihrer direkten Demokratie, in der es kaum eine einzelne Abstimmung oder Wahl gibt, die die politische Richtung für Jahre prägt. Einzelne Sachfragen können immer vor die Stimmbürgerinnen und Stimmbürger getragen werden. Nichtsdestotrotz beginnen Internet-Kriminelle ihre Aktivitäten sukzessive auch auf andere Anwendungen und Zielgruppen auszuweiten. Nach dem Internet-Banking ist z. B. gemäss Hoglund und McGraw (2007) die Welt der Online-Spieler in das Visier der Angreifer gerückt, und insofern ist es wohl nur eine Frage der Zeit, bis dies auch für das E-Voting geschieht.

«Bis-heute-ist-nichts-passiert»-Argument

In Sicherheitsdiskussionen wird leider oft von fehlenden Angriffen bzw. Angriffsversuchen auf die Sicherheit eines Systems geschlossen. Dieser Schluss ist falsch und trügerisch. Die Tatsache, dass ein System in der Vergangenheit nicht angegriffen worden ist, bedeutet nicht, dass es notwendigerweise sicher ist, sondern nur, dass kein Angreifer den

Kurz&bündig

In der Schweiz wird E-Voting im Sinne von «Remote Internet Voting» vorangetrieben und z. B. in den Kantonen Genf, Neuenburg und Zürich pilotiert. Das Problem der unsicheren Client-Plattformen ist dabei nach wie vor ungelöst. Die Malware-basierten Angriffe, die sich zurzeit gegen Internet-Banking-Lösungen richten, können grundsätzlich auch gegen E-Voting-Lösungen eingesetzt werden. «Code Voting» stellt eine konzeptionell einfache Möglichkeit dar, um das Problem der unsicheren Client-Plattformen anzugehen. Mithilfe von «CAPTCHA-basiertem Code Voting» kann zudem die Benutzerschnittstelle vereinfacht werden. Alternative Ansätze und Ausgestaltungen sind gefragt, um das Problem der unsicheren Client-Plattformen zu lösen.

erforderlichen Aufwand getrieben hat.

Stellen Sie sich in Analogie vor, Sie würden jeweils am letzten Tag jedes Monats einen Franken auf Ihre Bank tragen, und sie würden das jahrelang so tun. Stellen Sie sich weiter vor, Sie würden eines Tages beschliessen (und öffentlich bekannt geben), dass Sie am Ende des laufenden Monats CHF 1 000 000 auf Ihre Bank bringen werden. Können Sie nun aufgrund der Tatsache, dass Ihr Geldtransport jahrelang nicht angegriffen worden ist, darauf schliessen, dass das auch in diesem Monat der Fall sein wird? Wohl kaum. Aus der Sicht des Angreifers hat ein Franken bisher kein lohnendes Ziel dargestellt; es ist gewissermassen unter dem Radar durchmarschiert und auf seinem Schirm nicht aufgetaucht. Bei CHF 1 000 000 könnte die Situation anders aussehen.

In der Schweiz müssen die E-Voting-Urnengänge, wie sie in den Kantonen Genf, Neuenburg und Zürich durchgeführt werden, sicherheitstechnisch untersucht und einzeln bewilligt werden. Insbesondere muss für jeden Urnengang eine Obergrenze von stimmberechtigten Bürger(innen) festgelegt werden, die ihre Stimme elektronisch abgeben können. Diese Grenzen werden sinnvollerweise gerade so gewählt, dass eine massgebliche Beeinflussung des Ausgangs des Urnenganges im Falle einer Manipulation nicht möglich ist. Dadurch wird aber auch der Urnengang für einen potenziellen Angreifer unattraktiv. Dies gilt sowohl für den, der einen Angriff finanziert, als auch für den, der den Angriff ausführt. Beide werden warten, bis die Einsätze erhöht werden bzw. bis im E-Voting-Szenario die zugelassenen Obergrenzen den Ausgang der Abstimmung oder Wahl massgeblich beeinflussen können. Im angedachten Tempo der schrittweisen Erhöhung des Elektorates wird das noch einige Zeit dauern. Die in der Zwischenzeit erhoffte Sicherheit ist aber trügerisch und sollte nicht dazu verleiten, das Problem der unsicheren Client-Plattformen zu unterschätzen.

Lösungsansätze

Natürlich stellt sich die Frage, was man tun kann, um das Problem der unsicheren Client-Plattformen zu lösen oder wenigstens in seiner Brisanz zu mildern. Wie im Internet-Banking stehen auch im E-Voting grundsätzlich zwei Möglichkeiten zur Verfügung: Entweder kann man versuchen, die unsicheren Plattformen sicherer zu machen, oder man kann versuchen, die einzelnen Stimmabgaben – im Sinne von Transaktionen – abzusichern. Und ähnlich wie beim Internet-Banking erscheint auch beim E-Voting die zweite Möglichkeit einfacher und erfolgversprechender.

Im eingangs erwähnten Artikel wird «Code Voting» als Möglichkeit zur Absicherung von Stimmabgaben erwähnt. Beim Code Voting gibt eine Person ihre Stimme dadurch ab, dass sie anstelle von «Ja» oder «Nein» (im Falle einer Abstimmung) bzw. eines Namens einer Kandidatin oder eines Kandidaten (im Falle einer Wahl) einen vordefinierten und nur ihr bekannten Code eingibt. Die verschiedenen Codes sind (pseudo-)zufällig gewählt und werden über einen sicheren Kanal (z. B. Briefpost) verteilt. Die Idee ist, dass Malware, die eine Stimme ändern bzw. manipulieren will, den dafür erforderlichen Code nicht kennt und auch nicht in Erfahrung bringen kann. Im Fall einer Abstimmung würde mir als Stimmbürger z. B. postalisch mitgeteilt, dass – wenn ich «Ja» stimmen will – ich das dadurch ausdrücken kann, dass ich «5263» eingebe, bzw. dass ich ein «Nein» durch die Eingabe von «2132» ausdrücken kann. Wenn jetzt Malware auf meinem System feststellt, dass ich «2132» eingebe, weiss sie weder wofür dieser Code steht noch auf welchen Wert sie den Code setzen soll, um die Stimme zu ändern. Sie kann bestenfalls raten, und die Erfolgswahrscheinlichkeit von Raten kann durch das Anpassen von Codealphabet und -länge beliebig klein gemacht werden. Im Fall einer Wahl ist das Vorgehen analog, und es wird für jede Kandidatin und jeden Kandidaten ein separater persönlicher Code benötigt.

Natürlich gibt es auch alternative Möglichkeiten, um mit Codes zu arbeiten. Zum Beispiel könnte eine Person «normal» abstimmen und dann verifizieren, ob der Code, den ihr der Abstimmungsserver zurückgibt, mit einem Verifikationscode übereinstimmt. Selbstverständlich können auch beide Arten von Codes kombiniert und miteinander eingesetzt werden. In jedem Fall hat Code Voting aber auch Nachteile. So ist z. B.

Literatur

- Thomas Holderegger, Malware-Angriffe gegen E-Banking, digma 2008, 86 ff. (in dieser Nummer).
- Greg Hoglund/Gary McGraw, Exploiting Online Games: Cheating Massively Distributed Systems, Addison-Wesley, 2007.
- Rolf Oppliger/Jörg Schwenk/Christoph Löhr, CAPTCHA-based Code Voting, 3rd International Conference on E-Voting, Bregenz, 6.–9. August 2008.

sowohl das Eingeben der Codes als auch das Verifizieren der Codes nicht benutzerfreundlich und kann im zweiten Fall nicht einmal wirksam erzwungen werden. Entsprechend interessiert ist man an praktikablen Alternativen oder alternativen Ausgestaltungen von Code Voting. So werden in Oppliger/Schwenk (2008) z. B. Möglichkeiten diskutiert, maschinell nicht auslesbare Bilder – sog. CAPTCHAs (Completely Automated Public Turing tests to tell Computers and Humans Apart) – zur Darstellung von Abstimmungs- und Wahloptionen (in zufälliger Reihenfolge) einzusetzen, um das Code Voting für den Benutzer angenehmer zu gestalten. Anstelle einer Codeeingabe klickt der Benutzer dann auf ein CAPTCHA, das im Hintergrund die Übertragung des eigentlichen Codes auslöst. Solange das CAPTCHA sicher (d.h. maschinell nicht auslesbar) ist, kann die Malware nicht entscheiden, für welche Option sich der Benutzer entschieden hat bzw. welche Option wünschenswert wäre. Unter <http://wahlen.nds.rub.de> kann sich die interessierte Leserin oder der interessierte Leser einen ersten Eindruck über eine mögliche Ausgestaltung der Benutzerschnittstelle verschaffen. Natürlich steht und fällt die Sicherheit von CAPTCHA-basiertem Code Voting mit der Sicherheit (d.h. Nicht-Auslesbarkeit) der eingesetzten CAPTCHAs. Hier sind noch Fragen offen und Grundlagenarbeit erforderlich, damit man präzise Aussagen über die Sicherheit von CAPTCHA-basiertem Code Voting machen kann.

Zukunftsaussichten

Aus heutiger Sicht ist eines klar: Wenn wir fortfahren, im Zusammenhang mit E-Voting das Problem der unsicheren Client-Plattformen zu ignorieren oder unter Zuhilfenahme von statistischen Argumenten kleinzureden, laufen wir Gefahr, eines Tages und ohne Vorwarnung in den Grundpfeilern unserer Demokratie angegriffen und erschüttert zu werden. Nur im positiven Fall werden wir einen solchen Angriff überhaupt feststellen (z. B. im Rahmen eines «Denial-of-service»-Angriffs). Im negativen Fall wird Malware unterschwellig arbeiten und auf die beschriebene, nicht rekonstruierbare Art und Weise abgegebene Stimmen ändern. Zudem kann es natürlich immer sein, dass jemand behauptet, ein Angriff habe stattgefunden, ohne dass wir das verifizieren oder falsifizieren können. Im Zweifelsfall kann die Behauptung belegende Malware sogar ad hoc konstruiert und als «Beweis» vorgelegt werden.

Aus der Sicht der heute verfügbaren Technologien und Technologieansätze ist E-Voting ein Spiel mit dem Feuer. Solange die Möglichkeiten zur Beeinflussung des Ergebnisses eingeschränkt sind (z. B. durch ein klein gehaltenes Elektorat), wird wahrscheinlich nicht viel passieren. Sobald aber die Elektorate vergrössert und die Möglichkeiten zur Manipulation verbessert werden, wird auch die Attraktivität für Angreifer und damit die Wahrscheinlichkeit für Angriffe grösser. Darauf muss man vorbereitet sein. ■

Fussnoten

[1] Die Unterscheidung zwischen einem Computervirus und einem Computerwurm ist nicht präzis. Wenn sich eine Software primär durch das Ausführen einer Programmdatei dadurch reproduziert, dass sie weitere Programmdateien manipuliert (und damit infiziert), spricht man von einem Computervirus. Die Verbreitung erfolgt durch einen Benutzer bzw. dessen Aktivitäten. Demgegenüber bezeichnet man als Computerwurm eine Software, die sich über laufende Prozesse reproduziert, ohne dass der Benutzer etwas auslösen muss.

* Der Artikel gibt die persönliche Meinung des Autors wieder und ist nicht als Stellungnahme des ISB zu verstehen.

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info
erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 123.00** (inkl. Versandkosten)

Name Vorname

Firma

Strasse

PLZ Ort Land

Datum Unterschrift

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich
Telefon +41 44 200 29 19
Telefax +41 44 200 29 18
E-Mail: zs.verlag@schulthess.com
Homepage: www.schulthess.com

Schulthess §