Code Voting - Ein Verfahren für Aktiengesellschaften?

Jörg Helbach
Sprint Sanierung GmbH

Abstract: Nach einer EU-Richtlinie, die in 2007 verabschiedet wurde, müssen Aktiengesellschaften ihre Hauptversammlung für die Online-Teilnahme öffnen. Dies beinhaltet dann natürlich auch die Stimmabgabe bei Abstimmungen, z.B. der Entlastung des Vorstandes. In diesem Artikel wird Code Voting vorgestellt und analysiert, ob und wie dieses Verfahren für entsprechende Wahlen sinnvoll nutzbar ist.

Keywords. E-Voting, Code Voting, Aktiengesellschaften.

1 Einleitung

Nach einer im Januar 2007 verabschiedeten EU-Richtlinie müssen börsenorientierte Aktiengesellschaften ihre Hauptversammlungen für eine Online-Teilnahme öffnen [Zyp07]. Ziel dieser Richtlinie ist es die Rechte der Aktionäre - insbesondere auch der Kleinaktionäre - über EU-Grenzen hinweg zu stärken. Bei einer Hauptversammlung werden u.a. in der Regel ein oder mehrere Abstimmungen, wie z.B. die Frage nach der Entlastung des Vorstandes, durchgeführt. Daher muss allen Teilnehmern einer Hauptversammlung die Stimmabgabe ermöglicht werden. Dazu bietet sich an dieser Stelle die Nutzung einer elektronischen Wahlmöglichkeit an.

In diesem Beitrag werden in einem ersten Schritt die Anforderungen an Abstimmungen in Aktiengesellschaften, die sich in Teilen von denen an politische Wahlen unterscheiden, skizziert. Anschließend wird das Code Voting Verfahren erläutert und mit den ermittelten Anforderungen abgeglichen.

2 Anforderungen an Wahlen bei Aktiengesellschaften

Es gibt eine ganze Reihe von Untersuchungen, die sich mit Anforderungen an elektronische Wahlsysteme im Allgemeinen und den Anforderungen an Internetwahlsysteme im Speziellen beschäftigen. Im deutschsprachigen Raum sind an dieser Stelle der Katalog der PTB [PTB04] und die Empfehlungen des Europarates [CoE04] zu erwähnen. Generelle Anforderungen an elektronische Wahlsysteme sind z.B.:

- Das Wahlergebnis muss korrekt und vollständig sein,
- die Integrität des Wahlergebnisses, insbesondere auch der Schutz gegenüber Schadsoftware, muss gewährleistet sein und

- jeder Wahlberechtigte muss wählen können, jede nicht-wahlberechtigte Person darf nicht wählen können.
- Wenn gewünscht oder erforderlich muss die Anonymität der Wähler gewährleistet sein.

Erwähnenswert ist auch die Entwicklung eines Protection Profiles[1] gemäß Common Criteria in Kooperation des DFKI, des BSI und der GI [GKM+06], welches die Anforderungen, die für alle Wahlen gleich sind, zusammenfasst und somit die Kernanforderungen an elektronische Wahlsysteme auflistet. Herstellern elektronischer Wahlsoftware kann damit u.a. die Möglichkeit der Zertifizierung gegenüber diesen Anforderungen ermöglicht werden.

Ein wesentliches Unterscheidungsmerkmal zwischen (politischen) Wahlen und Abstimmungen bei Aktiengesellschaften ist, dass die stimmberechtigten Aktionäre im Falle der AG-Abstimmungen ihr Stimmrecht an andere Aktionäre übertragen bzw. deligieren können, so dass ein Wahlberechtigter durchaus mehrere Stimmen abgeben können muss. Weiter darf eine übermittelte Stimme natürlich nicht von "Außen" manipuliert werden, damit die Integrität der Abstimmung nicht gefährdet ist. Das Gefährdungspotential ist an dieser Stelle sehr hoch, da es sehr wahrscheinlich ist, dass Angreifer auf diese Weise versuchen könnten den Aktienkurs zu beinflussen. Beispielsweise könnte die (vor allem unerwartete) Nicht-Entlastung eines Vorstandes zu gewaltigen Einbrüchen des Aktienkurses führen, den der Angreifer zum Kauf einer großen Aktienmenge ausnutzen könnte. Aus diesem Grund nimmt auch die Verifizierbarkeit der abgegebenen Stimmen einen hohen Stellenwert ein. Dagegen ist die Anonymität der Stimmabgabe zwar in vielen Fällen gewünscht, aber nicht zwingend erforderlich.

3 Das "Secure Platform" Problem

Die meisten Internetwahlsysteme sind anfällig gegen einen einfachen Angriff: Wenn es einem Angreifer gelingt die Kommunikation zwischen Rechner und Benutzer zu kontrollieren, kann er dem Wähler einen falschen Stimmzettel anzeigen und die Wahlentscheidung des Wählers modifizieren oder verhindern, jeweils ohne dass der Wähler dies bemerken kann.

Daher ist bei Internetwahlsystemen, bei denen der PC des Wählers der Wahl-Client ist, Malware ein großes und zunehmendes Problem. Dazu wurde der Begriff "Secure Platform" Problem von Ronald Rivest bereits 2002 geprägt [Riv02]. Schätzungen zufolge sind etwa 25% aller Rechner, die einen Internetzugang haben, mit Schadsoftware verseucht [Web07]. Dies hat selbstverständlich auch einen großen Einfluss auf die Abstimmungen bei Aktiengesellschaften.

Die zwei Hauptalternativen, um das "Secure Platform" Problem zu lösen, sind:

- den PC gegen Schadsoftware zu sichern, z.B. durch den Einsatz von Trusted Computing Technologien und

[1] Das Protection Profile ist derzeit noch im Entwurfsstadium, steht aber kurz vor der Zertifizierung.

Tabelle 1: Code Sheet mit Wahl-TAN.

Kandidat	Wahl-TAN
Alice	738747987
Bob	983293774
Clark	192851911

- durch die Nutzung eines separaten Kommunikationskanals zwischen Wahlbehörde und Wähler.

Weitere Möglichkeiten finden sich in [Opp02].

An dieser Stelle lässt sich Code Voting, dass im nächsten Abschnitt vorgestellt wird, mit Nutzung von Post als separatem Kommunikationskanal einsetzen.

4 Code Voting

4.1 Grundidee

Das Code Voting Verfahren wurde im Jahr 2001 durch David Chaum mit seinem Wahlsystem Sure Vote eingeführt [Cha01]. Jeder Wahlberechtigte erhält dabei auf nicht elektronischem Weg, z.B. per Post, ein sog. Code Sheet, auf dem für jeden Wähler pro Wahlentscheidung eine eindeutige Nummer (Wahl-TAN) abgedruckt ist. Nachdem der Wähler sich mit dem Wahlserver verbunden hat, übermittelt er, anstatt des Namens seiner bevorzugten Wahlentscheidung, lediglich die zugehörige Wahl-TAN.

Damit das Code Voting Verfahren sinnvoll funktioniert wird angenommen, dass

- ein vertrauenswürdiger Wahlvorstand existiert, der jedem Wahlberechtigten ein gültiges Code Sheet zur Verfügung stellt und
- die verwendeten Wahlserver und Datenbanken zuverlässig, verfügbar und sicher sind.

Um Code Voting gegen passive Attacken[2] abzusichern, müssen zwei weitere, (relativ) leicht zu realisierende, Annahmen getroffen werden. Diese sind:

- Alle Wahl-TANs sind eindeutig und zufällig für alle Kandidaten und alle Code Sheets und
- alle Code Sheets dürfen nicht elektronisch zum Wähler übertragen werden.

[2] d.h. ein Angreifer liest die Wahlentscheidung mit, beeinfllusst sie aber nicht.

Tabelle 2: Code Sheet mit Wahl-, Bestätigungs- und Finalisierungs-TAN.

Wahl-TAN	Kandidat	Bestätigungs-TAN	Finalisierungs-TAN
738747987	Alice	332676873	442367810
983293774	Bob	676476488	123456789
192851911	Clark	301287123	520172861

Aktive Attacken sind trotz dieser Anforderungen möglich, da ein Angreifer - beispielsweise per Man-in-the-middle-Angriff - die Übermittlung der Wahl-TAN zum Wahlserver verhindern kann, ohne dass der Wähler dies bemerkt, da er keinerlei Möglichkeit hat zu verifizieren, ob seine Stimme bei dem Wahlserver angekommen ist. Alternativ kann der Angreifer die Wahl-TAN auch verfälschen, um sie so ungültig zu machen.

4.2 Erweitertes Code Voting

Da der Wähler über einen unsicheren Kanal mit dem Wahlserver kommuniziert, kann man nachweisen, dass es für beide Parteien unmöglich ist zu verifizieren, ob der Kommunikationspartner die abgeschickte Nachricht erhalten hat. Zurückführen lässt sich diese Problematik auf das Zwei-Armeen-Problem [AEH75] [Gra78].

In der Praxis haben sich als Lösungsnäherung 3-Wege-Verfahren bewährt[3], welche auch auf das Code Voting Verfahren angewendet werden können. Dazu wird das Code Sheet pro Wahlentscheidungsmöglichkeit um eine Bestätigungs-TAN und eine Finalisierungs-TAN erweitert [HS07].

Nachdem der Wähler seine Wahl-TAN an den Server übermittelt hat, antwortet dieser mit der korrespondierenden Bestätigung-TAN. Der Wähler kann seine Wahlentscheidung dann mit der Finalisierungs-TAN bestätigen. Solange eine Wahlentscheidung noch nicht finalisiert ist, kann der Wähler seine Stimme ändern, d.h. er kann eine andere Wahl-TAN seines Code Sheets an den Server übermitteln. In diesem Fall wird die ursprüngliche Entscheidung verworfen. Damit der Wähler überprüfen kann, ob seine Wahlentscheidung richtig am Wahlserver angekommen ist, kann er seine Finalisierungs-TAN erneut senden. Der Wahlserver antwortet dann mit einer Rückmeldung, dass bereits finalisiert wurde oder die zugehörige Wahl-TAN noch nicht eingegeben wurde[4].

5 Code Voting für Aktiengesellschaften

Jeder Aktionär, der online an der Hauptversammlung teilnimmt erhält für die Abstimmungen ein mehrfach verwendbares Code Sheet gemäß Tabelle 2. Pro Abstimmung kann das

[3] vgl. z.B. TCP-Handshake

[4] Der zweite Teil der Rückmeldung ist notwendig, damit der Wähler seine Wahlentscheidung nicht nachweisen kann.

Code Sheet aber selbstverständlich nur einmal verwendet werden. Jedes Code Sheet hat zusätzlich eine darauf angegebene Wertigkeit, so dass jeder Aktionär nur ein einziges Code Sheet erhält, egal wie viele Aktienanteile er an der Gesellschaft hält. Während einer Abstimmung muss diese Wertigkeit vom Wahlserver berücksichtigt werden.

Am Ende der Abstimmung werden alle gewerteten Voting TANs auf einem Bulletin Board veröffentlicht, so dass der Wähler überprüfen kann, dass sein Stimme auch in das Ergebnis eingegangen ist. An dieser Stelle muss man sich freilich ein Verfahren überlegen, dass angewendet werden kann, falls eine fehlende oder fehlerhafte TAN reklamiert wird. Generell besteht das Problem der Falschreklamation, d.h. ein Aktionär reklamiert eine vermeindliche falsche Wahl-TAN, obwohl das Wahlsystem korrekt gearbeitet hat. Zusätzlich werden die Wahl-TANs angezeigt, für die keine gültige Finalisierungs-TAN angekommen ist.

Das Code Voting Verfahren ist zwar generell anfällig gegen Stimmenkauf [OSH08], d.h. der Wähler kann jederzeit sein Code Sheet an Dritte weitergeben, bei Aktiengesellschaften ist dies aber eine gewünschte Eigenschaft, da ein Aktionär sein Stimmrecht an Dritte übertragen darf. Bei politischen und anderen Wahlen, bei denen die Stimmabgabe durch Dritte nicht rechtens ist, wird die sinnvolle Weitergabe des Code Sheets durch eine Kombination des Code Voting Verfahrens mit Gruppensignaturen [CH91][ACJT00] verhindert [HSS08].

Weiter ist durch die Nutzung von Code Voting die Integrität der Abstimmung gewährleistet, insbesondere da die Aktionäre die Möglichkeit der Verifikation haben. Aktive und passive Angriffe sind zwar weiterhin möglich, führen aber für einen Angreifer nicht zum gewünschten Ergebnis. Bei passiven Angriffen kann der Angreifer die übermittelten TANs mitlesen, aber nicht auf die Wahlentscheidung schliessen. Aktive Angriffe können nicht mehr unbemerkt vom Wähler ablaufen, da ein Angreifer nicht in der Lage ist die erwartete Bestätigungs-TAN zu berechnen.

Die Anonymität der Stimmabgabe ist sichergestellt, sofern der Aktionär sie nicht aktiv preis gibt. Voraussetzung dazu ist allerdings, dass die Erstellung und Verteilung der Code Sheets durch die entsprechende Wahlautorität anonymisiert erfolgt. Damit erfüllt Code Voting alle Anforderungen, die an die Stimmabgabe bei Hauptversammlungen börsenorientierter Unternehmen gekoppelt sind.

6 Fazit

Code Voting als elektronisches Wahlverfahren kann ideal für Abstimmungen bei Hauptversammlungen börsennotierter Unternehmen eingesetzt werden, da es alle Anforderungen an diese Abstimmungen erfüllt. Voraussetzung dafür ist allerdings, dass die eingesetzten Serversysteme zuverlässig und korrekt arbeiten. Daher kann es sinnvoll sein, die entsprechenden Serversysteme so einzusetzen, dass ein Vier-Augenprinzip gewährleistet ist. Ein generelles Problem in der Verwendung von Code Voting ist sicher noch die Usability des Verfahrens. Hier sind weitere Untersuchungen erforderlich, wie das Verfahren einfacher in der Handhabung werden kann.

Literatur

[ACJT00] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik: "A Practical and Provably Secure Coalition-Resistant Group Signature Schemeïn Advances in Cryptology - CRYPTO 2000, volume 1880 of Lecture Notes in Computer Science, pp. 255-270. Springer-Verlag, 2000.

[AEH75] E. A. Akkoyunlu, K. Ekanadham, and R. V. Huber: "Some Constraints and Tradeoffs in the Design of Network Communicationsïn ACM SIGOPS Operating Systems Review, volume 9, issue 5, p. 67-74, 1975.

[CH91] D. Chaum, E. van Heyst: "Group signatures" in Advances in Cryptology - EUROCRYPT '91, volume 547 of Lecture Notes in Computer Science, pp. 257-265, Springer-Verlag, 1991.

[Cha01] D. Chaum: "Sure Vote: Technical Overview" in Proceedings of the workshop on trustworthy elections (WOTE '01), presentation slides, `http://www.vote.caltech.edu/wote01/pdfs/surevote.pdf`, 2001.

[CoE04] Council of Europe (2004): "Legal, operational and technical standards for e-voting". Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum, Straßburg, 2004.

[GKM+06] R. Grimm, R. Krimmer, N. Meißner, K. Reinhard, M. Volkamer, M. Weinand, J. Helbach: "Security Requirements for Non-political Internet Voting.", Lecture Notes on Informatics 86. pp. 203-212. Electronic Voting 2006. Proceedings of the 2nd International Workshop on Electronic Voting 2006,(2-4 Aug 2006), Bregenz.

[Gra78] Jim Gray: "Notes on Data Base Operating Systems", in Lecture Notes in Computer Science, volume 60, pp. 393-481, 1978.

[HS07] J. Helbach, J. Schwenk: "Secure Internet Voting With Code Sheets", in Proceedings of the VOTE-ID 2007 Conference, LNCS 4896, pp. 166-177, 2007.

[HSS08] J. Helbach, S. Schäge, J. Schwenk: "Code Voting With Linkable Group Signatures", accepted for EVOTE08, 3rd International Workshop on Electronic Voting 2008.

[Opp02] R. Oppliger: "How to Address the Secure Platform Problem for Remote Internet Voting" in Proceedings 5^{th} Conf. Security in Information Systems (SIS 2002), vdf Hochschulverlag, pp. 153-173, 2002.

[OSH08] R. Oppliger, J. Schwenk and J. Helbach: "Protecting Code Voting Against Vote Selling" accepted for Sicherheit 2008, April 2^{nd}-4^{th}, 2008, Saarbrücken, Germany.

[PTB04] Physikalisch-Technische Bundesanstalt (PTB, 2004): "Online Voting Systems for Non-parliamentary Elections – Catalogue of Requirements", Technical Paper PTB-8.5-2004-1, Berlin, April 2004.

[Riv02] R. Rivest: "Electronic voting" in Financial Cryptography '01, p. 243-268, Springer-Verlag, LNCS 2339, 2002.

[Web07] T. Weber: "Criminals 'may overwhelm the web'", `http://news.bbc.co.uk/1/hi/business/6298641.stm`.

[Zyp07] Zypries: "Virtual general meetings" throughout Europe enhance the rights of shareholders. `http://www.bmj.de/files/-/1739/Press%20Release%20in%20english.pdf`