O02 Die Zukunft der SPD-internen Abstimmungen: Wir müssen mehr Zugriffsschutz wagen.

Antragsteller*in:	Jusos Dresden
Tagesordnungspunkt:	0.O - Organisation/Verbandsleben
Status:	Zurückgezogen

Antragstext

Die Jusos Sachsen mögen beschließen und über den Bundeskongress und den Landesparteitag an den Bundesparteitag weiterleiten. Im Weiteren wird der Antrag direkt an den Landeschäftsführer und den Bundesgeschäftsführer weitergeleitet.

Demokratie lebt von Beteiligung. Für die Partei, die wie keine andere für die Demokratisierung sämtlicher Lebensbereiche kämpft, ist es eine Selbstverständlichkeit auch und gerade intern wichtige Entscheidungen unter Einbeziehung aller zu treffen. Das Angebot digitaler Möglichkeiten bei parteiinternen Entscheidungen ist somit ein im Grundsatz richtiger, zumindest aber sehr nachvollziehbarer Schritt.

Leider haben wir dabei in der jüngeren Vergangenheit wichtige demokratische Grundprinzipien nicht beachtet und grundlegende Prinzipien der IT-Sicherheit nicht verstanden bzw. grob missachtet. Besonders bitter ist dabei, dass die vordringlichste Motivation die Kosteneinsparung ist. Die SPD darf demokratische Entscheidungsfindung nicht durch Sparzwänge gefährden. Demokratie ist keine Geldfrage. Lasst uns die Teilhabe ermöglichen, die unsere Partei braucht und die Mitglieder verdienen!

Konkret beziehen wir uns auf die Wahl zum Bundesvorsitzenden-Duo sowie die Abstimmung über den sächsischen Koalitionsvertrag:

Elektronische Wahlen

Für die Abstimmung über die künftige Parteispitze der SPD müssen die Wahlgrundsätze der Budesrepublik Grundlage sein. Eine solche Abstimmung muss also allgemein, frei, gleich, unmittelbar und geheim sein. Darüber hinaus muss das eingesetzte Verfahren für jede und jeden offensichtlich nachvollziehbar sein.

Ein digitales Verfahren führt dabei immer eine Verletzung des Wahlgeheimnisses oder der Unmittelbarkeit der Wahl. Entweder kann nicht nachvollzogen werden, dass meine Stimme am Ende unmittelbar und richtig abgegeben sowie gewertet wurde oder wenn dies überprüft werden könnte, wäre das Wahlgeheimnis verletzt. Das Problem liegt schlicht und ergreifend darin, dass niemand von uns in der Lage ist den Elektronenstrom in einem Transistor mit den eigenen Sinnen direkt nachzuvollziehen. Bei einer Urne mit Papierwahlzetteln geht das eben schon. Denn auch wenn tausende Tests mit dem Verfahren zu einem konsistenten Ergebnis führen, ist eben nicht klar, dass es beim tausend und ersten Mal wieder so ist oder letztlich gar eine Manipulation für den Testbetrieb vorlag.

Wenn das Bundesverfassungsgericht und der Chaos Computer Club sich bei einer digitalpolitischen Angelegenheit einig sind, ist davon auszugehen, dass sie Recht haben.

Daraus ergibt sich im Besonderen folgende Schlussfolgerung:

Wir erkennen an, dass es niemals eine Möglichkeit geben wird, Wahlen ausschließlich unter Einsatz digitaler Hilfsmittel unter Wahrung der Wahlgrundsätze nach Artikel 38 des Grundgesetzes durchzuführen. Dies betrifft sowohl Onlineverfahren als auch Abstimmgeräte auf Parteitagen. Es muss mindestens eine Absicherung des Verfahrens über eine für Laien einfach und offensichtlich nachvollziehbare erfolgen.

Wir fordern, dass alle Wahlen sowie damit verbundene Meinungsbildung entweder per Urnen- oder Briefwahl abgesichert werden.

Abstimmung über politische Sachverhalte

Wir halten es für richtig und gut, die Mitgliedschaft stärker einzubinden und in die Pflicht zu nehmen an den Entscheidungen des sächsischen Landesverbandes mitzuwirken. Dafür bilden digitale Meinungsfindungs- und Abstimmungsverfahren eine akzeptable Grundlage, wenn diese im informationstechnischen Sinne sicher sind.

Die Nachvollziehbarkeit kann hierbei jedoch durch eine öffentliche – für alle einsehbare – Aufzeichnung des individuellen Abstimmungsverhaltens sichergestellt werden. Prinzipiell wäre es also möglich Kaderlisten auf Basis von erwünschtem oder unerwünschtem Abstimmungsverhalten zu erstellen. Diesem Risiko muss bewusst begegnet werden. Eine zeitlich begrenzte öffentlich Verfügbarkeit der Daten schränkt die Auswertung zumindest etwas ein.

Elektronische Systeme, die es ermöglichen müssen insbesondere folgende Schutzziele der Informationssicherheit erfüllen: Vertraulichkeit, Integrität und

Authentizität. Das heißt mindestens – und es ist ein Armutszeugnis, dass wir so etwas beschließen müssen:

- kein Einsatz unverschlüsselter Kommunikation,
- Sicherstellung der richtigen Empfänger:innen (keine Verwendung unüberprüften Mail-Adreesen),
- verpflichtende Mehr-Faktor-Authentifizierung auf Empfänger:innen-Seite,
- Überprüfparkeit des eigenen Abstimmungsverhaltens durch Veröffentlichung namentlicher Abstimmungslisten,

Bis eine vollständige, überprüfbare informationstechnisch sichere elektronische Lösung nicht einsatzbereit ist, sollten wir darauf jedoch dringend verzichten.

Darüber hinaus regen wir an Möglichkeiten der Liquid Democracy, das heißt der themenspezifischen Stimmrechtsübertragung, stärker zur Entscheidungsfindung zu berücksichtigen.

Begründung

Der Antragstext enthält vor allem die grundsätzlichen Überlegungen für oder gegen elektronisch unterstützte Abstimmungsssyteme. Die Begründung soll insbesondere dazu dienen, die teils groben technischen Schnitzer für die Wahl der Bundesvorsitzenden bzw. der Abstimmmung über den Koalitionsvertrag hervorzuheben und damit den dringenden innerparteilichen Handlungsbedarf darzustellen.

Bei der Bundesvorsitzendenwahl wurde ein Opt-In-Verfahren benutzt, dass alle Abstimmungsberechtigten hatten die Möglichkeit durch eigenes Handeln statt an einer Briefwahl an einer digitalen Abstimmung teilzunehmen. Daraufhin wurden jedoch unverschlüsselte Mails an nicht überprüfte Mail-Adressen mit den jeweiligen Zugangsberechtigungen zur Abstimmungen versendet. In Kombination mit Mitgliedsnummer und Geburtsdatum konnten daraus die Abstimmungstokens generiert werden. Durch gezieltes Phishing, bereits kompromittierte IT-Sysmte auf Mitgliederseite oder schlichtweg gemeinsam genutzte Mail-Adressen, sind eine Reihe von Angriffsvektoren geöffnet worden.

Bei der Abstimmung über den Koalitionsvertrag sind die Zugangsberechtigungen darüber hinaus sogar über eine Serienbrieffunktion versendet worden, die es ermöglicht hat, die Zugangsberechtigungen aller Mitglieder außerhalb ihres Mailpostfachs über eine unverschlüsselte HTTP-Verbindung ohne SSL abzurufen. Die einzige „Sicherheit“ war eine bis zu 8 Stellen umfassende individuelle ID aus Großbuchstaben und Ziffern. Eine Größenordnung, die man durchaus mit einfachen Bruteforce-Methoden erreichen kann. Darüber hinaus gab es hier nur die Optout-Möglichkeit, das heißt alle abstimmungsberechtigten Mitglieder konnten dem Online-Verfahren lediglich widersprechen.