Hinweise zu den Online-Wahlen 2023
an der Martin-Luther-Universität Halle-Wittenberg

1. Allgemeines

In diesem Jahr finden die Wahlen der Vertreter*innen der Mitgliedergruppen 3 (Studierende) zum Senat und zu den Fakultätsräten, die Wahlen zum Studierendenrat und zu den Fachschaftsräten statt. Wählen dürfen damit in diesem Jahr alle zum Stichtag immatrikulierten und rückgemeldeten Studierenden der Universität.
Die Wahlen werden als internetbasierte Online-Wahlen durchgeführt. Die Online-Wahl erfolgt über einen Webbrowser (s. dazu unter 3.) und kann somit von jedem internetfähigen Endgerät aus erfolgen. Eine Spezialsoftware ist nicht notwendig.
Als technische Plattform wird das Online-Wahlsystem „uniWAHL OWS“ der Firma Electric Paper Informationssysteme GmbH mit einer auf die MLU-spezifischen Bedürfnisse angepassten Nutzerführung eingesetzt, die einfach und intuitiv zu bedienen ist.
Das Online-Wahlsystem erfüllt die aktuellen Anforderungen an Wahlsysteme (mindestens die Common Criteria). Eine entsprechende Zertifizierung gemäß den Vorgaben des BSI ist in Vorbereitung. Zudem werden unabhängige Penetrationstests von unabhängigen Sachverständigen nach Vorgaben des BSI durchgeführt. Das Wahlsystem zeichnet sich unter anderem durch eine dem aktuellen Stand der Technik entsprechend sichere, verschlüsselte Kommunikation, verschlüsselte und Ende-zu-Ende verifizierbare, datenschutzgerechte Verarbeitung, barrierefreie Darstellung nach den WCAG 2.1 AA sowie optimierte Nutzung auf mobilen Endgeräten aus. Es handelt sich zudem um Open Source-Software (OSS) mit einem umfassend dokumentierten, kryptographischen Konzept.

2. Das Onlinewahlsystem

2.1 Allgemeine Sicherheitshinweise

Die Abstimmung durch die Wahlberechtigten soll bei den als Online-Wahl durchgeführten Wahlen auf einem individuell genutzten Computerarbeitsplatz mit Internetanschluss erfolgen, über den die abgegebenen Stimmen verschlüsselt an das Wahlsystem übertragen werden. Die Beachtung der hier empfohlenen Sicherheitsmaßnahmen soll sicherstellen, dass geeignete Vorkehrungen getroffen sind, um ein Mindestmaß an Sicherheit zu gewährleisten: etwa, um Angriffe durch „Computerviren, Würmer, Trojaner“ (Schadprogramme) und ähnliche dienstbehindernde Attacken auf den Computerarbeitsplatz oder Wahlservern zu vermeiden oder um die Einhaltung des Wahlgeheimnisses zu gewährleisten.

2.2 Nutzbarkeit des Wahlsystems trotz technischer oder persönlicher Einschränkungen

Die Wahlanwendung ist grundsätzlich für alle berechtigten Nutzerinnen und Nutzer barrierearm zugänglich. Unabhängig von körperlichen oder technischen Möglichkeiten ist die Online-Wahl weitgehend uneingeschränkt ohne fremde Hilfe durchführbar. Dies schließt sowohl die Nutzung durch Personen mit und ohne gesundheitliche Beeinträchtigungen als auch die Nutzung mit technischen Einschränkungen (z.B. Textbrowser oder PDA) grundsätzlich ein. Das Vorlesen der dargestellten Informationsangebote über spezielle Computerprogramme (Screenreader) oder die Ausgabe in Braille-Schrift für Blinde und sehbehinderte Personen ist mit entsprechenden Hilfsmitteln möglich.

2.3 Online-Wahlsystem und Teilnahme an der Online-Wahl

Die Vorbereitung der Stimmzettel, die Erstellung des (pseudonymisierten) Wählerverzeichnisses sowie einer Datei zur Beschreibung der zu wählenden Gremien erfolgt in der Universität. Beides wird der Firma Electric Paper Informationssysteme GmbH über ein sicheres Austauschverfahren bereitgestellt und von dieser für die Vorbereitung der Wahl im Online-Wahlsystem weiterverarbeitet. Im pseudonymisierten Wählerverzeichnis sind keine personenbezogenen Daten enthalten, sondern lediglich Wahlnummern. Daten, die auf die persönliche Identität von Wahlberechtigten schließen lassen könnten, werden ausdrücklich nicht in uniWAHL OWS gespeichert. Die Sicherheit der für den Betrieb eingesetzten Server sowie die dort eingesetzten Verfahren werden durch die technischen Betreiber nach allgemein anerkannten Sicherheitsstandards gewährleistet.

Die Online-Wahlsystem ist eine Web-Anwendung (mit verifizierbarer Ende-zu-Ende-Verschlüsselung) und stellt eine digitale Wahlkabine sowie eine digitale Wahlurne inkl. Prüf-Funktionen der Integrität der Urne bereit. Die digitale Wahlurne wird für die Aufbewahrung und Zählung der Stimmen eingesetzt. Als Übertragungskanal wird bei der Online-Wahl das Internet genutzt.

2.4 Benutzer-Autorisierung für die Teilnahme an der Online-Wahl

Die wahlberechtigten Studierenden nutzen für die Teilnahme an der Online-Wahl zunächst ihren Zugang zum Löwenportal[1] und melden sich dort mit ihrer persönlichen Benutzerkennung und zugehörigem Passwort an.

Im Wahlzeitraum finden die Studierenden im Funktionsmenü des Löwenportals den Unterpunkt „Online-Wahlen“. Der bzw. die Studierende findet an dieser Stelle einen individualisierten und temporär gültigen Link (so genannter SmartLink) zum Wahlsystem. Über diesen Link erfolgt eine Weiterleitung zum Wahlsystem. Dort ist keine erneute Authentifizierung mehr notwendig und alle Wahlberechtigten können direkt mit der Stimmabgabe beginnen. Die Identität der Wähler ist dabei zu jeder Zeit geschützt.

2.5 Gültigkeit des SmartLinks und Ablauf der Online-Wahl

Bitte beachten Sie, dass der im Löwenportal im Unterpunkt „Online-Wahlen“ für Sie bereitstehende SmartLink nur temporär gültig ist. Dies bedeutet im Einzelnen:

1. Der SmartLink ist nach Aufrufen des Unterpunktes „Online-Wahlen“ nur 15 Minuten gültig, d.h. mit dem dort erzeugten SmartLink kann die digitale Wahlkabine nur innerhalb von 15 Minuten aufgerufen werden.

2. Ihre Autorisierung im uniWAHL OWS (digitale Wahlkabine) wird ungültig (Ablauf der Sitzung), sobald während des Wahlvorgangs für mehr als 15 Minuten keine Eingabe erfolgt ist. Sofern Sie bis dahin keinen Stimmzettel in der digitalen Wahlurne abgegeben haben, werden von Ihnen durchgeführte Aktionen (Kreuze in einem Stimmzettel) nicht gespeichert.

[1] Erreichbar über https://loewenportal.uni-halle.de

3. Sie können in diesem Fall, sofern der Wahlzeitraum noch nicht abgelaufen ist, im Löwenportal einen dort neu für Sie erstellten SmartLink nutzen und damit die digitale Wahlkabine erneut betreten. Bitte rufen Sie hierfür im Löwenportal den Unterpunkt „Online-Wahlen“ erneut auf.

4. Sie können Ihre Sitzung in der digitalen Wahlkabine auch selbst abbrechen und hierfür den Menüpunkt „Ausloggen“ in der oberen Leiste des uniWAHL OWS wählen. Auch in diesem Fall können Sie die digitale Wahlkabine über einen neu für Sie erstellten SmartLink im Wahlzeitraum erneut betreten, um Ihre Stimmen abzugeben.

5. Im uniWAHL OWS müssen die Stimmzettel einzeln aufgerufen und einzeln in die digitale Wahlurne abgegeben werden. Auch in diesem Fall können Sie die Sitzung in der digitalen Wahlkabine abbrechen und finden bei der erneuten Einwahl über einen neuen SmartLink nur noch die Stimmzettel vor, die Sie zuvor noch nicht in der digitalen Wahlurne abgegeben haben.

2.6 Verifikation der Stimmabgabe

Das Online-Wahlsystem uniWAHL OWS stellt die Möglichkeit für eine Verifikation Ihrer Stimmabgabe für Sie bereit. Nach Abgabe jedes Stimmzettels bestätigt das uniWAHL OWS Ihnen zunächst, dass Ihr Stimmzettel korrekt in die digitale Wahlurne abgegeben wurde und es wird Ihnen eine „Stimmabgabebeleg-ID“ angezeigt, mit der Sie selbst noch einmal nachvollziehen können, ob Ihr Stimmzettel abgegeben wurde.

Wichtig: Diese Verifikationsmöglichkeit bezieht sich nur auf die Abgabe der Stimmzettel selbst, jedoch nicht auf den Inhalt der Stimmzettel, so dass Sie nicht reproduzieren können, für wen Sie gestimmt haben. Somit ist das Wahlgeheimnis gewahrt.

3. Allgemeine sicherheitstechnische Hinweise

3.1 Sicherheitstechnische Anforderungen an den Computerarbeitsplatz, der zur Durchführung der Wahl genutzt wird

Zur Durchführung des Wahlvorgangs ist ein handelsüblicher Computerarbeitsplatz oder ein mobiles Endgerät mit funktionierendem Internetanschluss erforderlich.

Es wird empfohlen, ausschließlich Geräte in vertrauenswürdigen Umgebungen zu nutzen, bei denen die grundsätzliche Einhaltung der empfohlenen Sicherheitsmaßnahmen im Allgemeinen sichergestellt wird. Von der Nutzung von Computerarbeitsplätzen in nicht vertrauenswürdigen Umgebungen wird aus Sicherheitsgründen abgeraten.

Wahlberechtigte sind grundsätzlich selbst dafür verantwortlich, dass die Beachtung der hier empfohlenen Sicherheitsmaßnahmen am genutzten Computerarbeitsplatz gegeben ist. Diese Sicherheit wird z.B. auch in den Computerpools der Universität gewährleistet, sofern kein geeigneter Arbeitsplatz zur Verfügung steht. Alternativ besteht die Möglichkeit, für die Teilnahme an der Online-Wahl während des Wahlzeitraumes nach telefonischer Voranmeldung einen PC im Wahlamt zu nutzen.

3.2 Geheimhaltung der Zugangsdaten

Bitte achten Sie unbedingt darauf, dass Sie Ihren Zugang zum Löwenportal stets unter Verschluss zu halten haben und unberechtigte Dritte keinen Zugriff auf diese Daten bekommen dürfen.

3.3 Nutzung des Computerarbeitsplatzes ohne administrative Rechte

Wir empfehlen Ihnen dringend, das Internet nur mit einem Benutzerkonto ohne Administrationsrechte zu nutzen und zu verhindern, dass sich Schadprogramme unbeabsichtigt installieren können. Schadprogramme sind zur dauerhaften Installation auf fremden Rechnern meist darauf angewiesen, dass angemeldete Benutzerinnen und Benutzer über Administrationsrechte verfügen. Wie Sie ein solches Benutzungskonto ohne diese Rechte einrichten, können Sie der Dokumentation Ihres Betriebssystems entnehmen.

3.4 Internetbrowser

Achten Sie bitte darauf, dass Sie die eingesetzte Browser-Software aus vertrauenswürdigen Quellen bezogen haben, so dass sichergestellt ist, dass es sich um unveränderte Originalsoftware handelt. Bitte setzen Sie nur die folgenden Browser in der jeweils aktuellsten Version ein: Google Chrome, Mozilla Firefox, Opera, Safari und/oder Microsoft Edge.

Wichtig ist, dass Sie ihren Browser regelmäßig aktualisieren, um die Sicherheit Ihrer Internetverbindung zu wahren. Beim Bekanntwerden von Sicherheitsproblemen veröffentlichen die Softwarehersteller in der Regel zeitnah fehlerbereinigte Versionen (Updates). Informieren Sie sich daher regelmäßig über neue Sicherheitsupdates sowohl für das von Ihnen verwendete Betriebssystem und den Internet-Browser Ihres Computerarbeitsplatzes, z.B. für Microsoft-Produkte mit Hilfe der Windows-Update-Funktion, oder fragen Sie als Beschäftigte/r Ihre zuständige IT-Betreuung.

3.5 Einstellungen der Browser

Die Internet-Browser verschiedener Herstellerfirmen unterscheiden sich zwar in ihrer Handhabung und Konfiguration, einige Hinweise haben aber allgemeingültigen Charakter. Folgende Punkte sollten Sie beachten:

- Sie sollten während der Nutzung des Wahlsystems „uniWAHL OWS“ darauf verzichten, in einem zweiten Browser-Fenster oder -Tabs andere Internetseiten mit nicht vertrauenswürdigen Inhalten anzuzeigen.

- Die Aktivierung der objektbasierten Programmiersprache JavaScript, die häufig zur Unterstützung von benutzungsbezogenen Funktionen in internetbasierten Anwendungen eingesetzt wird, ist erforderlich.

- Stellen Sie Ihren Browser so ein, dass so genannte Session-Cookies gespeichert werden können.

- Deaktivieren Sie die Funktion, welche Benutzernamen und Kennwörter für die automatische Eingabe bei späteren Aufrufen speichert, d.h. wählen Sie bei einer entsprechenden Abfrage durch Ihren Browser „Anmeldedaten speichern?“ (o.ä.) „Nein“

bzw. „Nicht speichern“ aus.

- Sorgen Sie dafür, dass der sogenannte Browser-Cache (Speicherbereich, in dem zu vorangezeigte Seiten gespeichert werden) des Browsers nach jeder Sitzung gelöscht wird. Durch diese Maßnahme können Sie verhindern, dass die auf dem von Ihnen benutzten Computerarbeitsplatz aufgerufenen Seiten nachträglich angesehen werden können. Sie können die Browser aber auch im „Privaten Modus“ verwenden. Dabei nutzen Sie das Internet, ohne dass der Browser irgendwelche Daten über Ihre Webseitenbesuche auf Ihrem Rechner speichert. Für den Firefox kann der „Private Modus“ unter Windows & Linux mit Shift + CTRL / Strg + P und Mac OSX mit Shift +⌘ + P gestartet werden.

3.6 Sichere verschlüsselte Übertragung

Grundlage einer sicheren Internetverbindung ist die Verwendung eines sicheren Protokolls für die verschlüsselte Übertragung der Daten per SSL[2] . Das Bestehen einer solchen sicheren SSL-Verbindung wird Ihnen bei Verwendung von aktuellen Browsern in der Regel durch ein „geschlossenes Schloss-Symbol“ angezeigt.

Bitte achten Sie darauf, dass nach der Anmeldung am Online-Wahlsystem während der gesamten Verbindungsdauer dieses Symbol dargestellt wird. Durch Doppelklick auf das jeweilige Symbol werden Ihnen weitere Informationen zum Sicherheitszertifikat angezeigt. Die Darstellung ist abhängig von dem von Ihnen eingesetzten Internet-Browser.

Die Serverzertifikate der Wahlserver können Sie anhand der dazu gehörenden sogenannten elektronischen Fingerabdrücke (so genannten Fingerprints) prüfen. Hierzu überprüfen Sie bitte wie zuvor beschrieben die Internet-Adresse (URL), mit der Sie verbunden sind. Die Internetadresse muss während einer Sitzung mit „https://“ angezeigt werden und **nicht** mit „http://“. Das 's' in https signalisiert eine sichere Verbindung. Das Zertifikat des Servers für das Löwenportal für Studierende (https://loewenportal.uni-halle.de) hat folgende Fingerprints:

- SHA-1 Fingerprint:
  5A:7D:43:FA:05:74:F5:00:D5:86:9C:11:8A:E5:E3:49:64:4A:66:2A
- SHA-256 Fingerprint:
  FE:8F:32:0D:EA:40:84:FC:6A:F2:94:47:1B:C8:5A:69:45:43:AC:A2:3D:B5:DF:31:DC:FD:2D:91:EE:06:47:E1

Das Zertifikat des Wahl-Servers (https://uni-halle.gremienwahlen.de/) hat folgende Fingerprints:

- SHA-1-Fingerabdruck:
  6E:A2:85:6A:7A:D0:99:71:09:87:71:A5:19:11:77:C6:0C:A1:55:D9
- SHA-256-Fingerabdruck:
  8E:77:C3:F7:41:31:89:77:FB:A0:80:0E:70:C4:84:C3:69:2D:D9:AF:05:65:57:0C:80:47:BB:50:9D:36:DD:7E

[2] SSL – Secure Sockets Layer bezeichnet ein Netzwerkprotokoll zur sicheren Übertragung von Daten u.a. von Internetseiten

Nur wenn Sie diese Daten angezeigt bekommen, besteht eine sichere und verschlüsselte Verbindung zum Wahlserver. Sollten Sie andere Daten angezeigt bekommen, beenden Sie die Verbindung sofort und informieren Sie bitte umgehend das Wahlamt der Universität (Kontaktdaten siehe unten).

3.7 Schutz vor Computerviren

Ein Computervirus ist ein sich selbst vermehrendes Computerprogramm, das sich in andere Computerprogramme einschleust und sich damit reproduziert. Die Klassifizierung als Virus bezieht sich hierbei auf die Verbreitungs- und Infektionsfunktion. Einmal gestartet, kann es von einer Benutzerin oder einem Benutzer nicht kontrollierbare Veränderungen am Status der Hardware (z.B. Netzwerkverbindungen), am Betriebssystem oder an der Software vornehmen (Schadfunktion). Computerviren können durch von der erstellenden Person gewünschte oder nicht gewünschte Funktionen die Computersicherheit beeinträchtigen. Installieren Sie daher einen Virenscanner auf Ihrem Computerarbeitsplatz und lassen Sie diesen regelmäßig alle Dateien auf Viren überprüfen (scannen). Achten Sie darauf, dass Sie ständig (täglich) die neuesten Aktualisierungen (Updates) einspielen, die alle führenden Herstellerfirmen von Virenscannern anbieten.

3.8 Schutz vor dem Ausspähen von Benutzerdaten

Durch sogenannte „Trojanische Pferde“ (als „Trojanisches Pferd“, auch kurz „Trojaner“ genannt, bezeichnet man ein Programm, das als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen der nutzenden Person eine andere, meist unerwünschte Funktion erfüllt) können vertrauliche Daten ausgespäht und während einer Internetsitzung von Ihnen unbemerkt an Dritte übertragen werden („Phishing“). Dadurch besteht das potenzielle Risiko, dass Ihre Zugangsdaten bei der Eingabe über die Tastatur abgefangen und an Unberechtigte gesendet werden, die dann z.B. an Ihrer Stelle wählen könnten. Einen begrenzten Schutz gegen derartige Trojaner können auch sogenannte „Anti-Spy-Programme“ bieten, die als lizenzierte, kostenpflichtige Produkte oder als Freeware (unentgeltlich nutzbare Computerprogramme) zur Verfügung stehen. Als Spyware wird üblicherweise Software bezeichnet, die persönliche Daten ohne Wissen oder Zustimmung von Nutzerinnen oder Nutzern eines Computers an Dritte sendet. Darüber hinaus sollten Sie auch Software zur Fernwartung (z.B. TeamViewer) deaktivieren, um sicherzustellen, dass keine unbefugte Person den Wahlvorgang mitverfolgen kann und damit das Geheimnis der Wahl verletzt.

3.9 Überwachung des Datenverkehrs vom und zum Internet

Zusätzlichen Schutz vor „Trojanischen Pferden“ können auch sogenannte „Personal Firewalls“ bieten, die als lizenzierte, kostenpflichtige Produkte oder als Freeware zur Verfügung stehen. Dies sind Programme, die, richtig eingestellt, den gesamten Datenverkehr von und zum Internet überwachen. Sie können dadurch erkennen und verhindern, wenn ein anderes Programm als der von Ihnen benutzte Browser versucht, Datenpakete über das Internet zu versenden.

Bezugsquellen für Virenschutz-Software, Personal Firewalls und Anti-Spy-Programme finden Sie in Computer-Zeitschriften sowie an vielen Stellen im Internet.

Weitere nützliche Tipps zum Thema Sicherheit im Internet erhalten Sie auch hier:
https://www.bsi-fuer-buerger.de

4. Hilfestellungen bei Problemen und Fragen

Für die Durchführung des Wahlvorgangs finden Sie im Löwenportal bzw. in der Ihnen per E-Mail zugegangenen Wahlbenachrichtigung eine schriftliche Kurzanleitung. Im Wahlsystem uniWAHL OWS werden Sie zudem Schritt für Schritt durch die Stimmabgabe mit Hinweisen und Erläuterungen durchgeleitet.
Sollten Sie dennoch Fragen dazu haben, können Sie sich gern an das Wahlamt wenden. Dies gilt auch, wenn Sie eine sicherheitsrelevante Unregelmäßigkeit bemerken oder einen Verdacht auf Manipulation haben. In diesem Fall bitten wir um unverzügliche Information.
Sofern sich in Bezug auf Ihren persönlichen Computerarbeitsplatz technische Probleme oder Fragen ergeben sollten, wenden Sie sich bitte unmittelbar an die zuständigen IT-Verantwortlichen in Ihren Bereichen (Fakultät, Institut, Arbeitsgruppe) oder im Zweifel an den Helpdesk des ITZ.

5. Kontakt

Wahlamt der Martin-Luther-Universität Halle-Wittenberg
Barfüßerstraße 17, Hinterhaus
06108 Halle (Saale)

Ansprechpersonen:
Jana Fähling (Tel. 0345/55-21321)
Robert Felsch (Tel. 0345/55-21304)
E-Mail: orgawahlen@uni-halle.de
www.uni-halle.de/wahlen