Sicherheitshinweise
zu den Online-Wahlen der Universität zu Lübeck

1. Allgemeines

Die Wahlen zum Senat der Universität zu Lübeck, zum Senatsausschuss Medizin (SAM) und zum Senatsausschuss Informatik/Technik und Naturwissenschaften (SAMINT) an der Universität zu Lübeck in 2018 werden als Online-Wahlen durchgeführt. Die Online-Wahl erfolgt über einen Webbrowser, welcher bei jedem Betriebssystem standardmäßig vorinstalliert ist. Es wurde versucht, die Online-Wahl-Webseite einfach und intuitiv zu gestalten. Als technische Plattform wird die Anwendung POLYAS der POLYAS GmbH mit der auf die Universität zu Lübeck spezifischen Bedürfnisse angepassten Nutzerführung eingesetzt. POLYAS wurde 2016 durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Deutschland erstmals das Zertifikat für eine Online-Wahl-Software verliehen. Es basiert auf den Common Criteria für Online-Wahlen und dem Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte, die sich aus den allgemeinen Wahlgrundsätzen ableiten. Dementsprechend sind Online-Wahlen in der Konfiguration Polyas CORE 2.2.3 nach Maßgabe der BSI-Anforderungen sicher und erfüllen die Ansprüche an das demokratische Wahlrecht.

2. Briefwahl

Bis zum 7. Juni 2018 kann im Wahlamt ein Antrag auf Briefwahl eingereicht werden. Mit dem Versand oder der Aushändigung der Briefwahlunterlagen sind die Wahlberechtigten von der Online-Wahl ausgeschlossen.

3. Sicherheitshinweise

Allgemeine Sicherheitshinweise

Die Abstimmung durch die Wahlberechtigten erfolgt bei den als Online-Wahl durchgeführten Wahlen auf einem individuell genutzten Computerarbeitsplatz mit Internetanschluss, über welchen 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: um etwa Angriffe durch „Computerviren, Würmer, Trojaner“ (Schadprogramme) oder ähnliche beeinträchtigende Attacken auf den Computerarbeitsplatz oder Wahlservern zu vermeiden oder die Einhaltung des Wahlgeheimnisses zu gewährleisten.

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.

Wahlanwendung

Bei der Online-Wahl kommt die Anwendung POLYAS der POLYAS GmbH (www.polyas.de) zum Einsatz. Diese besteht aus drei technischen Modulen. Das Modul Wählerverzeichnis enthält ein anonymes Verzeichnis, in dem lediglich die Wahlnummern und keine personenbezogenen Daten enthalten sind. Das davon getrennte Modul Wahlfreigabe (Validator) erteilt die Wahlmöglichkeit und das gleichfalls unabhängige Modul Wahlurne wird für die Aufbewahrung und Zählung der Stimmen eingesetzt. Als Übertragungskanal wird bei der Online-Wahl das Internet genutzt. Die Kommunikation zwischen den Modulen erfolgt mittels des als hinreichend sicher geltenden Protokolls „HTTPS" ausschließlich verschlüsselt. Daten, welche auf die persönliche Identität von Wahlberechtigten schließen lassen könnten, werden ausdrücklich NICHT in POLYAS gespeichert. Die Sicherheit der für den Betrieb eingesetzten Server die streng getrennt arbeiten sowie die dort eingesetzten Verfahren werden durch die technischen Betreiber nach allgemein anerkannten Sicherheitsstandards gewährleistet.

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

Zur Durchführung des Wahlvorgangs ist ein handelsüblicher Computerarbeitsplatz mit funktionierendem Internetanschluss erforderlich, wie er in den Einrichtungen der Universität zu Lübeck und auch in vielen Privathaushalten üblich ist. Es wird empfohlen, ausschließlich Computerarbeitsplätze in vertrauenswürdigen Umgebungen zu nutzen, bei denen die grundsätzliche Einhaltung der empfohlenen Sicherheitsmaßnahmen im Allgemeinen sichergestellt wird. Diese Sicherheit wird z.B. in den Computerpools der Universität zu Lübeck gewährleistet. 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.

Benutzer-Autorisierung über den Identity Management Account (IDM)

Alle Wahlberechtigten, die über einen IDM-Account der Universität zu Lübeck verfügen, authentifizieren sich mittels Eingabe des Benutzernamens und des Passworts über das IDM-Selfservice-Portal unter https://idm.uni-luebeck.de. Nach Anmeldung prüft das System, ob die Nutzende oder der Nutzende wahlberechtigt ist und erzeugt daraufhin eine Kachel zum Wahlbereich. In diesem Wahlbereich finden Sie den persönlichen temporären Link (SecureLink) zur Online-Wahl.

Eine erneute Authentifizierung bei POLYAS ist dann nicht mehr notwendig und die Wahlberechtigten können direkt mit der Stimmabgabe beginnen. Die Identität des Wählers ist zu jeder Zeit geschützt.

Geheimhaltung der Zugangsdaten

Bitte achten Sie unbedingt darauf, dass Sie Ihren IDM-Account (Nutzername und Passwort) immer unter Verschluss halten und unberechtigte Dritte keinen Zugriff auf diese Daten bekommen.

Nutzung des Computerarbeitsplatzes ohne administrative Rechte

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

Einsatz von Computerprogrammen aus vertrauenswürdigen Quellen

Installieren und starten Sie keine Programme, die Sie von Unbekannten oder ungefragt von Bekannten per E-Mail oder aus anderen unsicheren Quellen erhalten haben. Vorsicht: Auch Bildschirmschoner sind Programme. Sofern auch nur geringe Zweifel an der Vertrauenswürdigkeit von Programmen bestehen, sollten Sie auf eine Installation auf Ihrem Rechner verzichten.

Software zum Anzeigen von Internetseiten (Browser)

Zur Anzeige der im Internet (World Wide Web) angebotenen Informationen (Webseiten) werden spezielle Computerprogramme (Internet-Browser) zum Betrachten eingesetzt. Achten Sie darauf, dass Sie die eingesetzte Internet-Browser-Software aus vertrauenswürdigen Quellen bezogen haben, so dass sichergestellt ist, dass es sich um unveränderte Originalsoftware handelt. Bitte setzen Sie nur vom Hersteller freigegebene Versionen der Internet-Browser (Firefox, Chrome, Opera, Safari, Edge/Internet Explorer etc.) ein. Beim Bekanntwerden von Sicherheitsproblemen veröffentlichen die Softwarehersteller in der Regel zeitnah fehlerbereinigte Versionen (Updates). Informieren Sie sich daher regelmäßig über neue Sicherheitsupdates für das Betriebssystem und den Internet-Browser Ihres Computerarbeitsplatzes, z.B. für Microsoft-Produkte mit Hilfe der Windows-Update-Funktion.

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 von POLYAS darauf verzichten, in einem zweiten Browser-Fenster andere Internetseiten mit nicht vertrauenswürdigen Inhalten anzuzeigen.

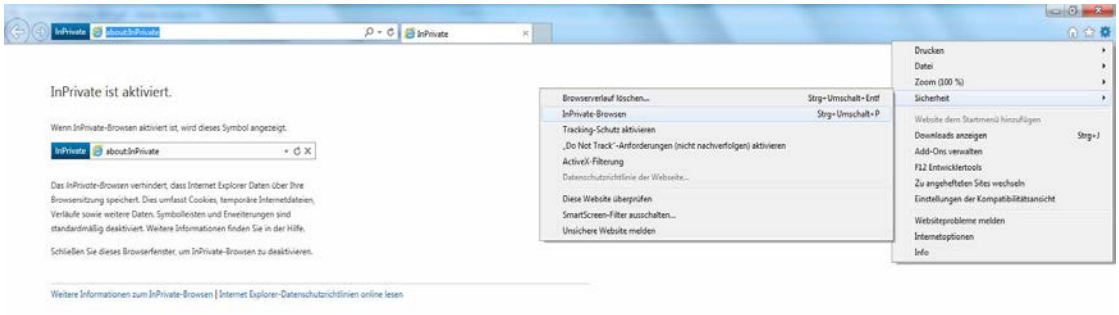
- Die Internetseiten von POLYAS benötigen für ihre Funktionsfähigkeit nicht das von Microsoft entwickelte Softwarekomponenten-Modell ActiveX für die Anzeige aktiver Inhalte. Da mit Hilfe von ActiveX auch Zugriffe auf die Daten und Komponenten Ihres Computers möglich sind, wird empfohlen, ActiveX im Browser generell zu deaktivieren (nur Internet Explorer).

- 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 verschlüsselte Seiten und sogenannte Cookies zum Speichern Ihrer persönlichen Einstellungen auf Webseiten gespeichert werden.

- Deaktivieren Sie die Funktion, welche Benutzernamen und Kennwörter für die automatische Eingabe bei späteren Aufrufen speichert. Beim Internet Explorer finden Sie diese Einstellungen unter „Internetoptionen/Inhalte/AutoVervollständigen“, bei anderen Browsern heißen sie z.B. Kennwort- oder Password-Manager.

- Sorgen Sie dafür, dass der sogenannte Cache (Speicherbereich, in dem zuvor angezeigte 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 Internetexplorer kann das z.B. über die Einstellung/Sicherheit praktiziert werden.



Sichere verschlüsselte Übertragung

Grundlage einer sicheren Internetverbindung ist die Verwendung eines sicheren Protokolls für die verschlüsselte Übertragung der Daten (SSL - Secure Sockets Layer bezeichnet ein Netzwerkprotokoll zur sicheren Übertragung von Daten u.a. von Internetseiten). Das Bestehen einer solchen sicheren SSL-Verbindung wird Ihnen bei Verwendung von Firefox, Chrome und Internet Explorer durch ein geschlossenes Schloss-Symbol angezeigt. Bitte achten Sie darauf, dass nach der Anmeldung am Wahlserver 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 (fingerprints) prüfen. Hierzu überprüfen Sie bitte wie zuvor beschrieben die Internet-Adresse (URL), mit der Sie verbunden sind. Als URL muss „https://idm.uni-luebeck.de/“ bzw. „https://vote.polyas.com“ angezeigt werden. 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 ersten Servers (https://idm.uni-luebeck.de) hat folgende Fingerprints:

- SHA-1 Fingerprint:

  B2 55 F8 16 3E A2 0A 3C 2E 65 E7 87 45 69 69 9A A1 28 BB 7B

- SHA-256 Fingerprint:

  EB 1F D3 C3 94 5F BC 1E CE 97 55 22 B4 0D 3B 90 77 17 50 73 EC 3A 26 F6 39 E1 7D CA 85 CE 62 D1

Das Zertifikat des zweiten Servers (https://vote.polyas.com/) hat folgende Fingerprints:

- SHA-1 Fingerprint :

  0C D0 0B B0 51 68 51 11 CF 4C EE 6E 20 82 DF D7 D1 46 B7 50

- SHA-256 Fingerprint:

  76 39 AD 3E A2 4B C1 63 34 3B FA 7A 13 FB 9C 02 FD C3 44 6F AB 05 DC 3C D6 59 70 FE 2A 85 9B E5

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 über die im Wahlschreiben oder bei POLYAS veröffentlichten Kontaktdaten.

Automatische Zeitüberwachung/Abmelden vom Wahlsystem

Verlassen Sie die Wahl bitte ordnungsgemäß über die Schaltfläche „Wahl abbrechen/Logout“ (oben), wenn Sie den Wahlvorgang ab- oder unterbrechen wollen. Sollten Sie einmal versäumt haben, die Wahlanwendung zu beenden oder längere Zeit Ihren Rechner unbeaufsichtigt lassen, bricht die im System eingebaute Zeitsperre aus Sicherheitsgründen den Wahlvorgang ab, sobald ca. 15 Minuten lang keine Eingabe erfolgt ist. Die von Ihnen durchgeführten Aktionen werden dabei ausdrücklich nicht gespeichert! In beiden vorgenannten Fällen müssen Sie sich daher erneut mit Ihren Zugangsdaten am Wahlserver anmelden und die von Ihnen durchgeführten Aktionen wiederholen.

Schutz vor Computerviren

Ein Computervirus ist ein sich selbst vermehrendes Computerprogramm, welches 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 gewünschten oder nicht gewünschten 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.

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 („Phising“). 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.

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.

Für Mitglieder der Universität zu Lübeck sind folgende Bezugsquellen zu empfehlen:

https://www.itsc.uni-luebeck.de/downloads/software.html

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 weitergehende Fragestellungen steht Ihnen eine ausführliche Wahlanleitung online zur Verfügung:

https://www.uni-luebeck.de/onlinewahlen

Wenn Sie eine sicherheitsrelevante Unregelmäßigkeit bemerken oder einen Verdacht auf Manipulation haben, wenden Sie sich bitte sofort an das Wahlamt der Universität zu Lübeck.

Sofern sich in Bezug auf Ihren persönlichen Computerarbeitsplatz technische Probleme oder Fragen ergeben sollten, wenden Sie sich bitte unmittelbar an die Zuständigen für das Rechnernetz, an das der von Ihnen genutzte Computerarbeitsplatz angeschlossen ist.

Kontakt

Wahlamt der Universität zu Lübeck:

Wahlleitung
Frau Tuğba Karacabey
Tel.: 0451/3101 1051
Fax: 0451 3101 1004
E-Mail: wahlleitung@uni-luebeck.de
Web: https://www.uni-luebeck.de/onlinewahlen

Stellvertretende Wahlleitung
Frau Andrea Köpke
Tel.: 0451/3101 1011
Fax: 0451/3101 1004
E-Mail: wahlleitung@uni-luebeck.de
Web: https://www.uni-luebeck.de/onlinewahlen