Sicherheitshinweise zu den Online-Wahlen der Christian-Albrechts-Universität zu Kiel - 2023 -

Allgemeines

Die studentischen Gremienwahlen der Universität zu Kiel (Erweiterter Senat, Konvente, Studierendenparlament, Fachschaften) werden im Jahr 2023 als Online-Wahl durchgeführt.

Als technische Plattform wird die Wahlsoftware der POLYAS GmbH mit einer auf die spezifischen Bedürfnisse der Universität angepassten Nutzerführung eingesetzt.

Allgemeine Sicherheitshinweise

Die Abstimmung durch die Wahlberechtigten soll bei den als Online-Wahl durchgeführten Wahlen auf einem individuell genutzten Computerarbeitsplatz mit Internetanschluss erfolgen, 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 und um etwa Angriffe durch Computerviren und andere Schadprogramme oder ähnliche beeinträchtigende Attacken auf den Computerarbeitsplatz oder auf Wahlserver zu vermeiden und die Einhaltung des Wahlgeheimnisses zu gewährleisten.

Wahlanwendung

Bei der Online-Wahl kommt die Wahlsoftware 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.
- 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 bei 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 Internet-anschluss erforderlich, wie er in den Einrichtungen der Universität zu Kiel und auch in vielen Privathaushalten üblich ist. Die Nutzung auf mobilen Endgeräten (Smartphone, Tablet etc.) ist möglich, wird aber nicht empfohlen. Es sollten möglichst ausschließlich Computerarbeitsplätze in vertrauenswürdigen Umgebungen genutzt werden, bei denen die grundsätzliche Einhaltung der empfohlenen Sicherheitsmaßnahmen im Allgemeinen sichergestellt wird. Diese Sicherheit wird z.B. in den Computerpools der CAU 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.

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 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 die folgenden Versionen von Internet-Browsern (Firefox, Chrome, Opera, Safari, Edge) 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 des Wahlvorgang 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.

- Deaktivieren Sie die Funktion, welche Benutzernamen und Kennwörter für die automatische Eingabe bei späteren Aufrufen speichert. Beim Internet Explorer finden Sie diese Einstellungen unter „Internet-optionen/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 Firefox kann der „Private Modus“ unter Windows & Linux mit Shift + CTRL / Strg + P und Mac OSX mit Shift + ⌘ + P gestartet 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://urne.uni-kiel.de/CAUwahl2023“ bzw. „https://election.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 hat folgende Fingerprints:

- SHA-1 Fingerprint:
  A0:EF:DA:13:BD:8C:1A:87:CD:69:D3:1C:B7:6B:D1:CA:85:D7:A1:C6

- SHA-256 Fingerprint:
  FD:1D:3B:2E:F1:1F:2B:2A:0A:9B:7B:A6:40:F8:BC:23:77:EC:F8:AF:8D:4A:DD:41:03:BB:23:25:9A:AD:54:CC

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

- SHA-1 Fingerprint :
  A5:2E:2D:05:C3:58:DF:9A:14:3B:58:BF:BC:D4:44:10:3B:D0:B9:8A

- SHA-256 Fingerprint:
  8A:72:DB:F3:42:F2:0D:C8:10:5D:9C:98:4F:91:A7:E4:CA:88:D3:57:D1:E3:AB:00:F6:1D:5F:95:43:C8:AE:C8

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 CAU über gremienwahlen@uv.uni-kiel.de.

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 gewünschte 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. Achten Sie darauf, dass Sie stets die neuesten Updates einspielen, die alle führenden Herstellerfirmen von Virenscannern anbieten.

Überwachung des Datenverkehrs vom und zum Internet

Zusätzlichen Schutz 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.

Das Rechenzentrum der CAU bietet Informationen für Mitglieder der Universität:
https://www.rz.uni-kiel.de/de/angebote/software/software-ueberblick

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