

Sicherheitshinweise zur Nutzung des elektronischen Wahlportals

Die Beachtung der hier empfohlenen Sicherheitsmaßnahmen soll sicherstellen, dass geeignete Vorkehrungen getroffen sind, um Attacken auf das Wahlverfahren zu vermeiden sowie die persönliche Einhaltung des Wahlgeheimnisses zu gewährleisten.

1. Allgemeines

Die Online-Wahl erfolgt über einen beliebigen Webbrowser, der bei jedem Betriebssystem standardmäßig vorinstalliert ist. Es wurde darauf geachtet, das Online-Wahlsystem einfach und intuitiv zu gestalten. Als technische Plattform wird das Online-Wahlsystem uniWAHL OWS der Electric Paper Informationssysteme GmbH (www.electricpaper.de) eingesetzt. Somit kann die Stimmabgabe innerhalb der Wahlfrist orts- und zeitunabhängig erfolgen. Die Online-Wahlen über uniWAHL OWS erfüllen die Ansprüche an das demokratische Wahlrecht und die Anforderungen des Bundesamts für Sicherheit in der Informationstechnik (BSI). Die Plattform nutzt fortschrittliche Verschlüsselungstechnologien und Mix-Netzwerk-Verfahren, um die Integrität und Vertraulichkeit der Wahlstimmen zu gewährleisten. Sie können Ihre Stimmabgabe unterbrechen und sich bis zum Ablauf des letzten Wahltages abermals am Portal anmelden. Es erfolgt keine Zwischenspeicherung der zuvor vorgenommen Vorauswahl vor Stimmabgabe.

2. Technische Sicherheitsanforderungen an das Endgerät

Die Durchführung der Wahl erfordert ein handelsübliches Gerät mit konstantem Internetanschluss. Sie müssen den für die Stimmabgabe genutzten Computer nach dem jeweils aktuellen Stand der Technik angemessen gegen Angriffe Dritter von außen schützen. Es wird dringend empfohlen, nur Geräte in vertrauenswürdigen Umgebungen zu verwenden, bei denen Sicherheitsmaßnahmen wie aktuelle Antivirensoftware und Firewalls installiert sind, um den Computer vor Angriffen durch Schadsoftware wie Viren, Würmer oder Trojaner zu schützen. Die genutzten Browser sollten stets auf dem neuesten Stand sein, um bekannte Sicherheitslücken zu vermeiden. Es sollten nur Programme aus vertrauenswürdigen Quellen installiert werden.

3. Nutzung des EDV-Endgerätes 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.

4. Einstellungen des Browsers

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 der Wahlkabine von Electric Paper darauf verzichten, in einem zweiten Browser-Fenster andere Internetseiten mit nicht vertrauenswürdigen Inhalten anzuzeigen.
- Die Internetseiten von Electric Paper 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 „Internetoptionen > Inhalte > AutoVervollständigen“, bei anderen Browsern heißen sie z.B. Kennwort- oder Password-Manager.

5. Geheimhaltung

Zur Sicherung einer geheimen Wahl müssen Sie dafür Sorge tragen, dass Sie Ihre Stimme unbeobachtet abgeben können. Die Zugangsdaten, die zur Authentifizierung für die Online-Wahl benötigt werden, dürfen nicht an Dritte weitergegeben werden. Die Wähler/innen sind selbst dafür verantwortlich, dass ihre Zugangsdaten sicher aufbewahrt werden. Nach der Stimmabgabe wird der Zugang zum Stimmzettel gesperrt, sodass keine nachträglichen Änderungen vorgenommen werden können. Hierzu wird Ihre Zugangsnummer von Electric Paper als „verbraucht“ gespeichert. Selbstverständlich ist kein Rückschluss von dieser Nummer auf die Art und Weise der Stimmabgabe möglich.

6. Verschlüsselung und sichere 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 Wahlsystem uniWAHL OWS verwendet HTTPS-Verschlüsselung zur sicheren Übertragung aller Daten zwischen den Wähler:innen und den Servern. Das Bestehen einer solchen sicheren SSL-Verbindung wird Ihnen bei Verwendung von Edge, Firefox und Chrome 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://ihk-coburg.gremienwahlen.de` 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 Onlinewahl-Servers hat folgende Fingerprints:

· SHA-1 Fingerprint :

BD:8B:EE:A5:F8:B9:D5:A2:FC:E1:52:3E:D6:47:0D:E4:CA:E6:C4:44

· SHA-256 Fingerprint:

51:66:89:DF:E8:4D:6B:6F:F9:B8:A7:A7:A4:A5:9A:10:78:D4:26:52:A9:7F:96:90:A9:18:92:8F:9B:B0:AA:33

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 Hochschule über die im Wahlschreiben oder bei uniWAHL veröffentlichten Kontaktdaten.

7. Anonymisierung der Stimmabgabe

Im Wahlsystem uniWAHL OWS erfolgt die Anonymisierung der Stimmabgabe, indem nach der Stimmabgabe die verschlüsselten Stimmzettel in einem Mixnet-Verfahren zufällig gemischt werden und so keiner Person mehr zugeordnet werden können. Die Integrität des Wahlvorgangs wird zusätzlich durch die Pseudonymisierung der Wählenden sichergestellt.

8. Schutz vor Computerviren

Ein Computervirus ist ein sich selbst vermehrendes Computerprogramm, welches sich in andere Computer-programme 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 Virens scanner 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 Virens cannern anbieten.

9. Vermeidung von Phishing und Datenlecks

Phishing-Angriffe zielen darauf ab, sensible Informationen wie Zugangsdaten abzufangen. Um das Risiko solcher Angriffe zu minimieren, sollte man auf verdächtige E-Mails oder Webseiten achten und

keine unbekannten Links anklicken. Zusätzlich sollten keine Remote-Access-Programme wie TeamViewer aktiviert sein, um das Wahlgeheimnis zu schützen.

10. Automatische Abmeldung und Sitzungsablauf

Um die Sicherheit des Wahlvorgangs zu gewährleisten, wird eine automatische Abmeldung vom Wahlsystem nach einer bestimmten Inaktivitätszeit vorgenommen. Wähler:innen müssen sich nach einer solchen Abmeldung erneut einloggen, um die Stimmabgabe fortzusetzen. Die von Ihnen durchgeführten Aktionen werden dabei ausdrücklich nicht gespeichert! Sie müssen sich daher erneut mit Ihren Zugangsdaten am Wahlserver anmelden und die von Ihnen durchgeführten Aktionen wiederholen.

11. Weitere Tipps zum Thema Sicherheit im Internet

Weitere Informationen und nützliche Tipps zum Thema Sicherheit im Internet erhalten Sie beim Bundesamt für Sicherheit in der Informationstechnik unter <http://www.bsi-fuer-buerger.de>.

Wenn Sie eine sicherheitsrelevante Unregelmäßigkeit bemerken oder einen Verdacht auf Manipulation haben, wenden Sie sich bitte sofort an den Wahlausschuss.

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.