Sichere verschlüsselte Übertragung

Grundlage einer sicheren Internetverbindung ist die Verwendung eines sicheren Protokolls für die verschlüsselte Übertragung der Daten per SSL (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. Die Internetadresse muss während einer Sitzung mit „https://“ angezeigt werden und **nicht** mit „http://“. Das 's' in https signalisiert eine sichere Verbindung.

Das Zertifikat Servers für das Löwenportal für Studierende (https://loewenportal.uni-halle.de/) hat folgende Fingerprints:

- SHA-1 Fingerprint:

  01:57:99:E2:B4:E6:7E:6F:A2:A6:36:A3:6C:3B:F8:34:8F:39:38:4A

- SHA-256 Fingerprint:

  ED:A7:1A:DF:21:F3:5D:39:2C:91:39:A4:6A:12:BE:5B:AA:15:0D:AA:58:F4:5E:03:9B:B2:8C:CA:A0:B2:34:2A

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

- SHA-1 Fingerprint :

  34 58 82 2D 3A 0D 1C 78 D2 14 78 56 1F 08 1E 2A 71 C4 27 0D

- SHA-256 Fingerprint:

  0D 15 9F 30 41 04 4C 9D AD 59 1D F4 1A 69 32 CD 5F 44 7D 9E 05 10 DD BB 98 F5 C5 A0 27 94 5F 3D

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).

Automatische Zeitüberwachung/Abmelden vom Wahlsystem

Verlassen Sie die Wahl bitte ordnungsgemäß über die Schaltfläche „Stimmabgabe abbrechen“, 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, 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.

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.

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. Zur von der Universität verwendeten Software „Sophos Endpoint Security“ finden Beschäftigte Informationen auf dieser Webseite des ITZ: https://www.itz.uni-halle.de/dienstleistungen/sophos/

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

3. Hilfestellungen bei Problemen und Fragen

Für die Durchführung des Wahlvorgangs finden Sie im Löwenportal bzw. in der Ihnen per E-Mail oder Post zugegangenen Wahlbenachrichtigung eine schriftliche Kurzanleitung. Im Wahlsystem von Polyas werden Sie zudem Schritt für Schritt durch die Stimmabgabe mit Hinweisen und Erläuterungen durchgeleitet. Sollten Sie dennoch Fragen dazu haben, können Sie sich 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.

Kontakt

Wahlamt der Martin-Luther-Universität Halle-Wittenberg
AnsprechpartnerIn:
Jana Fähling (Tel. 0345/55-21321)
Robert Felsch (Tel. 0345/55-21304)
orgawahlen@verwaltung.uni-halle.de
www.uni-halle.de/wahlen