stupa
Wahlausschuss

Sicherheitshinweise zu den Wahlen zum Studierendenparlament und den Fachschaftsräten

1. Allgemeines

Die Wahlen zu den Gremien der Hochschule Niederrhein im Sommersemester 2018 werden als internetbasierte Onlinewahlen durchgeführt.

Die Onlinewahl ist browserbasiert und betriebssystemunabhängig weltweit von den EDV-Endgeräten der Wahlberechtigten ohne Installation einer Spezialsoftware möglich sowie einfach und intuitiv zu navigieren. Als technische Plattform wird das Wahlsystem POLYAS der POLYAS GmbH mit der auf die Bedürfnisse der Studierendenschaft der Hochschule Niederrhein angepassten Nutzerführung des Wahlsystems eingesetzt. An POLYAS wurde 2016 durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Deutschland erstmals das Zertifikat für eine Onlinewahl-Software erteilt. Es basiert auf den Common Criteria für Onlinewahlen und dem Basisatz 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. Sicherheitshinweise

Die Abstimmung durch die Wahlberechtigten erfolgt bei den als Onlinewahl 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 und Angriffe durch ‚Computerviren, Würmer, Trojaner" (Schadprogramme) und ähnliche dienstebehindernde Attacken auf dem Computerarbeitsplatz und auf den Wahlservern zu vermeiden

sowie die persönliche Einhaltung des Wahlgeheimnisses zu gewährleisten.

Die Wahlanwendung ist grundsätzlich für alle berechtigten Nutzerinnen und Nutzer unabhängig von deren körperlichen und / oder technischen Möglichkeiten weitgehend uneingeschränkt ohne besondere Erschwernis und in der allgemein üblichen Weise zugänglich und kann grundsätzlich ohne fremde Hilfe genutzt werden (barrierearm). 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.

Bei der Onlinewahl kommt das Wahlsystem POLYAS der POLYAS GmbH (www.polyas.de) zum Einsatz. Das Wahlsystem 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 Onlinewahl 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 im Wahlsystem 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.

Zur Durchführung des Wahlvorgangs ist ein handelsüblicher Computerarbeitsplatz mit funktionierendem Internetanschluss erforderlich, wie er in den Einrichtungen der Hochschule Niederrhein 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 Hochschule Niederrhein 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.

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 (Browser) zum Betrachten eingesetzt. Achten Sie darauf, dass Sie die eingesetzte Browser-Software aus vertrauenswürdigen Quellen bezogen haben, sodass sichergestellt ist, dass es sich um unveränderte Originalsoftware handelt. Bitte setzen Sie nur vom Hersteller freigegebene Versionen der Internet-Browser (Firefox, Mozilla, Opera, Safari, Netscape bzw. 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 Browser Ihres Computerarbeitsplatzes, z.B. für Microsoft - Produkte mit Hilfe der Windows-Update-Funktion oder mit dem Internet Explorer unter http:\\windowsupdate.microsoft.com.

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 darauf verzichten, in einem zweiten Browser-Fenster andere Internetseiten mit nicht vertrauenswürdigen Inhalten anzuzeigen. Die Internetseiten des Wahlsystems 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 ebenfalls nicht erforderlich. Stellen Sie Ihren Browser so ein, dass verschlüsselte Seiten und sogenannte Cookies zum Speichern Ihrer persönlichen Einstellungen auf Webseiten nicht 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 "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.

Grundlage einer sicheren Internetverbindung ist die Verwendung eines sicheren Protokolls für die verschlüsselte Übertragung der Daten (SSL oder 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, Mozilla und MS Internet Explorer durch ein geschlossenes Schloss-Symbol angezeigt, bei Netscape durch die Darstellung eines

ungebrochenen Schlüsselsymbols. Bitte achten Sie darauf, dass nach der Anmeldung am Wahlsystem während der gesamten Verbindungsdauer dieses Symbol ungebrochen dargestellt wird. Durch Doppelklick auf das jeweilige Symbol werden Ihnen weitere Informationen zum Sicherheitszertifikat angezeigt. Die Darstellung ist abhängig von der von Ihnen eingesetzten Browserversion.
Die Serverzertifikate der Wahlserver können Sie anhand der dazu gehörenden sogenannten elektronischen Fingerabdrücke (fingerprints) prüfen.

Verlassen Sie das Wahlsystem bitte ordnungsgemäß über die Schaltfläche "Wahl abbrechen / ausloggen" (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 Wahlsystem 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 Wahlsystem anmelden und die von Ihnen durchgeführten Aktionen wiederholen.

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 Benutzerin oder 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)

Als Troyanische Pferde, kurz auch ‚Troyaner“ 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 die Geheimheit der Wahl verletzt.

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 Programmals der von Ihnen benutzte Browser versucht, Datenpakete über das Internet zu versenden.

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 auf der Seite des Bundesamtes für Sicherheit in der Informationstechnik; http://www.bsi-fuer-buerger.de.

3. Hilfestellungen bei Problemen und Fragen

Für Fragestellungen steht Ihnen darüber hinaus auch eine sehr ausführliche Wahlanleitung online im Wahlsystem zur Verfügung. Wenn Sie eine sicherheitsrelevante Unregelmäßigkeit bemerken oder einen Verdacht auf Manipulation haben, wenden Sie sich

bitte sofort an den Wahlausschuss des Studierendenparlaments der Hochschule Niederrhein.

Kontaktinformationen
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:
Wahlausschuss der Studierendenschaft
der Hochschule Niederrhein
Wahlleiter: Marco Patriarca (marco.patriarca@stud.hn.de)

Standort Krefeld:
Alderstraße 35, 47798 Krefeld

Standort Mönchengladbach:
Webschulstraße 20, 41065 Mönchengladbach