



INFORMATION FÜR GI-MITGLIEDER ZU MÖGLICHEN SICHERHEITSPROBLEMEN AUF CLIENTENSEITE BEI VORSTANDS- UND PRÄSIDIUMSWAHLEN MIT DEM ONLINEWahlVERFAHREN:

Bei der diesjährigen GI-Vorstands- und Präsidiumswahl wird – wie bereits im Vorjahr - neben der traditionellen Briefwahl eine Wahl mittels eines Onlinewahlverfahrens der Firma Micromata angeboten.

Bei diesem Verfahren werden an zentraler Stelle jeweils ein Server für die Prüfung der Wahlberechtigung und ein Urnenserver für die Zählung der Stimmen eingesetzt. Für die Sicherheit dieser Server - die streng getrennt arbeiten - sowie für die dort eingesetzten Verfahren sind auf der einen Seite die GI sowie auf der anderen Seite die Firma Micromata verantwortlich. Als Übertragungskanal wird das Internet vermittels des (als hinreichend sicher geltenden) Protokolls https genutzt.

Die Abstimmung eines jeden Mitglieds selbst erfolgt bei Einsatz des elektronischen Wahlverfahrens auf einem Clienten mit Internetanschluss, über welchen die Stimmen an die Wahlserver übertragen wird. Für die Sicherheit der Clienten ist das jeweilige Mitglied verantwortlich. Angesichts der bekannten Unsicherheit praktisch aller heute eingesetzter Clientsysteme muss die Wahlleitung davon ausgehen, dass an dem elektronischen Wahlverfahren teilnehmende GI-Mitglieder geeignete Vorkehrungen treffen, um ein Mindestmaß an Sicherheit zu erreichen und unliebsame Vorfälle wie "virale, wurmige, trojanische oder dienstbehindernde" Angriffe auf die Wahlserver zu vermeiden und die lokale Einhaltung des Wahlgeheimnisses zu gewährleisten. Hierzu werden an vielen Stellen „Best Practice“-Regeln angewendet, oft als „Goldenen Regeln der Client-Sicherheit“ bezeichnet.

Exemplarisch wird anliegend der Best Practice-Katalog der Sicherheitsfirma F-Secure angefügt, welchen der Sprecher der Fachgruppe „Sicherheit in Mobil- und Festnetzen (NetSEC)“ im FB SICHERHEIT der Gesellschaft für Informatik aus seiner beruflichen Praxis zur Verfügung gestellt hat. Die Sicherheit der Wahlsoftware wurde von einem GI-Expertenteam geprüft. Angesichts der Vielfalt von Clienten konnte dabei aber die Sicherheit einzelner Client-Betriebssysteme nicht geprüft werden.

Diese Gruppe hält einvernehmlich die Sicherheit des Wahlsystems als für einen weiteren experimentellen Einsatz angemessen, zumal Mitglieder bei Bedenken auf die Briefwahl zurückgreifen können.

Bei Fragen steht Ihnen das Onlinewahlteam unter onlinewahlen@gi-ev.de gerne zur Verfügung



BEST PRACTICE REGELN: „TIPPS FÜR SICHERES SURFEN UND E-MAILEN“

1. Halten Sie Betriebssystem und Applikationen auf aktuellem Stand und installieren Sie Patches (nur die vom Hersteller!), sobald diese verfügbar sind. Ein Antiviren-Programm mit aktuellen Signaturen und eine lokale Firewall sind ebenfalls Stand der Technik.
2. Verwenden Sie Attachements nur, wenn unbedingt notwendig (Senden und Empfangen!), da sie Programmteile enthalten und somit unvorhergesehene Wirkungen entfalten können. Blenden Sie bei Word-Attachments die Makros aus.
3. Konfigurieren Sie Windows so, dass Dateinamenerweiterungen immer angezeigt werden (im Explorer im Menü Extras/Ordneroptionen/Ansicht den Haken bei "Dateinamenerweiterungen bei bekannten Dateitypen ausblenden" entfernen).
4. Öffnen Sie niemals Attachments mit Dateinamenerweiterungen COM, VBS, SHS, PIF, BAT, CLP, EXE. Diese werden fast ausschließlich von Würmern und Viren verwendet, um sich zu verbreiten.
5. Öffnen Sie niemals Attachments mit doppelter Dateinamenerweiterung z.B.: Datei.BMP.EXE oder Datei.TXT.VBS (Ohne den Tipp 3 können Sie dies aber nicht erkennen!!!)
6. Vermeiden Sie Dateifreigaben für andere. Tauschen Sie Dateien über Server aus. Geben Sie niemals das ganze Laufwerk frei, sondern immer nur einzelne Unterverzeichnisse, nach Möglichkeit als "Nur lesen".
7. Trennen Sie den Rechner vom Modem oder Netzkabel, wenn Sie diese Verbindungen nicht benötigen.
8. Wenn Ihnen eine E-Mail von einem Bekannten merkwürdig vorkommt (andere Sprache, ungewöhnliche Wortwahl), fragen Sie Ihren Bekannten, bevor Sie ein Attachment öffnen.
9. Wenn Sie SPAM erhalten, öffnen Sie keine Attachements und klicken Sie nie auf angezeigte Links! Vertrauen Sie keiner E-Mail eines Absenders, der vorgibt, Ihre Bank zu sein und der zu Ihrer Sicherheit Ihre PIN oder TANs abfragt. Folgen Sie niemals den Links in einer solchen E-Mail, öffnen Sie niemals deren Attachments.
10. Attachements mit "sexuellen" Dateinamen wie PORNO.EXE oder PAMELA_NUDE.PIF stammen häufig von Würmern, um den Anwender neugierig zu machen. NICHT öffnen!
11. Vertrauen Sie niemals einer angezeigten Ikone eines Attachements. Würmer versenden ausführbare Dateien mit falschen Ikonen, um dem Anwender einen anderen Dateityp oder ein Verzeichnis vorzutäuschen.
12. Nehmen Sie niemals Dateien über IRC, ICQ, AOL Instant Messenger oder VoIP an. Nutzen Sie keine Peer-to-Peer Netze.
13. Nutzen Sie keine gehackte Software - abgesehen davon, dass es sich um eine Straftat handelt, öffnen Sie Ihr System für Viren und Trojaner!

(Quelle: (c) F-Secure Deutschland)