POLYAS

FAQ ZUR IT-SICHERHEIT

In diesem Dokument finden Sie Antworten auf häufig gestellte Fragen zur IT-Sicherheit bei POLYAS. Für weitere Rückfragen stehen Ihnen unsere Wahlexperten zur Verfügung.

Wo stehen die POLYAS Server?

Unsere Server stehen ausschließlich in Deutschland. Die Web-Server, die die Anwendung zur Verfügung stellen, sind über das Internet erreichbar. Sie stehen in einem Netzwerk mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die angeschlossenen Rechner und werden so gegen Angriffe aus dem Internet geschützt.

Nutzt POLYAS Cloud-Lösungen zur Speicherung von Wahl- und Wählerdaten?

Die Wählerdaten liegen ausschließlich auf den Servern von ISO 27001 zertifizierten Rechenzentren bzw. in einer nach TCDP 1.0 (Trusted Cloud Data Protection) zertifizierten Cloud in Deutschland.

Inwieweit trackt POLYAS das Wählerverhalten im Browser?

Zum Schutz Ihrer Daten und des Wahlgeheimnisses ist das Wahlsystem so aufgebaut, dass ein Tracking des Wählerverhalten im Browser nicht möglich ist.

Werden Cookies genutzt?

Ja, allerdings nur von der Anwendung selbst und nicht von anderen Websites oder Diensten.

Welche Browserversionen unterstützt POLYAS?

Generell gilt, dass unser Wahlsystem kompatibel mit allen gängigen Internetbrowsern funktioniert. So wurde das POLYAS Online-Wahlsystem durch uns mit folgenden Browsern erfolgreich getestet:

- ✓ Chrome
- ✓ Firefox
- ✓ Internet Explorer (ab Version 11)
- ✓ Opera
- ✓ Safari
- ✓ Edge

Wichtig ist jedoch, dass die Wähler ihren Browser regelmäßig updaten, um die Sicherheit ihrer Internetverbindung zu wahren und die Online-Wahl problemlos durchzuführen.

Wann genau wird das Token für den Wähler erzeugt?

Das Token wird bei der ersten erfolgreichen Anmeldung des Wahlberechtigten am Wahlsystem durch den Validator erzeugt, der es anschließend verschlüsselt an die Wahlurne und das Wählervetrzeichnis überträgt. Das Wählerverzeichnis wiederum sendet das Token an den Browser des Wahlberechtigten. Nun kann anhand des Tokens der Wahlberechtigte seine Stimmabgabe gleichzeitig geheim und eindeutig tätigen. Ebenso wird auf diese Weise sichergestellt, dass pro Wähler nur eine Stimmabgabe erfolgen kann. Hat der Wähler seine Stimme verbindlich abgegeben, wird das Token aus dem Wählerverzeichnis gelöscht, so dass keine erneute Stimmabgabe mehr erfolgen kann.

POLYAS

INFORMATIONEN ZUR IT-SICHERHEIT

Wie sieht die Sicherheit der Systeme bezüglich der Kundendaten aus?

Wir setzen auf den hohen Schutz von personenbezogenen Daten. Die Kundendaten befinden sich auf den Servern von ISO 27001-zertifizierten Rechenzentren bzw. in einer nach TCDP 1.0 (Trusted Cloud Data Protection) zertifizierten Cloud in Deutschland. Generell werden Zugriffsberechtigungen auf Kundendaten durch ein Rollenkonzept eingeschränkt. Es existieren auch entsprechende Archivierungs und Löschkonzepte.

Darf die IT-Abteilung des Kunden Pentests durchführen?

Ja, allerdings nur nach Absprache mit POLYAS.

Welche SSL-Protokoll-Version verwendet POLYAS?

Das Wahlsystem, das unter election.polyas.com erreichbar ist, lässt die Version TLS 1.0 nicht mehr zu. Unterstützt werden nur noch die Versionen TLS 1.1 und TLS 1.2. Das Wahlsystem verwendet beispielsweise TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256. Dies entspricht den Maßgaben der BSI TR-02102-2.

Werden Schlüsselgrößen zur Verschlüsselung gemäß BSI TR-02102-1 eingehalten?

Ja. POLYAS verwendet zur TLS-Verschlüsselung beispielsweise die Cipher Suite "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256". Für die Verschlüsselung der Stimmen kommen als symmetrisches Verfahren AES-128 und als Public-/Private-Key Verfahren derzeit RSA-2048 zum Einsatz.

Welche Klasse hat das Serverzertifikat des POLYAS Online-Wahlsystems?

Das POLYAS Online-Wahlsystem verfügt über ein Serverzertifikat der Class 3 (D-TRUST SSL Class 3 CA 1 EV 2009).

Wie werden Zugangsdaten, insbesondere Passwörter gespeichert?

Passwörter werden ausschließlich als Salted Hash (mit jeweils individuellem Salt) gespeichert.

Unterstützt POLYAS StartTLS, zur verschlüsselten Kommunikation der Mailserver?

StartTLS wird von dem auslieferenden Mailserver bevorzugt verwendet, sodass bei Verfügbarkeit von StartTLS im SMTP-Verbindungsaufbau eine verschlüsselte Übertragung auf dem Transportweg stattfindet.

Welche Standards und Verfahren setzt POLYAS zur Generierung der Zufallszahlen ein?

Wir nutzen den Zufallszahlengenerator SecureRandom von Java. Dieser ist erfüllt die "FIPS 140-2, Security Requirements for Cryptographic Modules, section 4.9.1."-Spezifikationen. Das von uns verwendete Token ist 128 Bit lang (dies entspricht 32 Hex-Zeichen) und somit in der gleichen Sicherheitsklasse wie die TLS Transportverschlüsselung (AES-128).

Haben Sie weitere Fragen? Die POLYAS Online-Wahlexperten beraten Sie gerne!

Kontakt

POLYAS GmbH
Boxhagener Str. 18
10245 Berlin

www.polyas.de
Mail: kontakt@polyas.de