POLYAS

INFORMATIONEN ZUR IT-SICHERHEIT

In diesem Dokument finden Sie Antworten auf häufig gestellte Fragen zur IT-Sicherheit bei POLYAS.

Wo stehen die POLYAS Server?

Unsere Server stehen ausschließlich in Deutschland. Der Web-Server, der die Anwendung zur Verfügung stellt, ist über das Internet erreichbar und steht hinter einer Firewall in einer DMZ (Demilitarisierte Zone = Netzwerk mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die angeschlossenen Rechner) und wird 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 tracken Sie das Wählerverhalten im Browser?

Aufgrund der Datenschutzbestimmungen und des Wahlgeheimnisses ist es nicht möglich das Wählerverhalten im Browser zu tracken.

Werden Cookies genutzt?

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

Welche Browserversionen unterstützt POLYAS?

Generell gilt, dass unser Wahlsystem kompatibel mit allen gängigen Internetbrowsern funktioniert. So können wir die reibungslose Nutzung des POLYAS-Online-Wahlsystems mit folgenden Browsern gewährleisten:

- ✓ Chrome
- ✓ Firefox
- ✓ Internet Explorer
- ✓ Opera
- ✓ Safari

Wichtig ist jedoch, dass die Wähler ihren Browser regelmäßig updaten, um die Sicherheit Ihrer Internetverbindung zu wahren.

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 überträgt. Denn nur auf diese Weise kann eine doppelte Stimmabgabe verhindert werden.

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.

POLYAS

INFORMATIONEN ZUR IT-SICHERHEIT

Darf unsere IT-Abteilung Pentests durchführen?

Ja, allerdings nur nach Absprache mit POLYAS.

Welche SSL-Protokoll-Version verwendet POLYAS?

Die URL polyas.com (IP-Adresse: 136.243.32.200) lässt Version TLS 1.0 und alle neueren TLS Versionen zu, damit auch ältere Browserversionen das Wahlsystem im Konfigurator bedienen können. Präferiert genutzt werden jedoch die Versionen TLS 1.1. und TLS 1.2, sofern der Browser diese unterstützt. Das Wahlsystem, das unter vote.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.. Im Wahlsystem wird außerdem TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 verwendet.

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).

Wird Cipher BSI TR-02102-21 (Datenverschlüsselungsstandard BSI) eingehalten?

Ja. POLYAS wendet folgenden Standard in der Verschlüsselung an: Cipher Suite "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256".

Werden Zugangsdaten als Salted Hash übertragen?

Nein. Allerdings werden die Zugangsdaten als Salted Hash gespeichert.

Unterstützt POLYAS StartTLS, sodass die Kommunikation der Mailserver verschlüsselt erfolgt?

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

Nach welchen Standards und Verfahren werden die Zufallszahlen der Anwendung generiert?

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).