Technisch-organisatorische Maßnahmen gemäß Anlage §9 BDSG

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerparteiliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogen Daten oder Datenkategorien geeignet sind, folgende Sicherheitmaßnahmen zu gewährleisten:

1. Zutrittskontrolle
2. Zugangskontrolle
3. Zugriffskontrolle
4. Weitergabekontrolle
5. Eingabekontrolle
6. Auftragskontrolle
7. Verfügbarkeitskontrolle
8. Trennungsgebot

Zutrittskontrolle

Zu den von der BundesIT benutzten Rechnern haben nur Mitarbeiter des beauftragten Hosting-Providers Zugriff, welche sich mit Hilfe von technischen Systemen identifizieren und authentisieren müssen. Somit wird sichergestellt dass Unbefugte nicht in das Rechenzentrum und an die Rechner der BundesIT Zugriff erhalten können. Das Core-Team der BundesIT hat nach Anmeldung Zugang zu den Rechnern.

Zugangskontrolle

Auf Betriebssystemebene (Shellzugriff, gegenebenfalls Zugriff auf GUIs) gibt es nur mit Hilfe von verschlüsselten Verbindungen (SSH) Zugriff auf die von uns verwalteten Systeme. Für besonders schützenswerte Systeme wird zusätzlich OpenVPN zur Authentisierung des Client-Rechners eingesetzt. Jeder Administrator hat sich mit seinem persönlichen Account anzumelden. Jeder Systemadministrator hat – wenn er angemeldet ist – die Möglichkeit, via sudo-Kommando administrative Kommandos auszuführen. Applikations-Administratoren haben keinen SSH-Zugriff. Wenn dieser benötigt werden sollte, wird via sudo der Zugriff auf seine Werkzeuge eingeschränkt.

Der Zugriff auf den Server direkt führt über einen Jump-Host für die Systemadministratoren.

Auf Applikationsseite haben Administratoren und Mitarbeiter ein personalisiertes Login, welches

über ACLs die Rechte regelt.

Zugriffskontrolle

Die Zugriffskontrolle auf Betriebssystem-Ebene wird systemseitig mit sudo-Berechtigungen realisiert. Die Administratoren sind in verschiedenen Gruppen, denen via sudo Adminstrations-Berechtigungen gegeben werden. Somit wird sichergestellt, dass jeder Administrator nur die Berechtigungen erhält die er für seine Tätigkeit braucht. Zusätzlich wird in einer Protokolldatei jeder Befehl, der getippt wird, für 2 Wochen gespeichert.

Applikationsbenutzer müssen personalisierte Account benutzen. Generische Accounts sind nur für Systemdienste wie cron erlaubt, da jederzeit zurückverfolgbar sein muss, welche Änderungen von welcher Person durchgeführt wurden.

Auf Datenbankebene gibt es ebenfalls Zugriffsberechtigungen, die personalisiert gesetzt werden. Datenbanken lassen keine Verbindungen von aussen zu, nur von localhost oder dem Datenbank-Netz.

Applikationen der BundesIT auf externen Cloud-Systemen zu nutzen ist nicht erlaubt.

Weitergabekontrolle

Daten dürfen nur via scp oder andere sichere Transportwege ausserhalb der Applikationslogik auf die Maschinen kopiert werden. Nur berechtigte Administratoren können dies (siehe Zugriffskontrolle) durchführen. Es dürfen keine Daten von den Maschinen auf andere Rechner, die nicht zur BundesIT gehören, kopiert werden

Die benutzten Newsserver feeden ihre Nachrichten an die anderen beteiligten Newsserver der Piratenpartei, aber nicht an externe Server.

Eingabekontrolle

Lediglich Administratoren, die dazu berechtigt sind, dürfen Daten erheben, verarbeiten oder nutzen. Auf Applikationsebene wird dies über die Zugangsberechtigung und – wo vorhanden – über die Applikation protokolliert.

Auftragskontrolle

Auftragnehmer für eine Auftragsdatenverarbeitung werden unter anderem nach datenschutzrechtlichen Kriterien ausgewählt. Mit allen Auftragnehmern der BundesIT wird eine Datenschutzvereinbarung abgeschlossen, in der getroffene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten hinterlegt sind. Ebenso werden Art und Umfang der beauftragten Verarbeitung und Nutzung der personenbezogenen Daten erfasst. Es wird auf die Zweckbindung der personenbezogenen Daten sowie das Verbot der Nutzung durch den Dienstleister außerhalb des schriftlich formulierten Auftrags hingewiesen. Der Datenschutzbeauftragte wird in regelmäßigen Abständen die technisch-organisatorischen Maßnahmen des Auftragnehmers überprüfen.

Verfügbarkeitskontrolle

Es wird täglich von allen Systemen ein Filesystem-FullBackup; bei Datenbanken ein Dump der Datenbanken erstellt.

Diese Backups werden auf unserem Storage gespeichert. Damit sind sie innerhalb unserer

Umgebung schnell verfügbar; gleichzeitig sind sie nur von den Rechner aus ansprechbar (IP-Adresse), die innerhalb unseres intenen Netzes erreichbar sind..

Aktuell halten wir die letzten sieben Tage, ein wöchtentliches und drei monatliche Backups vor. Die Ausnahme sind wichtige Systeme wie unsere Mitgliederverwaltung, bei denen mehr Generationen revisionssicher aufbewahrt werden.

Alle Maschinen sind durch redundante Netzteile und/oder eine unterbrechungsfreie Stromversorgung vor Stromausfall geschützt. Falls der Hauptstrom ausfällt hat der Hoster einen entsprechend starken Diesel-Generator der für die Überbrückungszeit den notwendigen Strom liefert.

Trennungsgebot

Applikationsdaten werden getrennt voneinander in verschiedenen Datenbank-Schemata oder -instanzen gespeichert. Jeder Benutzer und jede Applikation hat nur auf die Daten Zugriff, auf die er bzw. sie Zugriff braucht.