Sicherheits- und Betriebskonzept (SBK)

Ausgabe Mai 2019

1. Sicherheit

1.1. Datenhaltung

Auf den Servern von **vemap (Datenhaltung ausschließlich in Österreich)** werden wichtige Daten verschiedener Unternehmen (privater und öffentlicher Auftraggeber) ausgetauscht. Um den Anforderungen an Datenschutz bei der Übertragung, Speicherung und Bereitstellung gerecht zu werden, beachten wir folgende Grundregeln:

- Unsere Server sind nur berechtigten Personen zugänglich
- Daten dürfen Dritten nicht zugänglich gemacht werden
- Daten dürfen nur von berechtigten Nutzern geändert werden können

1.2. Verschlüsselung

Alle unsere Webseiten können ausschließlich über **verschlüsselte Verbindungen** („https“) aufgerufen werden. Als SSL Protokolle bieten wir dazu TLSv1, TLSv1.1 und TLSv1.2 an. SSLv3 wird aus Sicherheitsgründen nicht mehr unterstützt.
Wir unterstützen ausschließlich als **sicher geltende SSL-Cipher** für die HTTPS-Verbindung und bevorzugen sicherere Cipher gegenüber unsicheren. Bekannt unsichere Cipher werden von unserem Webserver abgelehnt. Standardmäßig verwenden wir eine AES-Verschlüsselung, je nach verwendetem Browser handelt sich dieser die verwendete Cypher mit dem Server individuell aus.

2. System

Das System richtet sich nach aktuellen Sicherheitsgrundregeln und besteht im Wesentlichen aus den Basisfunktionalitäten Security, User Management und den Applikationen. **Vier getrennte Systemumgebungen (Softwareversionen)** stellen sicher, dass der produktive Betrieb unabhängig von den Schulungen, den Tests und der Weiterentwicklung der Software laufen kann.

Die **Applikationen** sind zu Modulen zusammengefasst. Sie gliedern sich wie folgt:

- eScreening, eSourcing, eProcurement und eReaction für **private Auftraggeber**
- Pre-Award und Post-Award für **öffentliche Auftraggeber** nach Bundesvergabegesetz.

Bei der **Betriebssoftware** setzen wir bei unseren Systemen auf offene Standards und setzen wegen der höheren erwartbaren Sicherheit und der Offenheit des Quellcodes auf Open Source.

3. Verfügbarkeit

Die Verfügbarkeit der Dienste wird zu **99,8%** auf Monatsbasis werktags in der Zeit von 8:00 bis 18:00 (CET) gewährleistet. Sie bezieht sich auf die Nutzbarkeit unseres Übergangspunktes zu den Backbone- Leitungen des Internets.

4. Betriebskonzept für Hardware

Das **Serverhousing** erfolgt in zwei getrennten, unabhängigen Rechenzentren in Wien, die voneinander 7 km entfernt und mit den neuesten Sicherheitseinrichtungen ausgestattet sind. Die Datenübertragung zwischen beiden Systemen erfolgt verschlüsselt über IPSec und SSH mit Sicherheitsmonitoring. Dokumente die auf das System hochgeladen werden, werden einem Virusscan unterzogen.
Die **Datenverarbeitung** wird von **vemap** selbst durchgeführt (kein Subunternehmer).

4.1. Hauptsystem und On Site Backup System

4.1.1.Housing

Das Serverhousing für das **Hauptsystem** und das **On Site Backup System** erfolgt in einem Hochsicherheits- Rechenzentrum bei einem Carrier-neutralen Rechenzentrumsbetreiber in Wien mit **einer Redundante Highspeed-Internetanbindung an Backbone** (direkter Zugang zum VIX – Vienna Internet Exchange - und 96 Carriern/ISPs).

4.1.2. Hardware Hauptsystem

Hauptsystem als redundante Serverfarm mit folgender Konfiguration:

- Redundante Firewall
- getrennte Internetanbindung
- 3-fach redundanter Cluster für Application Server, Database Server Application Services, Fileserver
- Überwachung der Hosts und Services durch Nagios/Check_mk

4.1.3.Hardware On-Site Backup System

On-Site Backup System für **Long Term Storage**
auf NAS (Network Attached Unified Data Storage / iSCSI) auch als Disaster Recovery ausgelegt.
Speicherintervalle:

- 1x täglich inkrementelles Backup der Dateien (Dokumente, Beilagen)
- 1x täglich Full-Backup der Datenbanken
- Unbegrenzte Speicherzeit (gem. BVergG idgF = 48 Monate)
- Überwachungssystem: E-Mail- & SMS Reporting

4.1.4.Physikalischer Schutz der Infrastruktur

- **Strom:**
  - Die Speisung erfolgt durch zwei unterschiedliche Stromnetze
  - Redundantes Generator-Backup (2N)
  - USV gestütztes A Feed
  - "Clean-Earth" und Überspannungsschutz

- **Sicherheit:**
  - Kontaktlose Schlüsselkarten & biometrisches Zugangssystem & Personenvereinzelungs-anlage
  - 24x7 Sicherheitspersonal vor Ort
  - CCTV-Kameraüberwachung
  - Einbruchmeldeanlage
  - 24x7-Überwachung der gesamten Infrastruktur (Chiller, CRAC, Generatoren, UPS etc.)

- **Brandschutz:**
  - Inergenbasierendes Brandlöschsystem
  - Lasergesteuertes Brandfrüherkennungssystem (VESDA)

- **Brandschutzwände (F90)**
- **Klimatisierung:**
  - Luftfeuchtigkeit zwischen 40% und 60%
  - Redundantes System (N+1)
  - Klimatisierung gemäß ETS 300019 Klasse 3.1

4.2. Off-Site-Backup System

für **Disaster Recovery** und **Business Continuity** schützt gegen den **Totalverlust** des Haupt- und On Site Backup Systems und ist ebenfalls als Long Term Storage ausgelegt.
Es ist 7 km Luftlinie vom Hauptsystem entfernt und ausgestattet mit:

- Serverschrank-Monitoring durch AKCP:
  - Zutrittskontrolle & Kameraüberwachung
  - Wassermeldeanlage
  - Temperatur- und Brandmeldeanlage
- unterbrechungsfreie Stromversorgung
- Überspannungsschutz
- Klimatisierung mit automatischer Temperaturregelung und Warnmeldeanlage.

Backupsystem als Serverfarm mit folgender Konfiguration:

- 2-fach redundanter Cluster für Application Server, Database Server Application Services, Fileserver
- Firewall
- Redundanz durch laufende asynchrone Übertragung von Datenbanken und Daten über IPSec
- Überwachung der Hosts und Services durch Nagios/Check_mk

Business Continuity bei Totalverlust des Haupt- und On Site Backup Systems spätestens nach 2 Tagen.
Speicherintervalle:

- 1x täglich inkrementelles Backup der Dateien (Dokumente, Beilagen)
- 1x täglich Full-Backup der Datenbanken
- 1x täglich Snapshots der virtuellen Server (Applikation, Datenbank usw.)
- Unbegrenzte Speicherzeit für monatliche Full-Backups
- 1 Jahr Speicherzeit für wöchentliche Full-Backups

4.3. Monitoring

Das **Sicherheitsmonitoring** erfolgt rund um die Uhr sowohl On-Site, als auch Off-Site durch drei getrennte Sicherheitsmonitoring- Systeme (2x Nagios/Check_mk, 1x AKCP), die sich auch gegenseitig kontrollieren und hinsichtlich Leistung und Erreichbarkeit überwachen.
Bei Unregelmäßigkeiten werden nach einem festgelegten Alarmplan die verantwortlichen Personen durch E-Mail und SMS informiert.

5. Applikationen

Die Applikationen werden über eine eigen URL (eigenes Beschaffungsportal unter http://firmenname.vemap.com) erreicht. Die Lösung umfasst einen frei zugänglichen (ohne Login und Passwort) Bereich und einen nur für berechtigte Nutzer zugänglichen (Login und Passwort erforderlich) Privatbereich.

Im **frei zugänglichen Bereich** sind allgemeine Informationen, u. a. über vemap, über technische Voraussetzungen und über die Applikationen enthalten.
Die Zugangskontrolle für den **Privatbereich** erfolgt über eine Nutzerkennung (Login) und ein Passwort. Hinweise zur Passwort- Policy findet man direkt am Portal. Die Passwörter der Nutzer können vom Nutzer beliebig oft geändert bzw. müssen beim Erstlogin geändert werden. Hat ein Nutzer sein Passwort vergessen, kann selbständig ein neues Passwort angefordert oder durch den Administrator neues Passwort generiert werden. und automatisches abmelden nach Zeitüberschreitung.

Die Anbieter benötigen für die Abgabe von Angeboten und für die Teilnahme an Auktionen Transaktionsnummern, die die Rechtmäßigkeit der Angebote bestätigen. Diese **Transaktionsnummern** werden von der Software automatisch generiert und den Anbietern per E-Mai mit dem Login und Passwort gesendet.
Für die Abgabe nach dem **Bundesvergabegesetz** benötigen die Nutzer auch noch eine **Signaturmöglichkeit** (Karte oder Handy), die Signatursoftware von vemap und gegebenenfalls ein Kartenlesegerät. Entsprechende Hinweise und Bezugsmöglichkeiten werden direkt am Portal angeführt.

Je nach Berechtigungskonzept ist jeder Kunde für die Vergabe und Verwaltung von Zugangskennungen

seiner Nutzer wie Administratoren, Verwalter, Einkäufer, Beobachter, Anbieter, Besteller, und Lieferanten, selbst verantwortlich. Der individuelle Nutzer ist der Teilnehmer, der die eigentlichen Geschäfte als Käufer oder Verkäufer abwickelt. Die Abwicklung der Geschäfte erfolgt in einem in sich abgeschlossenen Bereich.

Es haben nur jene Nutzer Zugang, die vom Kunden dafür frei geschaltet / eingeladen werden bzw. sich über eine Bekanntmachung beworben haben..

Alle Daten und Dokumente, die auf die Server von vemap transferiert werden, werden in elektronischer Form über die gesamte Dauer der Zusammenarbeit aufbewahrt und in das Backup- System aufgenommen, sofern mit einzelnen Kunden nichts anderes vereinbart ist und sofern sie von den Nutzern nicht schon früher gelöscht werden.

6. Supporthotline

Die Hotline kann über eine zentrale Telefonnummer und über eine zentrale E-Mailadresse (Kontaktdaten Siehe jeweiliges Beschaffungsportal) kontaktiert werden. Die Hotline beantwortet in vier Sprachen inhaltliche und technische Fragen und sorgt bei speziellen Fragen für eine Beantwortung. Die Hotline verständigt die Kunden per E-Mail über eine geplante Nichtverfügbarkeit des Systems und über bekannte aktuelle Serverprobleme, die absehbar länger als 3 Stunden dauern werden.

Erreichbarkeit der Hotline:
Montag bis Donnerstag (werktags) von 08:00 Uhr bis 18:00 Uhr (CET).
Freitag (werktags) von 08:00 Uhr bis 14:30 Uhr (CET)

Wien, im Mai 2019