Piano della sicurezza e operativo (PSO)

Edizione gennaio 2016

1. Sicurezza

1.1. Conservazione/gestione dei dati

Sui server di **vemap (conservazione/gestione dei file esclusivamente in Austria)** vengono scambiati dati importanti tra diverse aziende (committenti pubblici e privati) . Per soddisfare i requisiti in termini di protezione dei dati nel trasferimento, il salvataggio e la distribuzione dei dati, rispettiamo le seguenti regole di base:

- I nostri server sono disponibili all'utilizzo da parte degli utenti autorizzati, entro i limiti tecnici.
- I dati sensibili non devono essere resi accessibili a soggetti terzi.
- I dati possono essere modificati solo dagli utenti autorizzati

1.2. Crittografia

Tutte le nostre pagine web possono essere visualizzate esclusivamente utilizzando **connessioni criptate** ("https"). Come protocolli SSL offriamo TLSv1, TLSv1. 1 e TLSv1. 2. Lo standard SSLv3 non viene più utilizzato per motivi di sicurezza.
Per la connessione HTTPS è supportata solamente **la crittografia SSL** e si preferiscono cifrature considerate sicure rispetto a quelle che offrono un grado inferiore di sicurezza. Le tipologie di crittografia notoriamente poco sicure vengono rifiutate automaticamente dal nostro web server. Per impostazione predefinita usiamo la crittografia AES, che in base al browser utilizzato negozierà la chiave individuale con il server.

2. Sistema

Il sistema si basa sugli attuali principi fondamentali di sicurezza e sostanzialmente comprende le funzionalità base di sicurezza, di gestione degli utenti e le applicazioni. **Quattro ambienti di sistema separati (versioni software)** assicurano che l'operatività possa svolgersi a prescindere dalle attività formative, dai test e dall'ulteriore sviluppo del software.

Le **applicazioni** sono raggruppate in moduli. E sono così strutturate:

- eScreening, eSourcing, eProcurement e eReaction per **clienti privati**
- Pre-Award e Post-Award per **committenti pubblici** ai sensi della Legge federale sugli appalti (Bundesvergabegesetz).

Per quanto riguarda il **software operativo**, per i nostri sistemi utilizziamo standard aperti ossia applicazioni open source poiché i loro standard di sicurezza sono solitamente più elevati e poiché i codici sorgente sono pubblici.

3. Disponibilità

La disponibilità dei servizi, nei giorni feriali, tra le 08:00 e le 18:00, è garantita al **99,8%** (CET), nell'arco di un mese. Questo dato descrive l'utilizzabilità della nostra connessione alla rete dorsale di Internet.

4. Schema operativo per l'hardware

Il servizio di **Serverhousing** è fornito attraverso due centri indipendenti di elaborazione dati a Vienna, distanti 7 km l'uno dall'altro e dotati delle più moderne attrezzature server. La trasmissione dei dati tra i due sistemi è criptato secondo gli standard IPSec e SSH con monitoraggio della sicurezza.
La **gestione dei dati** viene eseguita da **vemap** stessa (nessun subaffidatario).

4.1. Sistema principale e sistema di backup in loco

4.1.1.Housing

Il server che ospita il **sistema principale** e **il sistema di backup in loco** è situato in un centro di elaborazione dati ad alta sicurezza presso un provider indipendente a Vienna, con una **connessione alla dorsale internet ad alta velocità e ridondante,** (accesso diretto a VIX - Vienna Internet Exchange - e 96 provider/ISPs).

4.1.2. Hardware sistema principale

Sistema principale presso server farm ridondante con la seguente configurazione:

- Firewall ridondante
- 1 active router e 1 backup router
- Connessione a internet separata
- Cluster a tripla ridondanza per application server, database server e application services fileserver
- Cluster a doppia ridondanza per webserver, database server webservices, server ftp
- Monitoraggio dei host e dei servizi mediante Nagios/Check_mk

4.1.3.Hardware in loco sistema di backup

Sistema di backup in loco Sistema per **il salvataggio a lungo termine** su NAS (Network Attached Unified Data Storage / iSCSI) impostato anche per le Disaster Recovery di emergenza.

Intervalli di salvataggio:

- 1 backup incrementale giornaliero dei file (documenti, allegati)
- 1 backup giornaliero dell'intero database
- Periodo di conservazione illimitato (ai sensi della Legge austriaca sugli appalti (BVergG 2006) = 48 mesi)
- Sistemi di monitoraggio: Reporting via email & SMS

4.1.4.Protezione fisica dell'infrastruttura

- **Alimentazione elettrica:**
  - L'alimentazione è fornita da due diverse reti elettriche
  - Generatore di backup ridondante (2N)
  - A Feed basato su USV
  - "Clean-Earth" e relè di massima tensione

- **Sicurezza:**
  - Chiavi elettroniche contactless & sistema di accesso biometrico & sistema per il controllo del passaggio di una persona alla volta
  - Personale di sicurezza 24h/24
  - Sorveglianza a circuito chiuso
  - Impianto di allarme antintrusione
  - Sorveglianza 24h di tutta l'infrastruttura (Chiller, CRAC, generatori, UPS, ecc.)

- **Protezione antincendio:**
  - Impianto antincendio a inergen
  - Sistema di rilevamento incendi con controllo laser (VESDA)

- **Pareti tagliafuoco (F90)**
- **Climatizzazione:**
  - Umidità dell'aria 40% e 20%
  - Sistema ridondante (N+1)
  - Aria condizionata secondo ETS 300019 classe 3.1

4.2. Sistema di backup remoto

per garantire la **disaster recovery** e il **mantenimento dell'operatività (business continuity)** ed evitare quindi la **perdita totale dei dati** del sistema principale e del sistema di backup in loco; il sistema inoltre prevede la possibilità di salvare di dati a lungo termine (long term storage).
Si trova a 7 km, in linea d'aria, dal sistema principale ed è dotato di:

- monitoraggio rack server AKCP:
  - Controllo degli accessi & videosorveglianza
  - Sistema rilevamento entrate d'acqua
  - Impianto di rilevamento della temperatura e di incendi
- Gruppo di continuità
- Relè di massima tensione
- Aria condizionata con controllo automatico della temperatura e sistema di allarme.

Sistema di backup presso server farm con la seguente configurazione:

- firewall, application server, database server application services, fileserver, webserver, database server webservices, server ftp
- Ridondanza attraverso il trasferimento asincrono continuo di banche dati e dati tramite IPSec
- Monitoraggio dei host e dei servizi mediante Nagios/Check_mk

Business continuity in caso di perdita totale del sistema principale e di backup in loco al più tardi dopo 2 giorni.
Intervalli di salvataggio:

- 1 backup incrementale giornaliero dei file (documenti, allegati)
- 1 backup giornaliero dell'intero database
- periodo di conservazione illimitato per i backup completi mensili
- periodo di conservazione di 1 anno per i backup completi settimanali

4.3. Monitoraggio

Il **monitoraggio della sicurezza** è costante 24 ore al giorno, sia **in loco** che **in remoto** da tre sistemi separati di monitoraggio della sicurezza - (2 Nagios/Check_mk, 1 AKCP), che si controllano anche reciprocamente e monitorano più di 30 hosts e più di 200 servizi in termini di prestazioni e accessibilità.
In caso di irregolarità vengono inviati SMS e email alle persone responsabili secondo il piano di emergenza stabilito.

5. Applicazioni

Le applicazioni sono accessibili tramite un apposito URL (apposito portale appalti). La soluzione comprende una zona liberamente accessibile e una zona riservata solo agli utenti autorizzati.
Nella zona **liberamente accessibile** sono disponibili le informazioni di carattere generale, tra cui informazioni su vemap, sui requisiti tecnici e sulle applicazioni.
Il controllo di accesso per l'**area riservata** avviene tramite un ID univoco di utente (login) e la password secondo la password policy e con disconnessione automatica dopo il timeout. Le password utente possono essere cambiate un numero illimitato di volte. Se un utente dimentica la propria password, può essere generata una nuova password in modo autonomo oppure con l'intervento dell'amministratore di sistema.

Per la presentazione delle offerte e per la partecipazione alle aste i fornitori hanno bisogno di un numero di transazione a conferma della legittimità dell'offerta. Questi **numeri di transazione** sono generati dall'amministratore del cliente e trasmesso ai fornitori via email. Per le offerte ai sensi della **Legge austriaca sugli appalti BVergG** gli utenti necessitano di un **sistema di firma elettronica** (Card o telefono cellulare) ed eventualmente di un lettore di schede.

A seconda dello schema dei diritti di accesso, ogni cliente è responsabile dell'assegnazione e della gestione dei codici di accesso dei suoi utenti quali amministratori, manager, acquirenti, osservatori, offerenti, clienti, fornitori. Il singolo utente è un partecipante che svolge le effettive transazioni in veste di acquirente o venditore. Lo svolgimento delle operazioni avviene in un'area riservata

a cui hanno accesso solo gli utenti abilitati/invitati dal cliente.
Tutti i dati e documenti che vengono trasferiti al server di vemap sono conservati in forma elettronica per tutta la durata della collaborazione e conservati nel sistema di backup, salvo diversi accordi con un singolo cliente e salva l'eliminazione da parte dell'utente stesso.

6. Servizio di assistenza

Il servizio di assistenza può essere contattato sia via telefono che via email (per i contatti vedasi il proprio portale appalti di riferimento). Il servizio di assistenza risponde alle domande tecniche e contenutistiche in quattro lingue da parte di personale specializzato. Il servizio di assistenza comunica via email ai clienti l'eventuale indisponibilità pianificata del sistema e di problemi del server riscontrati di durata superiore alle 3 ore.

Orari del servizio di assistenza:
Dal lunedì al giovedì (giorni feriali) dalle 8:00 alle 18:00 (CET).
Venerdì (giorni feriali) dalle 8:00 alle 14:30 (CET).

Vienna, gennaio 2016