Whistleblowing Digitale GlobaLeaks

Sintesi delle modalità di fornitura SaaS

Documento aggiornato il 19 Maggio 2022

Il presente documento propone una sintesi delle principali caratteristiche del modello di fornitura in modalità SaaS del Servizio di Whistleblowing Digitale GlobaLeaks offerto nel progetto WhistleblowingPA dai partner di progetto Whistleblowing Solutions Impresa Sociale e Transparency International Italia.

Metodologia

La fornitura adotta la metodologia e le raccomandazioni ufficiali del progetto GlobaLeaks mantenuto e coordinato da Whistleblowing Solutions partner di progetto e fornitore SaaS del servizio erogato secondo modello di erogazione certificato ISO27001, ISO27017, ISO27018 e qualificato AGID.

Per le qualità specifiche dell'applicativo di whistleblowing si rimanda alla documentazione ufficiale di progetto e principalmente alle risorse:

- Modello di rischio: https://docs.globaleaks.org/en/main/security/ThreatModel.html
- Misure di sicurezza: https://docs.globaleaks.org/en/main/security/ApplicationSecurity.html
- Modello crittografico: https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html

- Lista dei report di audit internazionali indipendenti: https://docs.globaleaks.org/en/main/security/PenetrationTests.html

Architettura di sistema

L'architettura di sistema è principalmente composta da:

- Un network firewall perimetrale;
- Un cluster di due server fisici dedicati;
- Una Storage Area Network (SAN) in fiber channel ridondata.

I sistemi sono posizionati a Milano (Caldera) all'interno del datacenter di Seeweb S.r.l. (https://www.seeweb.it) fornitore IaaS impiegato nell'erogazione, italiano, qualificato AGID e ufficialmente nominato come sub-responsabile del trattamento ai sensi del GDPR.

Completa l'architettura di sistema un servizio di backup gestito dallo stesso fornitore Seeweb con tecnologia Veeam su area geografica secondaria (Frosinone) dove viene implementato backup giornaliero differenziale con copertura di 7 giorni per finalità di disaster recovery.

Non vengono usati altri fornitori o datacenter e non esiste alcun trasferimento fuori Italia.

Software impiegato

In aggiunta al software GlobaLeaks utilizzato per l'implementazione del servizio, per finalità di pubblicazione, documentazione e supporto del progetto vengono utilizzate altre tecnologie a codice aperto e di pubblico dominio la cui qualità è indipendentemente verificabile. Vengono anche in modo limitato utilizzate alcune note tecnologie proprietarie e licenziate necessarie per finalità di gestione infrastrutturale e backup professionale.

Vengono primariamente utilizzati le tecnologie open source:

- Debian/Linux: (principale sistema operativo utilizzato)
- Postfix (mail server)
- Bind9: (dns server con supporto dnsseq)
- Discourse (forum)
- Mattermost (chat di support utenti)
- NextCloud: (cloud privato)
- OPNSense (firewall)
- OpenVPN (vpn)

Le limitate componenti software di natura proprietaria impiegate sono:

- VMware: software di virtualizzazione
- Veeam: software di backup
- Plesk: software per realizzazione siti web di facciata del progetto

Predisposizione dei sistemi virtualizzati:

- I server eseguono software VMware e VCENTER abilitando funzionalità di High Availability (HA) e Dynamic Resource Scheduling (DRS);
- Su VMware vengono istanziate macchine virtuali Debian/Linux nelle sole versioni Long Term Support (LTS);
- Ogni macchina virtuale Debian implementa configurazione securizzata con: Full Disk Encryption (lvm/crypto), SecureBoot, Apparmor, Iptables;
- Entrambi i server fisici eseguono una macchina virtuale di Key Management System (KMS) per consentire continuità di servizio con immediato automatico riavvio dei sistemi senza intervento amministrativo anche in caso di totale fallimento di uno dei due server fisici componenti il cluster.

Architettura di rete:

- L'architettura di rete prevede un firewall perimetrale e segregazione della rete in molteplici VLAN al fine di isolare le differenti componenti secondo loro differente natura al fine di limitare ogni esposizione in caso di vulnerabilità su una singola componente;
- Una VPN consente l'accesso alla gestione dell'infrastruttura a un limitato e definito insieme di amministratori di sistema;
- Ogni connessione di rete implementa TLS 1.2+;
- Ogni macchina virtuale istanziata vede esposizione di rete limitata all'effettiva necessità.
- Tutti i dispositivi utilizzati quali applicativo GlobaLeaks, Log di sistema e Firewall sono configurati per non registrare alcun tipo di log di informazioni lesive della privacy e dell'anonimato del segnalante quali indirizzi IP e User Agents;
- L'applicativo GlobaLeaks vede abilitata la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.

Affidabilità del servizio

Per quanto i sistemi di whistleblowing rientrino tra i sistemi di tipo "non mission-critical" il design architetturale adottato garantisce alta affidabilità.

Il sistema è infatti ridondato pienamente tramite cluster di due server equivalenti e funzionalità VMware High Availability e Storage Area Network (SAN) in fiber channel completamente ridondata garantiti dal fornitore IaaS con SLA al 99,90%.

Per quanto non sia istanziata una completa infrastruttura di Disaster Recovery su area geografica secondaria, è definito internamente un piano di recupero che data la scelta di tecnologie comuni ad alta disponibilità e i backup giornalieri effettuati su area geografica secondaria garantisce assenza di perdita dei dati e tempi di ripristino stima su valori di RPO=24h e di RTO=48h.

Whistleblowing Solutions Impresa Sociale S.r.l.

Giovanni Pellerano