Profilo di sicurezza dell'infrastruttura

"eLogic Cloud Services"

1 Introduzione

eLogic offre servizi cloud di tipo *Infrastructure as a Service* (IaaS) e *Platform as a Service* (PaaS), che garantiscono ai clienti l'uso di risorse di elaborazione, piattaforme software e accesso Internet *come servizio* facilmente configurabile, flessibile e immediatamente adattabile in funzione delle necessità, che non richiede investimenti e ha costi operativi proporzionali alle risorse impegnate.

Questo documento fornisce una sintetica descrizione del profilo di sicurezza dei servizi cloud eLogic, dando evidenza delle misure tecniche e organizzative adottate, al fine di consentire ai nostri clienti una verifica trasparente e informata dell'adeguatezza dei nostri servizi alle loro esigenze di sicurezza.

Elogic è impegnata a rispettare le prescrizioni della normativa EU GDPR relativamente alle attività di elaborazione condotte in proprio e alla fornitura di infrastrutture che possono essere usate anche per il trattamento di dati personali. A garanzia di quest'impegno, eLogic ha aderito già nel 2017 al Codice di Condotta per Cloud Service Provider, elaborato dal CISPE[1] e sottoposto all'approvazione dell'autorità europea per la protezione dei dati personali (Art. 29 WP).

Il Codice di Condotta chiarisce le responsabilità reciproche di eLogic e del Cliente nel contesto della fornitura di servizi Cloud, adottando un modello di responsabilità condivisa, dove eLogic è responsabile della sicurezza dell'infrastruttura cloud (sicurezza del cloud) e i clienti sono responsabili della sicurezza dei loro dati e applicazioni sui server virtuali utilizzati (sicurezza nel cloud). Il testo del Codice di Condotta elaborato dal CISPE è disponibile sul sito eLogic e sul sito CISPE.

Tutti i data center e le infrastrutture usate da eLogic sono collocati sul territorio italiano, e i dati gestiti su questi data center non vengono mai trasferiti al di fuori del territorio italiano.

La prima sezione di questo documento descrive l'infrastruttura fisica su cui sono erogati i servizi eLogic Cloud Services e le misure tecniche adottate per la sicurezza dell'infrastruttura. La seconda sezione descrive le misure logiche e organizzative, e in generale il sistema di gestione della sicurezza.

[1] Il CISPE (Cloud Infrastructure Services Providers in Europe) è un'associazione che rappresenta i principali fornitori di infrastrutture e servizi Cloud operanti in Europa, e che dialoga con le autorità della UE nell'elaborazione delle politiche relative alla sicurezza e alla protezione dei dati personali (vedi https://cispe.cloud/ per ulteriori informazioni).

2 Infrastruttura eLogic Cloud

2.1 I Datacenter

L'infrastruttura Cloud eLogic risiede in due data center, gestiti da primari operatori specializzati, presso i quali sono collocati rack di apparti interamente e autonomamente gestiti da eLogic. Sono situati a Milano (Datacenter di BT Italia a Settimo Milanese, standard Tier 4) e a Bologna (Datacenter Retelit di Villanova di Castenaso, standard Tier 3). Entrambi i data center garantiscono elevati livelli di continuità, tramite la ridondanza delle fonti e della distribuzione di energia, dei sistemi di raffreddamento e delle connessioni di rete, e di sicurezza tramite il controllo degli accessi fisici e logici, e sistemi di gestione dei processi e della sicurezza certificati in conformità agli standard ISO 9001 e ISO 27001.

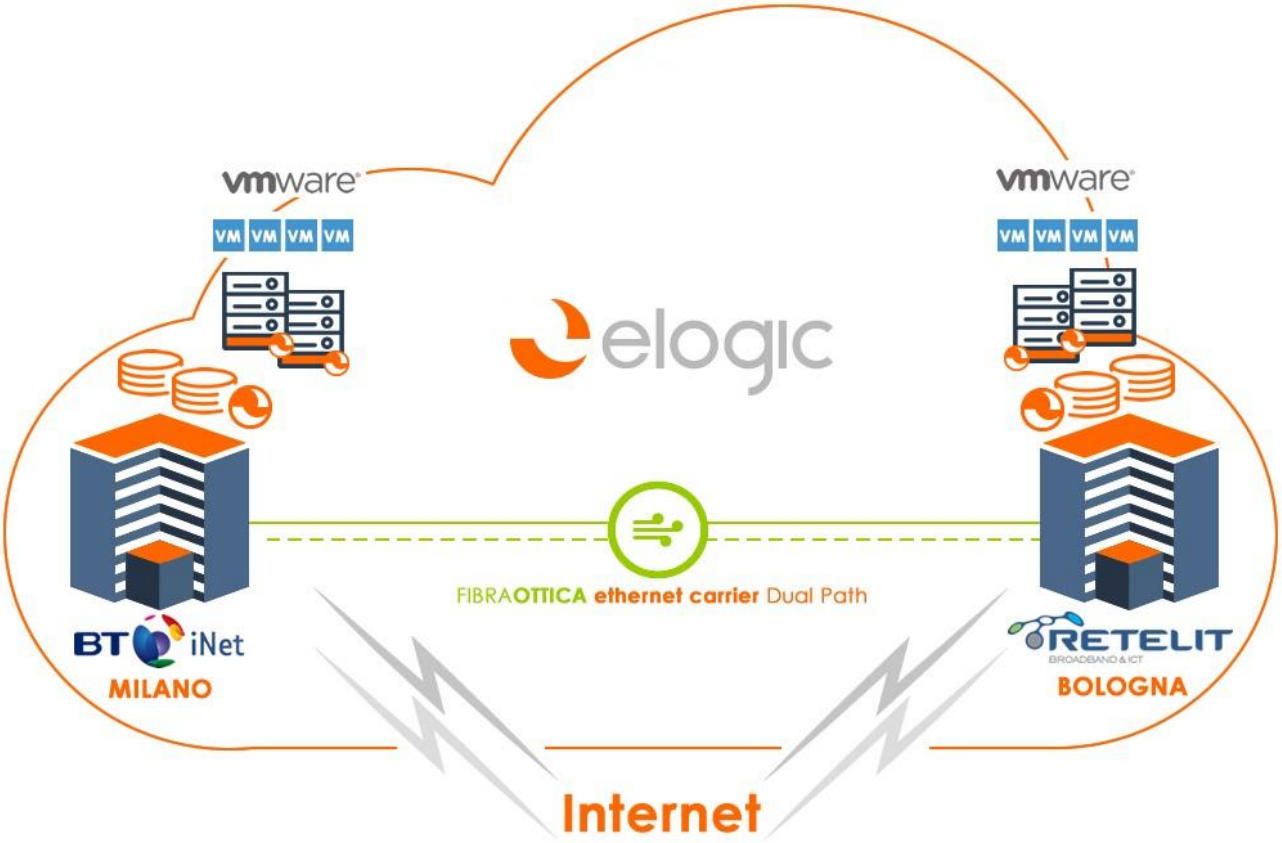

FIGURA 1 INFRASTRUTTURA CLOUD ELOGIC

Il sito di Milano/BT rappresenta il sito principale per l'erogazione dei nostri servizi, mentre il sito di Bologna è principalmente rivolto a servizi interni di replica dei dati e all'offerta di soluzioni di Disaster Recovery e replica geografica.

2.2 Le risorse di elaborazione

Così come i Data Center che la ospitano, anche l'infrastruttura gestita da eLogic è ridondata, a garanzia della continuità dei servizi. Le risorse di elaborazione sono erogate grazie alle potenzialità della piattaforma di virtualizzazione leader di mercato, VMware vSphere, sfruttando le funzionalità di "Software Defined Datacenter" orchestrate delle tecnologie VMware vCloud.

Le risorse virtuali sono fornite da cluster di elaborazione, che mettono in comune le capacità fornite da batterie di server fisici e sono quindi resilienti al guasto di uno o più server. Tutti i server sono ridondati sia nell'alimentazione che nei collegamenti alla rete Internet e alla SAN (la Storage Area

Network, costituita da diversi apparati di Storage, ciascuno ridondato nei controller, alimentazione e collegamenti Fibre Channel). Le infrastrutture di commutazione (Switch) della rete dati e della SAN sono anch'esse completamente ridondate, senza "single point of failure".

La piattaforma vSphere bilancia automaticamente l'allocazione delle macchine virtuali sulle batterie di server fisici tramite la tecnologia Distributed Resource Scheduling (DRS) e garantisce disponibilità tramite la funzione di High Availability (HA), che assicura il riavvio automatico di una macchina virtuale in caso di guasto del server fisico. La ridondanza delle infrastrutture e la virtualizzazione delle risorse consentono livelli di disponibilità elevati e SLA del 99,9 %.

2.3 Interconnessioni di rete e collegamento alla rete Internet

2.3.1 Infrastruttura di rete fisica e logica

Su ciascun data center, l'infrastruttura fisica di rete è composta da due dorsali Ethernet completamente ridondate, basate su Switch core ridondati e interconnessi che offrono connessioni a 10 e 40 Gbps e latenze sub-microsecondo.

Su questa infrastruttura fisica sono implementati, tramite tecniche di network overlay (VXLAN) o VLAN, i segmenti di rete assegnati ai server e ai data center virtuali dei clienti, in modo tale da garantire l'isolamento delle reti di un cliente rispetto alle reti di tutti gli altri clienti, o alle stesse reti di management di eLogic.

Tutto il traffico tra segmenti di rete diversi e verso la rete Internet passa tramite firewall perimetrali, che consentono esclusivamente le connessioni ammesse dalle politiche esplicitamente definite.

La gestione di tutti gli apparati che fanno parte dell'infrastruttura eLogic avviene tramite una rete di management separata e isolata dall'esterno, cui ha accesso controllato solo il personale eLogic.

2.3.2 Collegamento alla rete Internet

eLogic, in qualità di Autonomous System (AS 200760), dispone di proprie classi di indirizzi IPv4 e IPv6, e ne gestisce autonomamente la propagazione e il routing sulla global Internet tramite più fornitori di transito, garantendo ridondanza ed elevata raggiungibilità dei propri servizi e ottimizzando la qualità degli accessi da e verso Internet.

I data center elogic dispongono, ciascuno, di due router indipendenti, con connettività Gigabit. Ciascun router gestisce l'instradamento verso uno o più carrier Internet tramite protocollo BGP. La ridondanza di router e carrier, assieme all'interconnessione tra i due data center, consente di mantenere la raggiungibilità dei ns. sistemi anche in caso di fault su uno dei provider.

Al momento i carrier utilizzati sono BT e Retelit, ciascuno con una duplice connessione a 1Gbps.

2.3.3 Interconnessione tra i due data center

I due Data Center sono connessi tra loro da una linea dati dedicata Layer 2 con percorso diversificato in ridondanza, attualmente a 1Gbps (rapidamente scalabile a 10Gbps), che permette sia le funzioni di replica di dati e servizi, che il pieno controllo del routing Internet.

La disponibilità di un link L2 ad alta capacità offre un'elevata flessibilità nella configurazione di scenari di Disaster Recovery geografico.

2.3.4 Firewall perimetrali e firewall dedicati ai clienti

Su ciascun sito, il collegamento tra le reti interne e la rete Internet è filtrato da un firewall perimetrale, controllato esclusivamente da personale eLogic, sul quale sono definite le politiche di accesso alle reti, e che consentono il monitoraggio del traffico, mitigando attacchi e potenziali compromissioni.

A protezione della propria infrastruttura, i clienti possono richiedere firewall virtuali dedicati, sia gestiti autonomamente che affidati in gestione ad eLogic, e attivare ulteriori funzionalità di ispezione del traffico (come IPS, WAF etc.) in funzione delle proprie, specifiche esigenze di sicurezza.

2.4 Storage e sicurezza dei dati

L'infrastruttura fisica di storage, che fornisce dischi virtuali alle risorse cloud dei clienti, è basata su apparati SAN di altissima affidabilità, ciascuno ridondato nei controller, alimentazione e collegamenti Fibre Channel (su dorsali FC ridondate e indipendenti). Gli apparati SAN gestiscono pool di dischi di diverse capacità e prestazioni (SSD, SAS, NL) e consentono, tramite le funzioni di auto-tiering, l'erogazione di profili di storage diversificati.

Non sono, al momento, attive funzioni di replica dei dati tra apparati storage diversi e indipendenti. La sicurezza dei dati è quindi basata sull'intrinseca affidabilità degli apparati di storage (ridondanza dei controller, pool di dischi in RAID5 o RAID6, dischi spare) e ai sistemi di backup su apparati storage separati.

L'infrastruttura dispone di infatti di un sistema di backup a livello di hypervisor, che non interferisce con l'operatività dei server virtuali e non richiede l'installazione di agenti, e trasferisce il contenuto degli interi dischi delle VM (server virtuali) su una SAN separata e dedicata ai backup. La soluzione garantisce la possibilità di recuperare rapidamente non solo l'intera macchina virtuale, ma anche singoli file e applicazioni. La consistenza e integrità dei backup sono costantemente monitorate.

Il backup è un servizio opzionale.

Per i clienti che desiderino i livelli più elevati di affidabilità e disponibilità, è possibile attivare repliche di server o interi data center virtuali tra i due data center eLogic, mantenendo quindi una seconda copia "viva" dei sistemi, pronta a entrare in funzione in caso di necessità, garantendo bassi livelli di RPO e RTO. È possibile infine gestire una copia geografica ridondata dei backup.

È attualmente in fase di progettazione un potenziamento dell'infrastruttura di storage, che vedrà l'attivazione di sistemi di replica sincrona dei dati tra SAN indipendenti e geograficamente separate. La soluzione sarà progettata in modo da poter evolvere in un metro storage cluster, mettendo quindi a disposizione livelli di sicurezza e disponibilità elevati anche a fronte di eventi di fault a livello di data center.

Monitoraggio dell'infrastruttura

L'intera infrastruttura dei data center è costantemente monitorata tramite sistemi di controllo e allerta proattivi, consentendoci di intervenire immediatamente su qualsiasi problematica. Questi stessi sistemi possono essere messi a disposizione dei ns. clienti per il controllo personalizzato di server e applicazioni ospitate presso il Cloud eLogic.

Gli apparati più critici (SAN) sono monitorati anche dal fornitore, che garantisce un intervento proattivo 24x7 in caso di anomalie.

3 Gestione della sicurezza e protezione dei dati

Garantire la sicurezza della nostra infrastruttura Cloud, e l'integrità, la riservatezza e la disponibilità dei dati dei clienti è un nostro obiettivo fondamentale e un impegno di tutto lo staff eLogic, dal top management al personale operativo. A questo scopo eLogic adotta, oltre agli accorgimenti tecnici menzionati nelle precedenti sezioni, un sistema per la gestione della sicurezza delle informazioni che comprende la continua rivalutazione dei fattori di rischio esterni e interni e l'adozione di conseguenti idonee misure preventive e correttive, oltre che il costante aggiornamento e formazione del personale tecnico e operativo a tutti i livelli. Il sistema non è stato sottoposto a certificazione.

Qualora i nostri clienti svolgano, su nostra infrastruttura, attività di trattamento di dati personali, eLogic può garantire piena conformità agli adempimenti previsti dall'EU GDPR per i processori dei dati (ovvero responsabili del trattamento), e fornire consulenza sulla valutazione delle misure di sicurezza appropriate al tipo di dati e di trattamenti, e quindi agli specifici rischi.

3.1 Sistema di gestione della sicurezza

Il sistema di gestione della sicurezza dei sistemi informativi adottato da eLogic comprende i seguenti elementi:

Misure organizzative

- È definita e documentata una "politica della sicurezza" aziendale, che chiarisce a tutti i dipendenti e collaboratori le politiche di uso accettabile delle risorse, le responsabilità per la loro gestione, le regole di sicurezza, custodia e modifica delle password, le politiche di BYOD e di uso di dispositivi aziendali mobili, le regole di accesso ai sistemi informativi.
- Ruoli e responsabilità per la gestione dei sistemi informativi e delle risorse cloud sono chiaramente definiti e assegnati, in conformità alle politiche di sicurezza. È assegnato il ruolo di responsabile per la sicurezza dei sistemi informativi e servizi cloud.
- Politica di controllo degli accessi: i diritti di accesso alle risorse IT sono assegnati in maniera differenziata a ciascun ruolo, secondo il principio della necessità di sapere e operare e del minimo livello di autorizzazione. Tutti gli accessi di livello privilegiato vengono tracciati.
- In caso di riorganizzazioni del personale, le procedure di revoca dei diritti e delle responsabilità e di trasferimento ad altri sono chiaramente definite.

Personale

- Riservatezza: tutti i dipendenti comprendano le proprie responsabilità e gli obblighi relativi alla gestione dei sistemi informativi e al trattamento dei dati. I ruoli e le responsabilità sono chiaramente comunicati durante il processo di inserimento.
- Formazione: tutti i dipendenti siano adeguatamente informati sui rischi informatici e le misure di sicurezza da adottare relativi al lavoro quotidiano. I dipendenti coinvolti nella gestione dei servizi cloud devono avere adeguati requisiti di esperienza, competenza e professionalità, e sono costantemente aggiornati sulle tecnologie e le misure di sicurezza.

Gestione delle risorse e delle modifiche

- Gestione delle risorse: è gestito un registro di tutte le risorse IT (hardware, software e rete) impiegate nelle attività interne e nella gestione dei servizi cloud, con indicazione delle versioni di software applicativo e di sistema. Le connessioni alle reti aziendali sono controllate.
- Gestione delle modifiche: tutte le modifiche ai sistemi IT sono registrate e monitorate; le modifiche ai sistemi critici sono preventivamente validate.

Valutazione dei rischi

- Sono periodicamente valutati, sulla base delle esperienze aziendali, degli incidenti verificatisi, dell'evoluzione delle tecnologie e dei profili di attacco, e dell'evoluzione delle infrastrutture e dei servizi forniti, i rischi alla sicurezza, integrità e disponibilità dei sistemi informativi e dei servizi cloud. Nuove misure tecniche e organizzative di sicurezza possono essere attivate a seguito di questa valutazione. Queste attività sono documentate.
- Tutti gli incidenti relativi a sicurezza, integrità e disponibilità dei dati vengono documentati e devono dare luogo ad un'analisi delle cause e alla rivalutazione delle misure di sicurezza adottate.

Risposta agli incidenti e continuità operativa

- È definito un piano di risposta agli incidenti, con procedure e responsabilità dettagliate per garantire una risposta rapida e efficace, in particolare nel caso di perdita, uso improprio o acquisizione non autorizzata di dati personali.
- Continuità operativa: Sono definite le procedure e controlli da seguire al fine di garantire il livello richiesto di continuità e disponibilità dei sistemi e dei servizi cloud. In particolare sono definiti scenari e piani di recovery da guasti e incidenti maggiori, e controlli sulla disponibilità e integrità delle risorse necessarie.

Misure tecniche di sicurezza

- Tutti i sistemi interni sono periodicamente aggiornati con le patch di sicurezza rilasciate dai vendor. La sostituzione dei sistemi in end of life va pianificata e attuata prima che termini il supporto di manutenzione e aggiornamento del vendor.
- Tutti i server applicativi interni sono protetti da sistemi anti malware, costantemente aggiornati e monitorati. Gli accessi sono consentiti solo agli utenti autorizzati dalle politiche di accesso.
- Tutti gli accessi dall'esterno a risorse aziendali (inclusi siti web che gestiscono risorse) devono avvenire su canali di comunicazione cifrati. Dati sensibili non possono essere mai trasmessi in chiaro.
- Le reti dati interne sono controllate e consentono accesso solo a dispositivi fissi e mobili registrati e autorizzati.
- È definita, applicata e monitorata una politica di backup di tutti i sistemi server. I supporti di backup vengono periodicamente controllati.
- Alla dismissione di sistemi, i dischi contenenti dati sensibili vengono sottoposti a procedure di cancellazione.
- Il traffico da e verso i sistemi IT viene monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni. I segmenti di rete assegnati alle risorse cloud di clienti diversi sono separati e non comunicanti, se non tramite firewall e politiche di accesso.

4 Responsabilità dei clienti nella gestione delle proprie risorse

Come già accennato, e dettagliato nel Codice di Condotta elaborato dal CISPE cui eLogic aderisce, mentre eLogic è responsabile della sicurezza dell'infrastruttura cloud, i clienti sono responsabili della sicurezza dei loro dati e applicazioni sui server virtuali utilizzati (sicurezza nel cloud).

Contestualmente alla consegna delle risorse virtuali richieste (server o data center virtuali), eLogic consegna al cliente le credenziali di accesso amministrativo alle proprie risorse, che il cliente dovrà cambiare al primo accesso e custodire a propria cura. eLogic provvede inoltre alla configurazione iniziale del proprio firewall perimetrale, aprendo le porte richieste dal cliente (o eventualmente alla configurazione di un firewall dedicato al cliente, se richiesto), e alla configurazione iniziale delle politiche di backup dei server, se tale servizio viene acquistato.

È responsabilità del cliente la gestione della sicurezza della propria infrastruttura, incluse la custodia e la sicurezza delle password, l'aggiornamento delle patch di sistema e degli applicativi installati, la sicurezza delle applicazioni installate, la configurazione delle politiche di accesso sui firewall dedicati e gestiti autonomamente, il monitoraggio della funzionalità dei sistemi e di eventuali intrusioni.

4.1 Accesso amministrativo del personale eLogic a server di clienti

Qualora il cliente sottoscriva con eLogic contratti di assistenza sistemistica (servizi eLogic System Support e eLogic Extended Support), contestualmente assegna ad eLogic il diritto di accesso, con ruolo di amministratore di sistema, ai server oggetto di questi servizi.

eLogic accederà ai sistemi del Cliente, con i privilegi di amministratore, esclusivamente per svolgere le attività indispensabili a garantire i servizi oggetto di tali contratti, e in essi dettagliati.

eLogic consentirà l'accesso ai sistemi del Cliente solo a proprio personale diretto in carica, dotato di appropriata qualifica professionale ed esperienza, e vincolato da impegni contrattuali di integrità e riservatezza. Tali accessi saranno tracciati dai sistemi di logging di eLogic.

Su specifica richiesta del Cliente, eLogic fornirà i nominativi del personale che è autorizzato ad accedere ai sistemi Cliente con il ruolo di amministratore, ed i log di accesso (per server e intervallo temporale, limitato agli ultimi 365 giorni).

Il Cliente darà ad eLogic, per ciascun server oggetto dei servizi di supporto sistemistico, un singolo account (username e password) dotato dei privilegi amministrativi. L'account dovrà essere revocato dal cliente al termine del contratto.

L'elenco dei server oggetto di servizi di supporto sistemistico va allegato al contratto.

Salvo quanto dettagliato in separati e specifici contratti di servizio, l'accesso amministrativo ai sistemi del Cliente non comporta, da parte di eLogic, l'assunzione di incarichi relativi al trattamento di dati personali, qualora tali trattamenti siano svolti dal Cliente usando i sistemi forniti da eLogic.