Polo Strategico Nazionale

Shared Security Responsibilities – Schede di Servizio

Servizi BaaS

1 – Descrizione Servizi

2 – Metodologia

3 – Aree di responsabilità

4 - Riepilogo

Shared Security Responsibility Model

Backup as a Service

Attraverso il servizio di **Backup as a Service** è possibile per il cliente **estendere le capacità di backup del proprio servizio Cloud PSN** (oltre le capacity fornite dal backup default) permettendo quindi l'esecuzione di jobs di backup e restore dei svariati contesti (filesystem, virtual machine, database and application, posta elettronica, ecc) del cliente in modo efficace e sicuro.

Oltre al servizio backup standard di cui sopra, PSN mette a disposizione un servizio opzionale aggiuntivo attivabile separatamente di **Golden Copy**: si tratta di una funzionalità completamente gestita ed opzionale, attivabile su richiesta, in aggiunta al servizio di Backup standard: essa effettua la verifica e convalida dell'integrità dei dati durante le attività di backup e di esecuzione della golden copy.

Le principali caratteristiche del servizio sono: ✓ analisi automatizzata del backup per certificarne l'assenza di vulnerabilità (incluse attività sospette di ransomware); ✓ certificazione della Golden Copy da parte della NewCo PSN; ✓ protezione su storage distinto di backup, privo di ogni accesso fisico e logico; ✓ replica in Region diverse e su canale cifrato.

1 – Descrizione Servizi

2 – Metodologia

3 – Aree di responsabilità

4 - Riepilogo

Shared Security Responsibility Model

Lo scopo del presente documento è quello di identificare, per i servizi **Backup as a Service gli ambiti di responsabilità rispetto alla messa in sicurezza del servizio Cloud**.

Con un approccio basato su **trasparenza e condivisione**, vengono elencate le aree in cui la sicurezza è garantita dal PSN, nonché poste all'attenzione le **aree in cui la sicurezza è di responsabilità della Pubblica Amministrazione Cliente**, con l'obiettivo di garantire, **attraverso un approccio basato su sinergia e collaborazione**, la sicurezza dell'intero servizio in tutto il suo ciclo di vita e a beneficio di tutte le parti coinvolte.

LA SICUREZZA DEL TUO SERVIZIO CLOUD E' UNA RESPONSABILITÀ CONDIVISA

Polo Strategico Nazionale

Lo Shared Security Responsibility Model

Lo **Shared Security Responsibility Model (SSRM)** è lo strumento previsto all'interno della Cloud Control Matrix – dominio **«Supply Chain Management, Transparency and Accountability»**, attraverso il quale **Cloud Service Provider e Cloud Service Customer** definiscono e regolano in che modo la responsabilità e l'accountability per la sicurezza dei dati e delle risorse venga suddivisa nell'ambito di uno specifico **servizio Cloud**.

Per ogni controllo indicato all'interno della Cloud Control Matrix (e dunque per ogni ambito di sicurezza) viene **identificata l'ownership** specificando se questa spetta al *Cloud Service Provider*, al *Cloud Service Customer* o ad una *Terza Parte*.

CSC = P.A.

Il Customer che ha sottoscritto un contratto per usufruire del servizio

CSP = PSN

Il provider che ha contrattualizzato l'erogazione del servizio

Third Party = Gestori e Fornitori

Fornitore al quale il Provider o il Customer si rivolge per l'erogazione di una specifica componente del servizio.

Il provider è responsabile della sicurezza «del» Cloud,

il cliente è responsabile della sicurezza «nel» Cloud.

Polo Strategico Nazionale

Definizione delle responsabilità

Al seguito di poter **identificare i punti di confine delle responsabilità**, i domini elencati vengono inoltre inquadrati sulla base dei **layer di servizio** di seguito riportati.

DATA	I dati effettivamente gestiti e processati dalle applicazioni eseguite negli ambienti Cloud.
APPLICATION	Applicazioni/processi/funzioni sviluppate e gestite da parte del cliente.
RUNTIMES	Moduli eseguibili messi a disposizione dal provider che possono consentire lo sviluppo di applicazioni/processi/funzioni da parte del cliente.
MIDDLEWARE	Software di intermediazione che facilitano lo sviluppo, l'esecuzione e la comunicazione fra applicazioni.
OS (Operating System)	Software di base che dialoga con le risorse hardware virtualizzate dall'hypervisor il cui scopo è quello di ospitare e gestire il software dei livelli superiori (per estensione si intendono anche le Virtual Machine e le Virtual Appliances).
HYPERVISOR	Strumento di virtualizzazione delle risorse hardware e network, attraverso il quale sviluppare l'intera dimensione logica del servizio.
HARDWARE	Risorse fisiche messe a disposizione (CPU, RAM, Spazio su disco …).
NETWORK	Infrastruttura fisica di trasporto dei dati a supporto dell'infrastruttura di virtualizzazione (non vi rientrano le Virtual Network).
PHYSICAL	Spazi fisici che ospitano gli strumenti ed il personale che confluiscono nell'erogazione del servizio.

1 – Descrizione Servizi

2 – Metodologia

3 – Aree di responsabilità

4 - Riepilogo

Shared Security Responsibility Model

Responsabilità: Condivisa PSN e PA

Business Continuity Management and Operational Resilience

Il dominio Business Continuity and Operational Resilience (BCR) aiuta i CSP e i CSC a garantire che i servizi cloud siano affidabili. Il dominio guida le **strategie di continuità e resilienza**, per consentire alle organizzazioni di **continuare l'attività di fronte a interruzioni previste e impreviste**. Il dominio stabilisce i requisiti per definire il **governo della continuità** (politiche aziendali, valutare l'impatto dell'indisponibilità e dei rischi) sia **aspetti operativi** (creazione di piani di continuità operativa e la relativa documentazione, test dei piani di continuità documentati e capacità di comunicazione formale) ed **aspetti tecnologici** (capacità di **backup**, eventuali **Disaster Recovery** e ridondanze delle apparecchiature pertinenti).

Responsabilità Pubblica Amministrazione (CSC)

Nell'ambito del servizio BaaS il cliente è responsabile **di definire in autonomia le caratteristiche del proprio backup** (scope, retention, frequenza, numero di jobs) che nel caso di **servizio IaaS saranno gestiti in autonomia (un-managed)** mentre negli **altri servizi Cloud verranno gestiti da PSN sulla base dei requisiti forniti (managed).** Anche l'attività di restore è gestita in autonomia dal cliente nei servizi IaaS, mentre viene lasciata a gestione di PSN negli altri servizi.

E' inoltre possibile per il cliente attivare **on-top il servizio di Golden Copy**, il quale assicura che: 1- il backup viene svolto su copia "WORM" (write once, read multiple) che comporta la possibilità di scrivere solamente una volta e non poter sovrascrivere o cancellare fino alla scadenza della retention scelta dal cliente; 2- i repository delle Golden Copy sono distinti dai repository di backup, completamente separati e configurati in ottica air-gapped; 3 - l'ambiente Golden Copy è protetto da apposita tecnologia ransomware protection.

Responsabilità PSN (CSP)

PSN, nell'ambito dell'erogazione del servizio BaaS, definisce due modelli di servizio: Un-Managed (per servizi IaaS) e Managed (per altri servizi).

Servizi IaaS: il CSC definisce lo scope del backup (può essere inserito l'intero workload del servizio, non solo le VM) , la frequenza dei backup e le policy per configuare i job e la retention, che vengono eseguiti secondo quanto definito da policy.

Altri servizi: servizio managed gestito direttamente dal CSP che controlla in autonomia i job di backup (con retention 10 giorni, frequenza full settimanale, incrementale giornaliero - parametri che possono essere integrati dal CSC in sede di contrattualizzazione) e si assicura di comunicare al cliente eventuali job non andati a buon fine). Gestisce il restore sulla base della richiesta cliente.

Polo Strategico Nazionale

Navigatore

SERVICE LAYERS

- DATA
- APPLICATION
- RUNTIMES
- MIDDLEWARE
- OS (Operating System)
- HYPERVISOR
- HARDWARE
- NETWORK
- PHYSICAL

Legenda Responsabilità

= P.A.

= PSN

= Non Applicabile

1 – Descrizione Servizi

2 – Metodologia

3 – Aree di responsabilità

4 - Riepilogo

Shared Security Responsibility Model

Matrice di sintesi

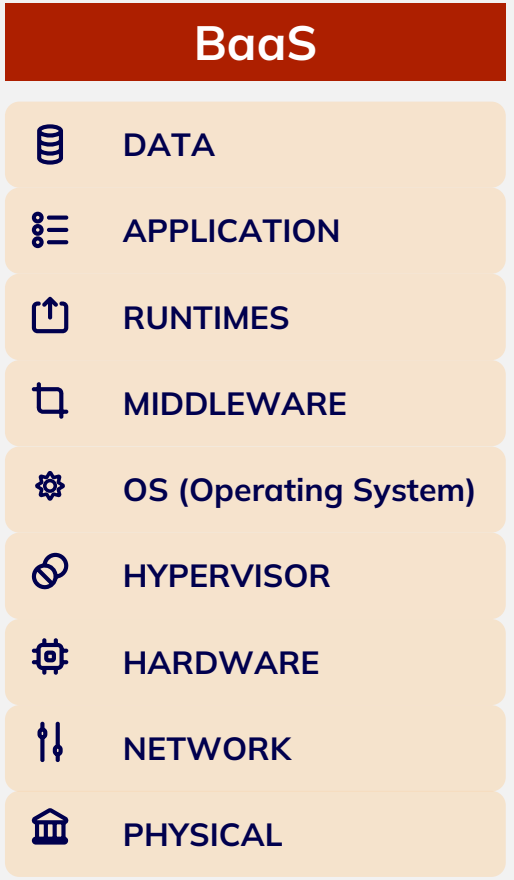
A riepilogo degli ambiti di responsabilità descritti all'interno documento, è possibile riassumere che per i servizi **BaaS** la sicurezza del servizio è suddivisa secondo le seguenti aree di responsabilità:

Responsabilità Pubblica Amministrazione (CSC)

Il servizio BaaS è acquistabile esclusivamente come integrazione ad un altro servizio erogato da PSN. Pertanto, **ad eccezione di quanto specificato nel dominio BCR**, assume le stesse responsabilità indicate nella Matrice di Responsabilità del servizio al quale viene associato.

Responsabilità PSN (CSP)

Il servizio BaaS è acquistabile esclusivamente come integrazione ad un altro servizio erogato da PSN. Pertanto, **ad eccezione di quanto specificato nel dominio BCR**, assume le stesse responsabilità indicate nella Matrice di Responsabilità del servizio al quale viene associato.



Polo Strategico Nazionale

Cloud sicuro per l'Italia digitale.

www.polostrategiconazionale.it