TRUSTED CLOUD

Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS)

Autore: Aldo Pedico – Enterprise Security & Privacy

Contatto: pedicoaldo@gmail.com

Suggerisco ai funzionari del #Governo italiano e ai politici che decideranno di esternalizzare (outsourcing) presso fornitori di servizi #cloud le attività informatiche pubbliche (che trattano anche dati miei!) di leggere attentamente la guida "NIST SP 1800-19 - TRUSTED CLOUD: SECURITY PRACTICE GUIDE FOR VMWARE HYBRID CLOUD INFRASTRUCTURE AS A SERVICE (IAAS) ENVIRONMENT"

PERCHÉ?

Perché le occupazioni principali (del cliente) sull'adozione della tecnologia cloud sono la protezione delle informazioni e delle risorse virtuali e la visibilità sufficiente per condurre la supervisione e garantire la conformità con le leggi e le pratiche aziendali applicabili.

*Il Cliente (*l'Ente di Stato*) può affrontare queste occupazioni (che non devono trasformarsi in PREOCCUPAZIONI) implementando i cosiddetti* TRUSTED COMPUTE POOLS.

Attraverso questi pool, l'organizzazione può salvaguardare la sicurezza e la privacy delle loro applicazioni e dei dati eseguiti all'interno di un cloud o trasferiti tra un cloud privato e un cloud ibrido o pubblico.

L'obiettivo deve essere, attraverso le sue capacità, la gestione della sicurezza fornite da pool di elaborazione affidabili in un modello di cloud ibrido, includendo le seguenti funzionalità:

- ✓ *unico punto di controllo per la gestione e il monitoraggio dei carichi di lavoro cloud, comprese le configurazioni software e le vulnerabilità;*
- ✓ *protezione dei dati e applicazione della gestione delle chiavi di crittografia incentrata su di un pool di risorse/fiducia e geolocalizzazione e migrazione sicura dei carichi di lavoro cloud;*
- ✓ *gestione delle chiavi e keystore controllati dall'organizzazione, non dal fornitore di servizi cloud;*
- ✓ *segmentazione persistente del flusso dei dati prima e dopo la migrazione sicura dei pool di risorse e che siano basati sulla fiducia e sulla geolocalizzazione;*

- ✓ *applicazione della compliance del settore industriale e/o dell'organizzazione aziendale per i carichi di lavoro regolamentati tra i cloud privati e ibridi/pubblici in locale.*

Queste funzionalità aggiuntive non solo garantiscono che i carichi di lavoro cloud siano eseguiti su hardware e in una geolocalizzazione affidabili o all'interno del confine logico, ma migliorano anche le protezioni per i dati nei carichi di lavoro e nei flussi di dati tra i carichi di lavoro.

Negli ambienti cloud, i carichi di lavoro sono costantemente aumentati, scalati, spostati e chiusi.

Il Cliente spesso può riscontrare che l'adozione di tecnologie cloud non sia una buona proposta commerciale perché incontrano uno o più dei problemi di seguito descritti.

1st. Non è possibile mantenere una sicurezza e una protezione della privacy coerenti per le informazioni (applicazioni, dati e metadati correlati) tra piattaforme, anche per una singola classe di informazioni.

2nd. Non si dispone della flessibilità necessaria per decidere come proteggere le diverse informazioni, ad esempio fornendo una protezione più forte per le informazioni più sensibili in un ambiente MULTI-TENANCY.

3rd. Non è possibile mantenere la visibilità su come le proprie informazioni sono protette per garantire la conformità coerente con i requisiti legali e aziendali.

Il Cliente, in particolare quelle in settori regolamentati come la #finanza e la #sanità, affronta ulteriori sfide perché le leggi sulla sicurezza e sulla privacy variano in tutto il mondo (sedi in cui il fornitore cloud mantiene le risorse per il Trattamento dei dati e i dati).

Le leggi (per la protezione delle informazioni che l'organizzazione raccoglie, elabora, trasmette o archivia) possono variare a seconda di chi sono le informazioni, che tipo di informazioni sono e dove si trovano.

Le tecnologie cloud possono spostare silenziosamente i dati di un'organizzazione da una giurisdizione all'altra.

Poiché le leggi in alcune giurisdizioni possono entrare in conflitto con le politiche di un'organizzazione o con le leggi e i regolamenti locali, un'organizzazione può decidere di dover limitare i server cloud privati o ibridi/pubblici locali che utilizza in base alla loro geolocalizzazione per evitare problemi di conformità.

Il Cliente DEVE *mantenere coerenti le protezioni della sicurezza e avere sia la visibilità sia il controllo per i propri carichi di lavoro su cloud privati "on-premise" e cloud ibridi/pubblici di terze parti al fine di soddisfare i propri requisiti di sicurezza e conformità.*

Ciò è ulteriormente complicato dalla necessità del Cliente di rispettare le leggi sulla sicurezza e sulla privacy applicabili alle informazioni che raccolgono, trasmettono o conservano, che possono cambiare a seconda di chi sono le informazioni (ad esempio, cittadini europei ai sensi del regolamento generale sulla protezione dei dati), che tipo di informazioni si tratta (ad es. informazioni sanitarie rispetto a informazioni finanziarie) e in quale stato o paese informazioni si trovino.

Inoltre, un Cliente deve essere in grado di soddisfare le proprie politiche implementando controlli appropriati dettati dalle sue decisioni basate sul rischio sulla necessaria sicurezza e riservatezza delle sue informazioni.

Poiché le leggi di una località possono entrare in conflitto con le politiche o i mandati di un Cliente, la sua organizzazione può decidere di dover limitare il tipo di server cloud che utilizza, in base allo stato o al paese.

Pertanto, gli ostacoli principali a una più ampia adozione delle #tecnologie cloud sono le capacità di proteggere le proprie informazioni e risorse virtuali nel cloud e di avere una visibilità sufficiente su tali informazioni in modo da poter svolgere la supervisione e garantire che essa e il suo fornitore cloud rispettino le leggi e le pratiche commerciali applicabili.

Inoltre, ci sono sfide tecniche e decisioni architetturali che devono essere prese quando si collegano due cloud diversi.

Una considerazione importante ruota attorno al tipo di rete geografica che collega il cloud perché può influire sulla latenza dei carichi di lavoro e sulla posizione di sicurezza del piano di gestione tra le due infrastrutture.

Il Cliente deve essere in grado di monitorare, tracciare, applicare e far rispettare le proprie politiche di sicurezza e privacy sui propri carichi di lavoro cloud in base ai requisiti aziendali in modo coerente, ripetibile e automatizzato.

La guida del NIST, precedentemente indicata, consentirà al Cliente, nei settori regolamentati di sfruttare la flessibilità, la disponibilità, la resilienza e la scalabilità dei servizi cloud.

L'organizzazione del Cliente sarà in grado di:

- ✓ *mantenere la sicurezza e la protezione della privacy coerenti per le informazioni attraverso le piattaforme cloud;*
- ✓ *dettare come proteggere le diverse informazioni, ad esempio avere una protezione più forte per le informazioni più sensibili;*
- ✓ *mantenere la visibilità su come le loro informazioni sono protette, al fine di garantire la conformità coerente con i requisiti legali e aziendali.*