Residenza dei dati

Prospettive delle Policy di AWS

Agosto 2020

Avvisi

I clienti sono responsabili della propria valutazione autonoma delle informazioni contenute in questo documento. Questo documento: (a) è solo a scopo informativo, (b) mostra le offerte e le pratiche attuali dei prodotti AWS soggette a modifiche senza preavviso e (c) non crea alcun impegno o garanzia da parte di AWS e dei suoi affiliati, fornitori o licenziatari. I prodotti o servizi AWS sono forniti "così come sono" senza garanzie, dichiarazioni o condizioni di alcun tipo, sia esplicite che implicite. Le responsabilità e gli obblighi di AWS verso i propri clienti sono disciplinati dagli accordi AWS e il presente documento non è né parte né modifica di alcun accordo tra AWS e i suoi clienti.

Sommario

Introduzione

Nell'attuale complesso ambiente digitale, le organizzazioni pubbliche continuano ad avere dubbi legittimi per quanto riguarda la sicurezza dei loro dati. Di conseguenza, alcuni governi hanno stabilito che l'obbligo di residenza dei dati, che richiede che tutti i contenuti dei clienti elaborati e memorizzati in un sistema IT rimangano all'interno dei confini di uno specifico paese, fornisce un ulteriore livello di sicurezza. La residenza dei dati riflette una combinazione di problemi associati soprattutto con i rischi di sicurezza percepiti (e in alcuni casi reali) per quanto riguarda l'accesso ai dati da terze parti, come forze dell'ordine straniere. I clienti del settore pubblico vogliono essere sicuri che i propri dati siano protetti da accessi indesiderati che provengono non solo da minacce illecite, ma anche da altri governi.

Una posizione rigorosa riguardo la residenza dei dati a volte limita l'utilizzo di fornitori di servizi cloud (CSP, Cloud Service Providers) su larga scala e multinazionali (spesso chiamati CSP "hyperscale"). Problemi generali di sicurezza cibernetica e di potenziali intrusioni da parte di entità governative hanno contribuito a una continua percezione secondo la quale alcuni tipi di dati dovrebbero essere conservati nel paese di provenienza. Tuttavia, tali percezioni si rivelano controproducenti rispetto all'obiettivo di mettere efficacemente al sicuro i dati del settore pubblico. Come sarà discusso in seguito, un CSP hyperscale, che può avere infrastrutture in un paese diverso da quello del settore pubblico in questione, offre ai propri clienti alti livelli di protezione dati attraverso la protezione della propria piattaforma e con strumenti chiavi in mano per i propri clienti. Architetture solide e pratiche di gestione del cloud, quindi, incrinano i dubbi che portano i clienti a considerare restrizioni nella residenza dei dati.

I servizi cloud hyperscale rappresentano un elemento di assoluta trasformazione nell'uso della tecnologia, grazie all'alto grado di efficienza, agilità e innovazione in grado di fornire una sicurezza di prim'ordine a supporto dei propri clienti. I CSP hyperscale creano, operano e gestiscono servizi per consentire ai clienti di diversi settori (commerciali, pubblici, regolamentati) di risolvere alcuni dei rischi e delle vulnerabilità più comuni. I clienti si affidano alle offerte del CSP hyperscale per attuare pratiche di sicurezza dinamiche e reattive alle minacce in tempo reale, migliorando così notevolmente il livello di sicurezza di ogni cliente. I CSP, in particolare i CSP con servizi a pagamento in base al consumo (pay-as-you-go), sono incentivati a mantenere una sicurezza cibernetica di elevato livello in quanto altrimenti andrebbero incontro a importanti conseguenze a lungo termine, come impatti associati a sistemi compromessi, perdita della fiducia dei clienti e danni alla propria immagine. In altre parole, una sicurezza all'avanguardia è fondamentale per CSP hyperscale di successo e la sicurezza deve essere integrata completamente nel disegno, nello sviluppo e nell'operatività di servizi cloud hyperscale.

Questo documento si concentrerà sui seguenti punti:

- Sfatare i luoghi comuni sui rischi di sicurezza percepiti dai governi e che portano a preferire una residenza dei dati nel paese di origine.
- Illustrare gli impatti negativi nei settori commerciale, pubblico e, in generale, tecnologico che nascono da politiche di residenza dei dati nel paese di origine per quanto riguarda i dati governativi.
- Esprimere considerazioni che i governi devono valutare prima di mettere in atto requisiti che possono limitare involontariamente gli obiettivi di trasformazione digitale del settore pubblico e che portano a un aumento del rischio di sicurezza cibernetica.

Perché la residenza dei dati non fornisce una maggiore sicurezza

La proprietà e il posizionamento geografico dei dati sono diventati un argomento fondamentale per le iniziative di cybersecurity e cloud policy in tutto il mondo. Storicamente, comando e controllo sui dati sensibili delle aziende significavano ospitare le informazioni in locale o in strutture di proprietà fisicamente accessibili di un appaltatore situate all'interno del paese.

Possedere l'intero "stack", ovvero dal pavimento dell'edificio ai software nei server, ha convinto le persone che i propri dati fossero più al sicuro possibile. Questa logica esiste ancora per molti governi.

Con l'evoluzione della tecnologia, tre fondamentali realtà hanno ridimensionato il tradizionale modello del "full stack control":

1. **La maggior parte delle vulnerabilità sono sfruttate in modalità remoto.** La collocazione fisica dei dati ha un impatto minimo o nullo sulle minacce provenienti dalla rete. I sistemi connessi a Internet espongono un'organizzazione a un ampio spazio di minacce, che si propagano da qualsiasi luogo. Per esempio, il recente ransomware Petya ha colpito i servizi sanitari rallentando le loro operazioni e la capacità di prestare le cure ai pazienti. Questo è stato il risultato di un malware diffuso attraverso internet che ha colpito il data center locale. Nonostante un grande sforzo per mettere al sicuro i sistemi interconnessi tramite firewall e altri dispositivi anti-intrusione, l'esperienza ci ha insegnato che la sicurezza perimetrale è solamente una piccolissima parte di un sistema protetto. Indipendentemente dall'ubicazione fisica, se i sistemi informatici sono in qualche modo collegati a internet (o ad altre reti multi-party), anche indirettamente, corrono il rischio e sono suscettibili a un ampio spettro di minacce di accesso logico.

Indipendentemente dall'ubicazione fisica, se i sistemi IT sono in qualche modo collegati a internet (o ad altre reti multi-party), anche indirettamente, sono esposti a un notevole rischio.

2. **I processi manuali presentano il rischio di errore umano.** Gli errori nei processi manuali sono una delle cause principali (se non l'unica causa) della maggior parte degli eventi di cybersecurity. Un esempio comune è la mancata applicazione di patch a sistemi vulnerabili con aggiornamenti software pubblicati molti mesi prima di un exploit. Il processo manuale di aggiornamento dei sistemi con le patch più recenti è difficile e non praticabile regolarmente senza automazione.
3. **Le minacce interne rimangono un rischio importante.** La stragrande maggioranza dei principali furti di dati si è verificata a causa di errori involontari o di comportamenti intenzionali da parte di individui che hanno utilizzato account autorizzati e hanno permesso tali furti. Le maggiori violazioni di dati degli ultimi anni si devono principalmente a pratiche scadenti di sicurezza digitale. Gli scenari di minacce più comuni provenienti da account autorizzati includono:

- Atti involontari: credenziali perse o mal gestite sfruttate da un hacker in grado così di accedere a sistemi attraverso un account valido.
- Ingegneria sociale: attacchi di phishing e di ingegneria sociale che permettono agli hacker ti ottenere credenziali di accesso da utenti o amministratori attraverso l'inganno.
- Comportamenti dolosi: classica minaccia interna (malintenzionati all'interno dell'organizzazione con intenti illeciti).

La collocazione fisica dei dati non protegge da nessuna delle realtà menzionate sopra.

Nell'attuale clima digitale, la gestione del rischio è un'attività ancora più ardua quando si prendono in considerazione la tecnologia mobile e le correlazioni tra entità esterne e interne. Qualsiasi architettura di sistema senza appropriate misure di sicurezza è esposta a concreti vettori d'attacco, indipendentemente dal luogo fisico dell'infrastruttura o del sistema stesso. Siccome la tecnologia continua ad avanzare e le vulnerabilità e i vettori delle minacce per i clienti continuano a cambiare, i governi devono rivalutare il modo in cui stanno modellando le loro strategie e la tolleranza al rischio. Esempi dal mondo reale hanno dimostrato che conservare i dati sui propri server, i propri centri di elaborazione dati o nei paesi di provenienza non è una misura adeguata per mettere al sicuro i dati.

Per esempio, a causa di un furto di credenziali utenti in un'agenzia governativa degli Stati Uniti, si è verificata un'importante violazione di dati che risiedevano in un ambiente locale, causando un impatto su più di 20 milioni di dipendenti federali. Queste credenziali sono state compromesse e usate tramite internet da vari luoghi bypassando tutte le protezioni che l'ambiente in locale offriva. La violazione dati di quest'agenzia governativa degli Stati Uniti è un ottimo esempio di minaccia proveniente dalla rete che ha colpito un sistema, indipendentemente dalla posizione dei dati o dai confini geografici in cui risiedevano.

Possiamo riscontrare questo problema su molti sistemi, non solo quelli connessi a internet. In sistemi senza connessione diretta a internet gli utenti possono accedere alla rete tramite rete VPN (Virtual Private Network) utilizzando laptop, computer fissi o dispositivi mobili. Le violazioni non richiedono un accesso fisico a un server, ma sfruttano la mancanza di controlli di sicurezza logica implementati in modo efficiente. Questo dimostra che la residenza geografica dei dati ha poca rilevanza quando si tratta di proteggere le informazioni dalle attuali minacce. - Al contrario, il miglior meccanismo per proteggere, rilevare, reagire e attuare attività di ripristino è utilizzare la sicurezza offerta da un CSP hyperscale attraverso la modernizzazione e l'automazione. I CSP hyperscale, come AWS, investono sulle migliori pratiche di sicurezza tecnica e operativa e le mettono in atto, perché tale approccio è il fulcro delle loro operazioni e delle loro offerte. I clienti traggono vantaggio dall'utilizzo di un CSP come l'infrastruttura e i servizi cloud di AWS.

Gartner[1] e IDC[2], due organizzazioni di ricerca leader nel settore IT, hanno affermato che il grado di sicurezza della maggior parte dei CSP è maggiore o uguale a quello dei migliori centri di elaborazione dati e che la sicurezza non dovrebbe più essere considerata un inibitore primario all'adozione dei servizi cloud. Le organizzazioni in realtà traggono maggior beneficio dai sistemi di sicurezza nativi nel cloud.

Perché il cloud non influenza il rischio di accesso forzato

Per alcuni governi, la richiesta di residenza dei dati serve a mitigare i rischi relativi all'accesso di un'altra entità ai propri dati. Questa sezione intende confrontarsi con l'idea secondo la quale memorizzare i dati di un'entità sovrana in un ambiente CSP hyperscale comporti il rischio che un'entità "forzi l'accesso" a tali dati. Il concetto di "divulgazione forzata" o "accesso forzato" si riferisce ai diritti di accesso ai dati da parte dei governi o dei loro agenti ai sensi di leggi e regolamenti a livello nazionale, provinciale e settoriale in un determinato paese. La preoccupazione percepita è che la divulgazione forzata possa potenzialmente togliere al proprietario dei dati la possibilità di proteggere i propri dati, non potendo impedire che un soggetto governativo vi acceda

invocando l’applicazione di una legge. Tuttavia, un accesso legale ai dati da parte di una nazione sovrana non è un problema specifico del cloud.

Il possesso del sistema fisico, direttamente o attraverso un contratto di outsourcing, non riduce il rischio di accesso forzato perché esistono già altri meccanismi legali che danno ai governi di una giurisdizione i mezzi per richiedere l'accesso ai dati memorizzati in un'altra giurisdizione. Per esempio, i Trattati di mutua assistenza giudiziaria (MLAT, Mutual Legal Assistance Treaties)[3] e le rogatorie[4] sono stati utilizzati per governare le richieste di dati di una nazione sovrana molto prima della nascita della tecnologia cloud.

Rispetto a un tradizionale ambiente locale, le forze dell'ordine devono generalmente superare un numero maggiore di barriere quando cercano di costringere un CSP a rivelare i dati di un altro cliente. Le forze dell'ordine non possono cercare o sequestrare i dati memorizzati nei server di un CSP senza rispettare i quadri giuridici che supportano un insieme ristretto di finalità di applicazione della legge. Inoltre, i CSP possono contestare eventuali richieste estensive, che superano l'autorità del richiedente o non completamente conformi alle leggi applicabili.

Ancora più importante, i CSP come AWS si impegnano pienamente a fornire ai clienti la notifica delle richieste di dati, consentendo al cliente di rivolgersi alle autorità e/o di intraprendere ulteriori azioni appropriate per prevenire la divulgazione non autorizzata dei dati. È importante riconoscere che questa complessa sfida non riguarda solo il governo degli Stati Uniti o le aziende con sede negli Stati Uniti, perché qualsiasi multinazionale è soggetta alle leggi e ai regolamenti applicabili a livello nazionale, provinciale e di settore in qualsiasi paese, indipendentemente dall'ubicazione dei dati.

Limiti all’accesso forzato

Dal XX secolo, molti paesi hanno creato meccanismi legali che consentono l’accesso alle informazioni conservate all’estero per rispondere ad appropriate richieste legittime di informazioni essenziali per indagini e accuse criminali. Per esempio, una società che lavora in un Paese X potrebbe essere soggetta a una richiesta legale di informazioni anche se il contenuto è conservato in un Paese Y come stabilito da accordi legali bilaterali e multilaterali. In molti casi, il meccanismo legale riconosciuto è un trattato di mutua assistenza giudiziaria (MLAT, Mutual Legal Assistance Treaty).

Insieme a MLAT bilaterali tra paesi, ci sono anche MLAT su base regionale, come il MLAT interamericano, il MLAT EU-US e l’ASEAN MLAT. In mancanza di un MLAT, i paesi possono ottenere una rogatoria per chiedere aiuto a governi stranieri. La legge di ogni giurisdizione dovrà contenere criteri che devono essere soddisfatti affinché le forze dell’ordine possano formulare una richiesta valida. Per esempio, un’agenzia governativa che vuole accedere a specifici dati necessiterà di un mandato o

documento del tribunale che dimostrino la ragione valida di tale richiesta. Pur essendo meccanismi legittimi, questi strumenti giuridici non sono stati concepiti per affrontare il problema dell'accesso ai dati da parte delle forze dell'ordine in un mondo digitale.

> Le leggi che permettono alle forze dell'ordine di accedere ai dati conservati all'estero per indagini di crimini seri, come minacce terroristiche, non sono state formulate tenendo in considerazione le tecnologie moderne. Questo ha portato a casi in cui alcune società di tecnologia, che dovevano seguire un provvedimento giurisdizionale ai sensi di una legge di un determinato paese, si trovavano comunque davanti al rischio di violare leggi di un altro paese che proibiva la divulgazione dei dati.
>
> Il CLOUD Act, una legge statunitense sull'uso legale dei dati all'estero, offre un nuovo quadro su come rispondere alle richieste da parte delle forze dell'ordine in caso di accordi esecutivi tra gli Stati Uniti e un altro paese e conferma inoltre, secondo i principi di cortesia tra le nazioni, il diritto dei fornitori di servizi di non divulgare alcun dato qualora si entrasse in conflitto con le leggi di un altro stato, anche in assenza di un accordo esecutivo. Inoltre, questa legge consente ai fornitori di servizi cloud di divulgare i dati ai governi che emettono ordini o mandati per l'accesso alle informazioni, sulla base di fatti sufficienti a dimostrare che si è verificato un reato grave e che le informazioni ricercate sono direttamente collegate a tale reato.

Tentando quindi di allineare le leggi con la moderna tecnologia, gli Stati Uniti hanno approvato il CLOUD Act (Clarifying Lawful Overseas Use of Data) nel marzo del 2018. Il CLOUD Act prevede un terzo meccanismo legale internazionale per accedere ai dati conservati in un altro paese attraverso richieste dirette ai fornitori di servizi.[5] Il CLOUD Act stabilisce le procedure per stipulare accordi esecutivi tra Stati Uniti e altri paesi. Questi accordi esecutivi mirano a rimuovere le restrizioni legali che impediscono ad alcune nazioni straniere di richiedere dati direttamente ai fornitori statunitensi, a condizione che le leggi della nazione straniera siano considerate sicure dagli Stati Uniti in termini di tutela della privacy e delle libertà civili. Secondo il CLOUD Act, i CSP hanno il diritto di non divulgare informazioni se questo non rispettasse le leggi di un altro paese. Il MLAT, le rogatorie e gli accordi esecutivi del CLOUD Act offrono reciprocamente meccanismi legali internazionali che permettono alle forze dell'ordine di accedere ai dati conservati all'estero.

Le leggi nazionali di un paese si applicano in genere a tutte le società che operano in quel paese, indipendentemente dal luogo in cui la società è costituita o dal fatto che le informazioni siano memorizzate in cloud, data center in locale o in record fisici. Mentre i paesi continuano a digitalizzare e avanzare verso società più moderne basate sulle

informazioni, si sono evoluti anche i regimi di accesso forzato legale a sostegno delle indagini per i reati gravi che hanno un impatto sulla sicurezza nazionale, come il terrorismo. La promulgazione del CLOUD Act è un altro quadro che mira a rafforzare il processo legale per le richieste da parte delle autorità giudiziarie in questo contesto moderno.

> Costringere i CSP a una solo giurisdizione non isola meglio i dati da accessi governativi.
>
> Un'analisi legale indipendente condotta tra i primi utilizzatori di cloud computing governativi ha valutato le leggi specifiche del paese che regolano l'accesso delle forze dell'ordine ai dati nei cloud archiviati all'estero. Questo studio ha valutato 10 giurisdizioni internazionali: Australia, Canada, Danimarca, Francia, Germania, Irlanda, Giappone, Spagna,
>
> Regno Unito e Stati Uniti e ne è risultato che costringere i CSP a una solo giurisdizione non isola meglio i dati da accessi governativi.

La realtà è che tale accesso forzato si verifica in un numero molto limitato di casi e generalmente solo quando c'è un estremo bisogno di informazioni (ad esempio, per prevenire eventi relativi ad attacchi terroristici). Per mitigare anche questo ridotto rischio, le organizzazioni possono mettere in campo attività di "due diligence" e sviluppare i propri sistemi di protezione con i servizi cloud disponibili. Con AWS, mitigazioni come la cifratura di dati a riposo e in transito, la decomposizione e la distribuzione dei dati e le strategie di tokenizzazione possono essere utilizzate per una frazione del carico di risorse, sostituendo soluzioni in locale.

AWS protegge i contenuti dei propri clienti, indipendentemente dalla provenienza della richiesta o da chi sia il cliente. AWS non divulgherà i contenuti del cliente, a meno che ciò non si renda necessario per ottemperare a un ordine legalmente valido e vincolante, come un mandato di comparizione o un ordine del tribunale. AWS esaminerà attentamente ogni richiesta, per accertarne l'accuratezza e verificarne la conformità alle leggi applicabili. AWS rigetterà eventuali richieste estensive, che superano l'autorità del richiedente o non sono completamente conformi alle leggi applicabili. Salvo diversa disposizione ai sensi di legge, AWS tenterà inoltre di reindirizzare la richiesta direttamente al cliente, offrendo così la possibilità di agire contro tale richiesta. Per ulteriori informazioni visitare il nostro ultimo report sulla trasparenza e le nostre linee guida Amazon Law Enforcement.[6]

Perché il rischio di accessi non autorizzati è inferiore nel cloud

Per alcuni governi, la richiesta di residenza dei dati serve a mitigare i rischi relativi all'accesso di un'altra entità ai propri dati. Questa sezione intende confrontarsi con l'idea secondo la quale il rischio di accesso non autorizzato sarebbe più grande quando si utilizza un CSP hyperscale. Gli accessi non autorizzati sono le minacce più comuni provenienti da entità malevole che vogliono ottenere l'accesso ai dati dei clienti per diversi usi. L'accesso non autorizzato può includere preoccupazioni di accesso di terzi, compresa la possibilità di minacce da parte di fonti interne o di attori esterni malintenzionati.

I requisiti di residenza dei dati non tengono conto delle vie comuni utilizzate dagli aggressori per accedere ai dati. Lo sfruttamento di questi vettori è quasi sempre il risultato di noncuranza nell'applicazione delle discipline di sicurezza digitale, come la gestione dell'inventario del sistema, la gestione della configurazione, la crittografia dei dati e la gestione degli accessi privilegiati.

Mitigare gli accessi non autorizzati

Per prevenire gli accessi non autorizzati è necessario applicare adeguatamente le norme sulla sicurezza e implementare robuste azioni preventive e analitiche. Per esempio, i sistemi devono essere progettati per limitare il "raggio d'azione" di ogni intrusione in modo che un nodo compromesso abbia il minor impatto possibile su qualsiasi altro nodo dell'organizzazione. I CSP Hyperscale, come AWS, offrono un ambiente dotato di strumenti di sicurezza che consentono ai clienti di avere comunicazioni criptate e implementare le necessarie protezioni da manomissioni per mitigare il rischio di accessi non autorizzati. I contenuti degli account dei clienti non sono né accessibili, né visibili per AWS, indipendentemente dal fatto che questi includano o meno informazioni personali. I clienti AWS possono usare diverse tecniche, come cifratura,[7] tokenizzazione, decomposizione dei dati e meccanismi di "deception technology" per rendere i contenuti non visibili a AWS o altre parti che cercano di accedervi.

- Cifratura - Cifrare in maniera appropriata i dati li può rendere non leggibili. Questo significa che conservare dati cifrati nel cloud, indipendentemente dalla collocazione geografica, può offrire un'adeguata protezione contro la maggior parte delle minacce di esfiltrazione. È fondamentale che le chiavi di cifratura di questi dati siano gestite con attenzione per assicurare che le protezioni possano far fronte a qualsiasi tipo di intercettazione. AWS offre servizi in grado di fornire queste funzionalità a livello aziendale con AWS CloudHSM o AWS Key Management Service (KMS).[8] Il livello di controllo sul metodo di crittografia, la

memorizzazione delle chiavi crittografiche e la gestione delle chiavi crittografiche utilizzate con i dati è a discrezione del cliente.[9]

- Tokenizzazione - La tokenizzazione è un processo che permette di definire una sequenza di dati per rappresentare un'informazione altrimenti sensibile (ad esempio, un token che rappresenti il numero della carta di credito di un cliente). Un token non ha senso da solo e non può essere ricondotto ai dati che rappresenta senza l'uso del sistema di tokenizzazione. Gli archivi dei token possono essere sviluppati in VPC per memorizzare informazioni sensibili in forma cifrata, condividendo i token con i servizi approvati per la trasmissione di dati offuscati. Inoltre, AWS collabora con partner specializzati nell'offrire servizi di tokenizzazione integrabili con i database più comuni e altri servizi di archiviazione.
- Decomposizione dei dati – Si tratta di un processo che riduce insiemi di dati in elementi irriconoscibili che da soli non hanno alcun significato.[10] Questi elementi o frammenti vengono poi memorizzati in maniera distribuita, in modo che qualsiasi elemento compromesso in un nodo produca solo un frammento di dati di dimensioni irrisorie. Un particolare vantaggio di questa tecnica è il fatto che le minacce devono compromettere tutti i nodi, ottenere tutti i frammenti e conoscere l'algoritmo (o lo schema di frammentazione) per riunire i dati in maniera coerente.
- Cyber difesa mediante deception technology – Le architetture e le soluzioni di deception possono essere componenti chiave per mitigare gli agenti malevoli più evoluti. Le soluzioni di deception possono utilizzare trappole ed esche talmente sofisticate da dare a un aggressore la percezione di essersi infiltrato nel sistema, mentre in realtà viene deviato in un ambiente altamente controllato. Vengono raccolte informazioni sull'aggressore per mitigare le minacce future e l'attacco viene neutralizzato.

I clienti sono anche preoccupati dell'adeguatezza delle misure di controllo degli accessi per prevenire l'accesso non autorizzato da parte del personale CSP. Obblighi e aree di responsabilità (per esempio, richieste e approvazioni di accesso, richieste e approvazioni sulla gestione dei cambiamenti, ecc.) devono essere isolati tra diverse persone per ridurre le opportunità di una modifica non autorizzata o involontaria o per un uso improprio dei sistemi AWS. Il personale AWS che ha la necessità di accedere al sistema di gestione deve prima utilizzare l'autenticazione multi-fattore, diversa dalle normali credenziali aziendali di Amazon, per accedere a host amministrativi costruiti ad hoc. Questi host amministrativi sono sistemi progettati, sviluppati, configurati e rafforzati specificamente per proteggere il sistema di gestione. Tutti questi accessi predispongono accurati log e associati strumenti di audit. Quando un dipendente non ha più una necessità aziendale di accedere al sistema di gestione, gli sono revocati privilegi e accesso a questi host e ai relativi sistemi. AWS ha implementato una politica

di blocco di sessione che è applicata in maniera sistematica. Il blocco della sessione viene mantenuto fino a quando non vengono eseguite le procedure di identificazione e autenticazione stabilite.

AWS controlla anche che non avvengano gestioni remote non autorizzate e, se necessario, disconnette o disattiva rapidamente l'accesso remoto non autorizzato. Tutti i tentativi di accesso amministrativi remoti sono registrati e i log sono controllati per rilevare eventuali attività sospette; ciò avviene non solo da parte del personale, ma anche da sistemi di apprendimento automatico, sviluppati dal team di sicurezza AWS per individuare schemi di accesso insoliti che potrebbero indicare tentativi non autorizzati di accesso ai dati. Se viene rilevata un'attività sospetta, verranno avviate le relative procedure di risposta agli incidenti. Inoltre, AWS ha stabilito politiche e procedure formali per delineare standard di accesso logico alle infrastrutture e agli host AWS. Queste politiche identificano inoltre responsabilità funzionali per l'amministrazione di accesso logico e sicurezza. A meno che non sia proibito dalla legge, AWS richiede che tutti i dipendenti siano sottoposti a un background check commisurato alla loro posizione e al loro livello di accesso.

Infine, le istanze virtuali dei clienti sono controllate esclusivamente dal cliente che ha il pieno accesso *root* o il controllo amministrativo su account, servizi e applicazioni. Il personale AWS non può eseguire l'accesso alle istanze dei clienti.

Cloud hyperscale: un approccio trasformazionale alla sicurezza

I CSP hyperscale leader nel settore, come AWS, offrono ai clienti l'opportunità di sviluppare sistemi di sicurezza adattivi e altamente resilienti per i propri carichi di lavoro. Limitare le operazioni a specifici requisiti del paese, dove è presente una regione AWS, inibirebbe l'innovazione dei servizi e ostacolerebbe la capacità di compensare le minacce, come quelle che mirano alla disponibilità. Un'altra conseguenza dei vincoli geografici legati al paese è che gli attori della minaccia possono ottenere un'accuratezza nella fase di identificazione dei bersagli sapendo che i dati devono risiedere in aree specifiche. I CSP hyperscale hanno a disposizione servizi e architetture di supporto per offrire sia la protezione in profondità[11] che la difesa in ampiezza[12] . Ciò è dovuto al fatto che i meccanismi di sicurezza sono intrinseci alla progettazione e al funzionamento delle offerte dei CSP hyperscale.

> Una conseguenza non intenzionale dei requisiti di residenza dei dati all'interno del paese è il fatto che i malintenzionati possono ottenere una maggiore precisione nella fase di identificazione dei bersagli sapendo che i dati risiedono in luoghi specifici.

I seguenti 6 elementi riflettono gli attributi centrali di sicurezza che sono una parte integrante di un CSP hyperscale come AWS:

1. Un'integrazione profonda di sicurezza e conformità (ottenuta raramente con i sistemi tradizionali) significa che la sicurezza trae direttamente beneficio dalla conformità in quanto i controlli di sicurezza sono costantemente monitorati e aggiornati.
2. Le economie di scala si applicano non solo alla tecnologia, ma anche al personale e ai processi di sicurezza, con un ritorno sull'investimento senza precedenti rispetto ai sistemi tradizionali.
3. Il CSP controlla la maggior parte della "superficie" di sicurezza, eseguendo con professionalità e competenza superiori a quelle di quasi tutti i clienti sulla terra. Di conseguenza, i clienti possono concentrare i loro professionisti della sicurezza e le loro risorse su una porzione molto più piccola della superficie da proteggere, come la sicurezza delle applicazioni.
4. Il cloud offre visibilità, omogeneità e automazione mai viste prima nei sistemi tradizionali, a tutto vantaggio della sicurezza. Ciò include capacità di auditing e di logging molto approfondite: ad esempio, un cliente ha la possibilità di tenere traccia di tutte le chiamate API che registrano le azioni intraprese da un CSP relativamente al proprio account.
5. I CSP operano come una sorta di "contenitore di sistema" che fornisce una comprensione molto più approfondita del comportamento e del funzionamento del sistema, comprese le operazioni di sicurezza, fornendo ai clienti un nuovo livello di protezione.
6. Con un accesso facile ed economico a enormi quantità di storage e capacità di elaborazione, i clienti AWS "usano il cloud per proteggere il cloud", ovvero eseguono un'analisi accurata sui big data generati dai dati di sicurezza e di monitoraggio. Ciò fornisce una maggiore comprensione della loro security posture e si traduce in una soluzione molto più rapida dei problemi.

Con la velocità dell'innovazione e la crescente scalabilità, la storia della sicurezza nel cloud non potrà che migliorare. Ad esempio, nell'ultimo anno solamente AWS ha aggiunto potenti funzionalità di sicurezza come Amazon GuardDuty [13], un servizio di rilevamento delle minacce gestito da AWS che monitora continuamente la presenza di comportamenti dannosi o non autorizzati; Amazon Macie [14], un servizio che utilizza l'apprendimento automatico per proteggere i dati sensibili; AWS CloudHSM 2.0 [15], un servizio completamente gestito che utilizza hardware convalidato FIPS 140-2 Livello 3 [16] implementato automaticamente in un cluster distribuito su più zone di disponibilità che consente ai clienti di generare, gestire e utilizzare facilmente le proprie chiavi di cifratura in AWS Cloud, senza che AWS possa avere accesso alle chiavi master o alle

operazioni di crittografia di base.

La cifratura dovrebbe essere considerata un servizio essenziale perché funge da mezzo di protezione dati nel caso in cui altri meccanismi non siano in grado di fermare le minacce. Aggiunge un ulteriore livello di sicurezza e garanzia per la riservatezza e l'integrità dei dati in transito e a riposo. La combinazione di AWS Key Management Service (KMS) e di AWS CloudHSM è il fulcro di una soluzione rigorosa per la crittografia.[17] I CSP hyperscale come AWS offrono ubiquitous encryption che possono non essere sostenibili in ambienti on-premise. Per esempio, AWS Key Management Service (KMS), certificato FIPS 140-2 Livello 2, offre un'opzione Bring Your Own Keys (BYOK) che permette ai clienti di usare le proprie chiavi generate e conservate nei loro ambienti in locale, all'interno dei servizi AWS. I clienti possono soddisfare specifici requisiti di sicurezza e conformità su carichi di lavoro altamente sensibili con questi meccanismi in quanto hanno la possibilità di conservare e gestire le proprie chiavi fuori da AWS.

Responsabilità del CSP: sicurezza nativa nel cloud

L'infrastruttura di AWS è creata appositamente per il cloud, presenta tutti gli elementi progettati per intercomunicare efficacemente ed espone al rischio di attacchi una superficie quanto più piccola possibile. Inoltre, i controlli di sicurezza fisici nei nostri centri di elaborazione dati sono stati progettati per essere tra i più severi al mondo. L'architettura AWS è stata rivista e validata attraverso decine di programmi internazionali sulla conformità.[18] Usiamo auditor e sistemi di valutazione indipendenti per valutare e certificare la nostra aderenza a tali regimi e offriamo ai clienti l'accesso ai report con i risultati e le prove a sostegno. Per soddisfare una così vasta gamma di requisiti di sicurezza, AWS costruisce i propri centri di elaborazione dati e la propria architettura in modo da scalare e progredire di pari passo con l'innovazione. Questo approccio ha fatto sì che quella di AWS diventasse un'infrastruttura affidabile per governi, organizzazioni militari, banche globali, istituzioni sanitarie e altre organizzazioni che operano dati altamente sensibili.

Per AWS, il nostro ambiente unico è stato uno stimolo a costruire molti dei nostri strumenti di sicurezza. Questi strumenti automatizzano un'ampia gamma di attività di routine, consentendo ai nostri esperti di sicurezza di concentrarsi sugli aspetti critici come la sicurezza dell'ambiente. I nostri strumenti si traducono in requisiti di sicurezza che costituiscono parte integrante e vengono soddisfatti durante tutto il ciclo di vita dello sviluppo del sistema. I problemi comuni di sicurezza vengono risolti nelle fasi iniziali di sviluppo del sistema, consentendo ai nostri esperti di sicurezza di concentrarsi sulla mitigazione di minacce avanzate e complesse in fase di produzione.

I nostri team di sicurezza controllano l'infrastruttura tutto il giorno, ogni giorno e sono connessi con tutti i principali gruppi watchdog e fornitori per identificare

immediatamente le potenziali minacce. Ciò avviene su vasta scala ed è un elemento che contraddistingue l'organizzazione di sicurezza di AWS. Utilizzando complessi algoritmi per analizzare milioni di account attivi dei clienti che eseguono praticamente ogni tipo di carico di lavoro immaginabile, siamo in grado di individuare problemi che possono verificarsi solo una volta su un miliardo di operazioni più volte al giorno. Quando risolviamo il problema, lo facciamo per l'intera piattaforma. Questo tipo di visibilità e reazione non è facile da ottenere per la maggior parte delle organizzazioni con centri di elaborazione dati on- premise. Il valore che deriva dalla competenza focalizzata e dall'alta scalabilità spiega perché Gartner e IDC hanno stabilito che i carichi di lavoro su cloud pubblici di tipo infrastructure as a service (Iaas) subiranno meno incidenti di sicurezza rispetto a quelli dei centri di elaborazione dati tradizionali. La ricerca di Gartner stima una riduzione di almeno il 60% negli incidenti di sicurezza cibernetica.[19]

Ulteriore opzione on-premise per esigenze di localizzazione

L'adozione del cloud è un percorso in più fasi che consiste in una migrazione graduale, spesso riflessa in un approccio di cloud ibrido (cioè, carichi di lavoro distribuiti in ambienti on-premise e su ambienti cloud commerciali). Per diversi motivi, i clienti possono pensare che alcuni carichi di lavoro siano più adatti per una gestione in locale, sia che si tratti di latenze più ridotte o di altre necessità locali di elaborazione.

AWS continua a innovare per fornire ai clienti un ulteriore controllo e maggiore flessibilità nell'implementazione del loro approccio di migrazione del cloud. Per esempio, soluzioni ibride come AWS Outposts[20] forniscono un'opzione che porta i servizi cloud AWS nei centri di elaborazione dati dei clienti, migliorando la flessibilità di scegliere dove distribuire le applicazioni cloud, compresi i carichi di lavoro sensibili.

Prima che AWS lanciasse Outposts, i clienti dovevano operare nella regione AWS più vicina per mantenere i propri dati vicini. Estendendo l'infrastruttura e i servizi AWS al loro ambiente, i clienti possono supportare i carichi di lavoro che devono rimanere in locale utilizzando però le capacità dei servizi cloud commerciali sia in termini operativi che di sicurezza.

Outposts si collegherà all'infrastruttura AWS in una regione a scelta del cliente per scambiare i dati utilizzati per fornire, migliorare e rendere sicuro il servizio. I clienti possono scegliere di conservare i propri contenuti in locale con servizi di storage in Outpost, come EBS. I clienti possono anche scegliere di conservare i propri contenuti all'interno di una regione, per ragioni di disponibilità e durabilità, tipicamente in forma cifrata, per esempio utilizzando snapshot EBS, back-up RDS, ecc.

AWS incoraggia i clienti ad eseguire la classificazione dei propri dati e a individuare quali dati devono rimanere all'interno del loro paese o della loro regione e perché. In tal modo, i clienti potrebbero scoprire che i loro dati, potenzialmente anche sensibili e

critici, possono essere memorizzati e/o replicati altrove se non vi è un particolare requisito geografico legale o di policy. Ciò può ridurre ulteriormente il rischio di perdite in caso di eventi disastrosi e fornire l'accesso a tecnologie e capacità che potrebbero non essere disponibili nella loro area.

Responsabilità del cliente: approccio alle architetture sicure

Le capacità di sicurezza native dei fornitori di cloud hyperscale come AWS danno ai clienti la possibilità di creare architetture uniche per mitigare i rischi di accesso. Le strutture on-premise o simili mancano dell'omogeneità, delle economie di scala, della visibilità e dell'automazione che possono portare grandi progressi in materia di sicurezza. Questi progressi sono necessari per sviluppare sistemi altamente sicuri per contrastare le minacce in evoluzione sia dall'esterno che dall'interno. Le strutture on-premise faticano a impiegare questi nuovi concetti operativi a causa dei requisiti di risorse per la rifattorizzazione della rete, dell'approvvigionamento di nuovi sistemi e del lavoro umano richiesto a causa della mancanza di software-defined infrastructure. I CSP hyperscale costruiscono un livello di agilità e adattabilità nella loro infrastruttura per implementare organicamente questi progressi in materia di sicurezza. Ciò significa che i clienti possono utilizzare più facilmente le nuove funzionalità incluse in quanto queste sono nativamente integrate nell'offerta del CSP, consentendo ai clienti di realizzare sistemi che utilizzano architetture uniche come la micro-segmentazione, i polymorphic design [21] e le reti di deception technology a più livelli.

Ad esempio, dando un'occhiata più da vicino alla progettazione basata sulla micro-segmentazione su AWS, un cliente può utilizzare una vasta gamma di tecnologie tra cui Amazon Virtual Private Cloud (Amazon VPC), AWS Identity and Access Management (IAM), Security Groups, Network Access Control Lists, numerosi servizi di cifratura e di logging e servizi come AWS Certificate Manager per formare la base per lo sviluppo di una rete Zero Trust Model [22] (ZTM). Il modello ZTM può offrire un vantaggio importante per la mitigazione delle minacce e per prestazioni di monitoraggio. Le organizzazioni hanno una chiara necessità di implementare una segmentazione di sicurezza di tipo ZTM o simile per contrastare le minacce attuali, ma è estremamente difficile e costoso sviluppare questo tipo di architettura in ambienti aziendali tradizionali. Il passaggio a un fornitore di servizi cloud pubblico offre alle organizzazioni l'opportunità di implementare concetti ZTM e simili senza il significativo costo e onere di risorse associato all'ammodernamento/sviluppo della rete fisica.

Ruoli per la protezione dei dati

Il modello di responsabilità condivisa prevede cinque concetti fondamentali riguardo la proprietà e la gestione dei dati:

1. I clienti continuano a possedere i propri dati.
2. I clienti scelgono le aree geografiche in cui conservare i propri dati. Questi non verranno spostati a meno che non sia il cliente a decidere di farlo.
3. I clienti possono scaricare o cancellare i propri dati ogni volta in cui lo desiderano.
4. I clienti possono scegliere la “crypto-deletion” dei propri dati cancellando le chiavi master di cifratura richieste per decrittare le chiavi dei dati che sono, a loro volta, richieste per decrittare i dati.
5. I clienti dovrebbero tenere conto della sensibilità dei propri dati e decidere se e come criptarli mentre sono in transito o a riposo.

Le misure di protezione dei dati sono applicate nel modo più efficace dopo aver definito i ruoli rispetto al trattamento dei dati per determinare i ruoli e le responsabilità appropriate degli stakeholder. La maggior parte degli schemi di protezione dei dati fanno una distinzione tra titolare e responsabile del trattamento dei dati e impongono obblighi basati su questi ruoli specifici. Per esempio, secondo il regolamento generale sulla protezione dei dati dell’UE, il titolare del trattamento dei dati è responsabile dell’attuazione di misure tecniche e organizzative appropriate per proteggere i dati dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati.
Qualora il trattamento venisse effettuato da un responsabile del trattamento per conto del titolare del trattamento, quest'ultimo dovrà scegliere un responsabile che attui misure tecniche e organizzative per il trattamento dei dati. Queste distinzioni aiutano a delineare le responsabilità tra il fornitore del servizio e i clienti.

Quando AWS si prefigura come fornitore di infrastrutture self-service, sotto il completo controllo del cliente anche per quanto riguarda le modalità di un eventuale trattamento dei dati, AWS eroga i servizi di infrastruttura per gli utenti che vogliono caricare e trattare contenuti su AWS. AWS non ha alcuna possibilità di visualizzare o conoscere ciò che i clienti caricano sulla propria rete e non sa, quindi, se i contenuti includono dati personali. I clienti di AWS sono inoltre autorizzati e incoraggiati a utilizzare la cifratura per rendere il contenuto incomprensibile per AWS e per qualsiasi terza parte che cerchi di accedere ai dati.

La libera circolazione dei dati non personali proposta come standard de facto dall'UE e l'accordo Trans-pacifico.

La Commissione europea ha recentemente pubblicato un regolamento sulla libera circolazione dei dati ***che vieta le norme nazionali sulla localizzazione dei dati negli Stati membri dell'UE*** e riconosce il principio della libera circolazione dei dati non personali all'interno dell'UE. Questa proposta stabilisce il flusso transfrontaliero di dati come standard de facto, imponendo agli Stati membri l'onere di fornire una giustificazione di sicurezza pubblica per l'imposizione di requisiti di localizzazione dei dati.
Questa proposta riconosce i flussi di dati transfrontalieri come dei vantaggi economici e di sicurezza, che scavalcano qualsiasi tesi a favore dell'imposizione di politiche per la residenza dei dati.

Inoltre, all'inizio del 2018, l'**Accordo globale e progressivo di partenariato transpacifico**, stabilito tra 11 paesi, ha espresso il suo supporto ai ***flussi di dati transfrontalieri*** e, tra le sue condizioni, non prevede che le aziende stabiliscano strutture informatiche nel paese in cui vogliono fare affari.

I servizi AWS sono agnostici rispetto ai contenuti, in quanto offrono lo stesso elevato livello di sicurezza a tutti i clienti, indipendentemente dal tipo di regione geografica del contenuto trattato o conservato. In altre parole, AWS adotta lo stesso livello di sicurezza in tutti i suoi servizi. Ciò significa che scegliamo il più alto livello di classificazione dei dati che transitano o vengono memorizzati nel nostro cloud commerciale e applichiamo gli stessi livelli di protezione a tutti i nostri servizi e per tutti i nostri clienti. Questi servizi sono poi considerati nei processi di certificazione secondo alti standard di sicurezza e conformità, il che si traduce in clienti che beneficiano di elevati livelli di protezione per i dati elaborati e memorizzati nel cloud. Il Cloud AWS è stato certificato secondo gli standard di numerosi settori regolamentati (sanitario, finanziario, ecc.), nazionali (ad es. U.S. FedRAMP, Germany C5, Australia IRAP), e accreditazioni globali (ad es. ISO 27001,[23] ISO 27018,[24] Payment Card Industry (PCI), Data Security Standard (DSS),[25] e Service Organization Controls (SOC)[26], che testano e convalidano la sicurezza dei nostri sistemi rispetto agli standard più rigorosi.

Allineare politica della sicurezza cibernetica, trasformazione digitale e crescita economica

Le politiche devono evolversi per soddisfare le mutevoli realtà della tecnologia e del mondo che essa contribuisce a creare. Diversamente, i governi continueranno a rimanere indietro nel migliorare le loro operazioni, nel servire i cittadini e nell'adottare le

soluzioni più moderne e sicure. Questa sezione descrive come AWS affronta gli obiettivi di sicurezza alla base dei requisiti di residenza dei dati per ridurre le preoccupazioni dei decisori politici. Esplora inoltre le sfide economiche e di modernizzazione IT associate alla residenza dei dati e le considerazioni sulle politiche per far progredire l'adozione sicura del cloud nel settore pubblico.

Le sfide nel settore commerciale e pubblico rispetto alla residenza dei dati

I governi devono considerare in che modo le politiche nazionali fungono da detonatore o ostacolo per le opportunità di crescita economica e sviluppo della forza lavoro, rese possibili dai servizi di cloud hyperscale. Ci possono essere impatti negativi significativi nell'implementazione dei requisiti di residenza dei dati, come ad esempio:

- **Effetto negativo sugli sforzi di espansione commerciale multinazionale delle imprese locali** - Poiché le imprese crescono e si espandono al di fuori delle operazioni regionali, è fondamentale che abbiano accesso a risorse che abbiano una portata globale. La limitazione dell'accesso ai servizi di CSP hyperscale non sviluppa il livello di esperienza utente che un'azienda può fornire alla sua base globale di clienti.
- **Opzioni di ridondanza geografica limitate rispetto alle regioni CSP globali** - Per la stabilità di governi e imprese, è vitale garantire la ridondanza in caso di guasti operativi dovuti a eventi disastrosi o altre circostanze. Avere operazioni raggruppate in un solo paese espone l'organizzazione a un livello di rischio che può superare di gran lunga le preoccupazioni relative all'accesso ai dati.
- **Strutture ad alti costi necessarie per soddisfare requisiti stringenti** - Gli ambienti "cloud" single tenant o sviluppati per una comunità richiedono un livello di prezzi per la sostenibilità operativa che può effettivamente scoraggiare l'acquisizione delle capacità aggiuntive necessarie per raggiungere una protezione in profondità.

La tecnologia cloud è la base per i progressi del settore pubblico e commerciale e la misura in cui i governi promuovono o si oppongono al principio dei flussi di dati transfrontalieri influenzerà la forza delle loro economie locali e la loro competitività sul mercato globale.

Impatto commerciale

Permettere il libero flusso di dati tra le frontiere ha un impatto assolutamente positivo sull’economia globale. Recenti studi provenienti da varie organizzazioni di ricerca enfatizzano questo impatto e sottolineano il costo di stabilire barriere al flusso dati. Un

report del febbraio 2016 del McKinsey Global Institute ha stimato che il flusso dati tra frontiere ha contribuito a quasi 2,8 trilioni di dollari all'economia globale nel 2014[27] attraverso l'attivazione del flusso di beni, servizi e altre risorse. I report stimano che questa cifra potrebbe raggiungere gli 11 trilioni di dollari entro il 2025. I governi che vogliono la localizzazione di dati e limitano i flussi economici tra le frontiere pagano un alto prezzo. Lo European Centre for International Political Economy (ECIPE), un think tank politico indipendente, ha pubblicato uno studio sull'impatto economico dei requisiti di localizzazione dei dati che discriminano i fornitori stranieri in sette giurisdizioni: Brasile, Cina, UE, India, Indonesia, Corea del Sud e Vietnam. [28] La loro ricerca ha concluso che le restrizioni unilaterali al flusso transfrontaliero di dati e all'accesso ai mercati esteri incidono negativamente sulla crescita economica e sulla ripresa poiché limitano l'accesso a prezzi competitivi, la crescita dell'occupazione in molti settori di servizi e produzione e le opportunità di investimento. Lo studio ha evidenziato che i requisiti di residenza dei dati non solo influiscono sul flusso dei dati, ma anche su un maggiore gruppo di opportunità di espansione commerciale che dipende dal flusso di dati tra frontiere.

Uno studio simile della Banca Mondiale ha analizzato 6 paesi in via di sviluppo e 28 stati membri dell'Unione Europea e ha scoperto che i requisiti sulla localizzazione dei dati possono ridurre il PIL fino all'1,7%, gli investimenti fino al 4,2% e le esportazioni fino all'1,7%.[29] Ciò influisce principalmente sulle piccole imprese e sulle start-up. Attraverso l'uso della tecnologia cloud, per esempio, i singoli individui e le piccole-medie imprese (PMI) possono accedere a risorse IT con costi e scalabilità un tempo accessibili solo a capitali più grandi. Le PMI sono il motore primario per la creazione di nuovi posti di lavoro. L'elaborazione in cloud abbassa le barriere per la creazione di imprese e l'accesso al mercato, consentendo la formazione di un maggior numero di start-up, creando in ultima analisi più posti di lavoro. Tuttavia, secondo la Commissione Europea, le aziende di tecnologia come un CSP devono affrontare costi significativi per adattarsi alle varie leggi nazionali che portano i costi della vendita online a superare i benefici. Recentemente, nel maggio 2017, l'Information Technology and Innovation Foundation, un istituto di ricerca indipendente, ha ottenuto gli stessi risultati.[30]

Una conclusione chiave coerente in tutti questi studi è che il divieto di flussi di dati transfrontalieri sotto forma di requisiti di residenza dei dati può avere un impatto sulla crescita economica locale e regionale e sulla competitività nel mercato globale, con il maggiore impatto a carico delle PMI. Un sistema sicuro nell'UE non è né più né meno sicuro di un sistema con un'architettura simile in America Latina. Non è sempre chiaro ai governi che la protezione dei dati generalmente non dipende dal luogo in cui sono conservate le informazioni, ma piuttosto dalle misure usate per proteggere quei dati. Generalmente i luoghi fisici non hanno importanza perché i data center sono quasi sempre connessi a reti ad alta accessibilità e quindi la sicurezza reale dipende dalle pratiche e dai processi tecnici, operativi e gestionali

implementati dal CSP e dal cliente.[31]

Costi di gestione di data center operanti esclusivamente in un paese

Uno studio del 2015 di una società di sicurezza cibernetica ha dimostrato come un modello di data center nazionale è molto più costoso rispetto all'utilizzo di CSP globali. Lo studio ha dimostrato che il costo dei servizi cloud può aumentare sostanzialmente a causa della localizzazione dei dati in base alla disponibilità di servizi alternativi. Lo studio ha dimostrato che:

Se il Brasile avesse approvato la localizzazione dei dati nel suo "Internet Bill of Rights" nel 2014, le società avrebbero dovuto pagare in media il 54% in più per usare i servizi cloud (di tutte le categorie) di fornitori di cloud locali rispetto al prezzo più basso mondiale.

Se l'Unione Europea avesse adottato la localizzazione dei dati, le aziende avrebbero comunque dovuto pagare fino al 36% in più per utilizzare servizi simili forniti da CSP hyperscale. Nel periodo dello studio, alcuni dei data center più economici si trovavano nell'Unione Europea.[32]

Impatto nel Settore pubblico

I paesi che applicano barriere ai flussi di dati possono limitare la capacità dei propri cittadini di usufruire di servizi innovativi che migliorano la qualità della vita e la fornitura di servizi pubblici. Per esempio, le applicazioni che sfruttano l'intelligenza artificiale e il machine learning (AI/ML) richiedono infrastrutture personalizzate per un funzionamento ottimale[33] e anche se i CSP globali continuano a espandere l'impronta dei propri data center, non è realistico pensare che tali data center saranno presenti in ogni paese. Quindi, mentre tecnologie di AI/ML sono usate sempre di più per migliorare servizi come prognosi sanitarie e previsioni del tempo per la gestione delle emergenze, i cittadini in paesi con stringenti requisiti di residenza dei dati rimarranno indietro nell'accesso a tecnologie all'avanguardia per servizi ai cittadini.

Limitare il flusso di dati ha anche conseguenze socio-economiche, in particolare sulla competitività commerciale e lo sviluppo della forza lavoro. Mentre la tecnologia cloud è sempre più presente e legata all'avanzamento economico, il commercio digitale (e la conseguente riduzione delle barriere ad esso legate) diventerà una priorità sempre più grande per i governi. I paesi che consentono il libero flusso di dati saranno avvantaggiati dall'accesso a tecnologie all'avanguardia, che a loro volta influenzeranno la modernizzazione dei servizi del settore pubblico e commerciale, miglioreranno la produttività dei lavoratori e accelereranno la crescita locale di posti di lavoro e di competenze in tutti i settori. I paesi che vogliono porre barriere al flusso di dati e al commercio digitale con il tempo avranno uno svantaggio competitivo.

Per esempio, tutti i benefici associati all'IoT per permettere l'agricoltura, l'industria manifatturiera o le città "intelligenti" non possono essere raggiunti con politiche restrittive che pongono dei limiti alle analisi di big data, al machine learning o ad altre caratteristiche che un flusso di dati libero ma sicuro garantisce.

> La domanda di competenze di cloud computing continua ad essere elevata in aree chiave come la sicurezza delle applicazioni, lo sviluppo di applicazioni aziendali nel cloud, la migrazione del cloud aziendale e i big data. L'U.S. Bureau of Labor Statistics indica che la domanda futura per lavori nella sicurezza cibernetica crescerà a un tasso del 37% tra il 2012 e il 2022. Per soddisfare la domanda di posti di lavoro, i governi dovranno investire in opportunità di istruzione e formazione per permettere agli individui di sviluppare le adeguate abilità tecnologiche.

Limitare l'accesso al genere di servizi IT sofisticati forniti da CSP hyperscale porterà anche a un continuo ritardo nello sviluppo e nel mantenimento di una forza lavoro tecnologica e altamente qualificata. Questo perché l'attitudine della forza lavoro è correlata alla complessità tecnologica di un'organizzazione, che a sua volta si basa sulla capacità dell'organizzazione di accedere a tecnologie all'avanguardia. Un uso efficace della tecnologia moderna richiede una forza lavoro con abilità commisurate alla tecnologia che utilizza. Per l'ampiezza e il ritmo dell'innovazione con i servizi cloud, c'è un noto e crescente divario di competenze. I governi, in particolare, sono rimasti indietro nella corsa agli esperti, essenziali per modernizzare le applicazioni e allo stesso tempo per proteggere le informazioni e i sistemi del settore pubblico da avversari e minacce altamente complesse che aumentano in frequenza e impatto.

Considerazioni nella creazione di politiche riguardo la residenza dei dati

Come discusso in precedenza, la sovranità normativa degli stati nazionali sui dati può ancora essere ottenuta sfruttando i vantaggi in termini di costi e di sicurezza di CSP hyperscale come AWS. Le misure di sicurezza distribuite attraverso i servizi AWS e verificate attraverso audit di terze parti offrono un alto livello di garanzia per evitare e affrontare situazioni di rischio di accesi illeciti ai dati.

Incoraggiamo i governi a considerare le seguenti politiche per rispettare gli obiettivi di sicurezza associati con la residenza dei dati.

1. Sviluppare politiche e requisiti che permettano di usare strutture di trattamento dati fuori dal paese se i dati sono trattati e conservati in ambienti cloud hyperscale moderni e altamente sicuri. I clienti possono anche scegliere paesi che dispongono di leggi sulla protezione dei dati coerenti con le proprie e dove

sono già in vigore accordi per il trasferimento dei dati.

2. Allineare le politiche nazionali e i requisiti istituzionali con il principio di libero movimento dei dati transfrontalieri per trovare un efficace bilanciamento tra sicurezza, economia e obiettivi di modernizzazione IT.

3. Valutare i modelli di trasferimento dei dati, come l'Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules system (CBPR) e le clausole contrattuali standardizzate, come le clausole modello dell'UE, approvate dalle autorità di protezione dei dati dell'UE e che possono essere utilizzate negli accordi tra i fornitori di servizi e i loro clienti per garantire che tutti i dati personali che lasciano lo Spazio Economico Europeo siano trasferiti in conformità con il regolamento generale sulla protezione dei dati (GDPR).[34] Questi tipi di accordi per il trasferimento dei dati forniscono garanzie sul fatto che i CSP stanno salvaguardando i dati personali in modo responsabile, nonché un mezzo pre-approvato per proteggere e supportare il flusso internazionale dei dati in modo sicuro e conforme.

Il regolamento generale dell'UE sulla protezione dei dati, entrato in vigore nel maggio 2018, mira ad armonizzare le leggi sulla protezione dei dati in tutta l'Unione Europea (UE) applicando un'unica legge sulla protezione dei dati che è vincolante in tutti gli Stati membri. Il GDPR non richiede leggi sulla residenza dei dati all'interno dell'UE, ma sostiene piuttosto quadri giuridici sotto forma di modelli di trasferimento dei dati e di clausole contrattuali standardizzate (cioè le clausole modello dell'UE) per incoraggiare i flussi di dati transregionali.

L'articolo 45 del GDPR stabilisce il principio secondo cui i trasferimenti di dati personali a un paese terzo o a un'organizzazione internazionale possono avvenire se il paese terzo, il territorio, uno o più settori specifici all'interno di tale paese o l'organizzazione internazionale in questione garantisce un livello di protezione adeguato. Per ottenere questo, i governi possono:

- Cambiare le loro leggi esistenti sulla protezione dei dati e iniziare discussioni con altri paesi sull'adeguatezza. Ad esempio, la Nuova Zelanda sta per ottenere una decisione di adeguatezza da parte della Commissione UE.
- Stabilire quadri bilaterali come le Regole sulla privacy transfrontaliera dell'APEC.

4. Assicurare che i CSP e i fornitori di terze parti dimostrino robusti controlli di sicurezza per poter affrontare accessi non autorizzati di terze parti a dati, sistemi e asset attraverso certificazioni di terze parti riconosciute a livello internazionale (ad esempio, ISO 27001, ISO 27018, SOC, PCI DSS, ecc).
5. Classificare i dati e definire i ruoli e le responsabilità di trattamento dei dati per determinare gli obblighi di protezione dei dati appropriati per ciascuna parte. I governi devono selezionare modelli appropriati di distribuzione cloud in base alle proprie necessità, al tipo di dati che gestiscono e al profilo di rischio. Per l'insieme più ristretto di dati classificati al più alto livello di sensibilità, i governi possono trovare più adatte le opzioni ibride. I governi devono inoltre considerare l'uso di ISO 27018 per definire i ruoli di titolare e responsabile del trattamento dei dati. I governi possono lavorare con i CSP per comprendere e applicare adeguatamente le responsabilità di protezione dei dati per il titolare e il responsabile del trattamento dei dati, per ciascuno dei modelli di servizio.
6. Garantire ai clienti la comprensione e l'implementazione di servizi di sicurezza per la cifratura dei dati. AWS è pioniere nei servizi di cifratura che forniscono ai clienti la possibilità di controllare completamente le chiavi di cifratura. AWS offre ai clienti la possibilità di cifrare i dati utilizzando le proprie chiavi che possono essere memorizzate al di fuori di AWS o in modo sicuro all'interno dei servizi, consentendo loro di controllare le chiavi e di accedere ai dati, il tutto nel rispetto dei rigorosi obblighi di sicurezza e di conformità.
7. Impegnarsi in sforzi bilaterali e multilaterali per aggiornare il processo MLAT in modo da bilanciare le esigenze dei governi per ottenere rapidamente le prove necessarie nelle indagini e nei procedimenti giudiziari con il diritto alla privacy dei singoli individui sui contenuti elettronici di loro proprietà. Sosteniamo l'aggiornamento della legislazione in merito alla privacy e all'accesso da parte delle forze dell'ordine nel contesto della comunicazione elettronica, sia a livello nazionale che internazionale. Incoraggiamo inoltre i governi a rivedere e aggiornare le loro leggi nazionali per affrontare i ruoli, le responsabilità e i meccanismi che disciplinano l'accesso legale ai dati in linea con i principi del processo MLAT.

Conclusioni

Sebbene i governi possano percepire un senso di maggiore sicurezza imponendo requisiti di residenza dei dati per i dati elaborati e conservati in strutture IT locali perché offrono vicinanza e controllo fisico, una valutazione più approfondita mostra che limitare i servizi IT alla sola giurisdizione locale non garantisce una migliore sicurezza generale dei dati. Dal punto di vista del rapporto rischio-beneficio, i CSP hyperscale, come AWS, possono aiutare a gestire meglio i rischi di sicurezza informatica, riducendo al minimo il rischio di accesso ai dati da parte di governi stranieri. I governi devono inoltre considerare gli importanti compromessi associati con i requisiti di residenza dei dati. Non solo i governi che utilizzano requisiti restrittivi per la residenza dei dati perderanno l'accesso ad alcuni degli ambienti informatici più sicuri del mondo, ma, al di là della sicurezza, saranno costretti ad affrontare un continuo ritardo nell'accesso alla tecnologia all'avanguardia ed economica necessaria per la propria trasformazione digitale.

Incoraggiamo i governi a rivalutare gli obiettivi di sicurezza che effettivamente raggiungono attraverso le restrizioni sulla localizzazione dei dati in relazione ai significativi costi in termini economici, di modernizzazione IT e di opportunità di sicurezza. Le capacità di sicurezza dei CSP hyperscale non solo affrontano le preoccupazioni più importanti, ma forniscono un livello di sicurezza superiore di quello dei tradizionali servizi in locale o delle strutture appaltate a livello locale. Le soluzioni politiche, come gli accordi per il trasferimento dei dati e l'utilizzo di certificazioni di sicurezza internazionali ben note, possono servire come mezzi sufficienti per raggiungere gli obiettivi di residenza dei dati, promuovendo al contempo gli obiettivi di trasformazione digitale del settore pubblico.

Revisioni del documento

Data	Descrizione
Agosto 2020	Aggiornamenti minori di testo per una maggiore accuratezza
Novembre 2019	Prima pubblicazione

Note

1 http://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

2 Pete Lindstrom, “Assessing the Risk: Yes, the Cloud Can Be More Secure Than Your On-Premises Environment,” International Data Corporation (July 2015).

3 Mutual Legal Assistance Treaties (MLATs) generally allow for the exchange of evidence and information in criminal and related matters. https://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm

4 Le rogatorie sono richieste dei tribunali di un paese ai tribunali di un altro paese che richiedono l'esecuzione di un’azione che, se compiuta senza l’autorizzazione del tribunale straniero, potrebbe costituire una violazione della sovranità di quel paese. Le rogatorie possono essere utilizzate per la notifica di un processo o per ottenere prove, se tale atto è consentito dalle leggi del paese straniero. https://travel.state.gov/ content/ travel/en/legal/travel-legal-considerations/internl- judicial-asst/obtaining-evidence/Preparation-Letters-Rogatory.html

5. Il CLOUD Act è applicato negli Stati Uniti e in società estere che operano negli Stati Uniti e che offrono “servizi di comunicazioni elettroniche”, come le aziende che offrono servizi di posta elettronica, messaggistica elettronica o servizi di cloud storage al pubblico.

6 http://d1.awsstatic.com/certifications/Amazon_LawEnforcement_Guidelines.pdf

7. AWS consente ai clienti di utilizzare i propri meccanismi di crittografia per quasi tutti i servizi AWS, inclusi Amazon S3, Amazon EBS, Amazon DynamoDB e Amazon EC2. I tunnel da IPSec a VPC sono anch'essi crittografati. Amazon S3 offre inoltre, come opzione per i clienti, la crittografia lato server. I clienti possono utilizzare anche tecnologie di crittografia di terze parti.

8 Il servizio AWS CloudHSM (Hardware Security Module) consente di proteggere le chiavi crittografiche all'interno di HSM progettati e convalidati secondo gli standard governativi (FIPS 140-2 Livello 3) per la gestione sicura delle chiavi (inclusa una robusta protezione anti-manomissione). AWS KMS, che rispetta lo standard FIPS 140-2 Livello 2, offre un servizio simile, ma più scalabile e integrato più in profondità in numerosi servizi AWS in modo che le protezioni siano fornite automaticamente in base a semplici modifiche della configurazione del servizio. Attraverso uno qualsiasi di questi servizi, è possibile generare, archiviare e gestire in modo sicuro le chiavi crittografiche usate per la crittografia dei dati, in modo che siano accessibili solo all’utente. Per ulteriori informazioni https://aws.amazon.com/cloudhsm/ e https://aws.amazon.com/kms/.

9 Le opzioni di cifratura AWS sono dettagliate tramite i seguenti link: 1) Securing Data at Rest with Encryption, 2) Protecting Data Using Encryption in Amazon S3, 3)AWS Key Management Service Cryptographic Details, e 4) Overview of AWS Security Processes.

10 È disponibile una serie di ricerche sulle tecniche di decomposizione dei dati. Una di queste, esaminata per questo documento, è: Data protection by means of fragmentation in various different distributed storage systems - a survey, Kapusta and Memmi, June 20, 2017.

[11] La protezione in profondità è la pratica di implementare più livelli di controllo di sicurezza per fornire indipendenza e ridondanza. Se un livello di controllo fallisce, il livello successivo è disponibile per mitigare un'ulteriore incursione contro un asset.

[12] La difesa in ampiezza è l'approccio che consiste nell'utilizzare attività multidisciplinari per fornire numerosi meccanismi di protezione a ogni livello di difesa identificato. In generale, questo significa più automazione e controlli di sicurezza più variegati a ogni livello.

[13] https://aws.amazon.com/guardduty/

[14] https://aws.amazon.com/macie/

[15] https://aws.amazon.com/cloudhsm/

[16] La certificazione FIPS 140-2, sui requisiti di sicurezza per moduli di cifratura, copre 11 aree relative a progettazione e implementazione di un modulo di cifratura.

[17] https://d1.awsstatic.com/whitepapers/compliance/AWS_Logical_Separation_Handbook.pdf

[18] https://aws.amazon.com/compliance

[19] https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

[20] AWS Outposts porta servizi, infrastrutture e modelli operativi nativi di AWS in praticamente ogni data center, housing o strutture on-premise. Per ulteriori informazioni visitare https://aws.amazon.com/outposts/

[21] In altre parole, la progettazione polimorfica consente la creazione di bersagli mobili rendendo più difficile l'esito positivo degli attacchi da parte di agenti malevoli.

[22] Il concetto è stato in origine coniato da Forrester Research. Afferma che nessuna entità nella rete è affidabile. L'obiettivo è rafforzare gli accessi di sicurezza per tutte le risorse, sia interne che esterne. Ciò significa che un'organizzazione deve comprendere e classificare i propri dati e mappare il modo in cui questi dati, in particolare quelli sensibili, si spostano tra conservazione, trattamento, transito e cliente. Poi, una volta compresi i dati, un'organizzazione può implementare i meccanismi ZTM che applicano e automatizzano il minor privilegio possibile, la cifratura end-to-end e l'ispezione completa del traffico.

[23] ISO 27001/27002 è uno standard di sicurezza globale adottato su vasta scala che

stabilisce i requisiti e le best practice per un approccio sistematico alla gestione delle informazioni aziendali e dei clienti basato su valutazioni periodiche del rischio idonee a scenari di rischio in continua evoluzione.

[24] La norma ISO 27018 è un codice di condotta che si concentra sulla protezione dei dati personali nel cloud. È basata sullo standard ISO di sicurezza delle informazioni 27002 e fornisce linee guida per l'implementazione di controlli di sicurezza previsti dalla ISO 27002 applicabili alle informazioni che consentono l'identificazione personale degli utenti o PII (Personally Identifiable Information) in cloud pubblici. Fornisce inoltre un set di controlli e linee guida aggiuntivi tesi a soddisfare i requisiti di protezione delle PII in cloud pubblici non trattati dal set di controlli ISO

27002 esistente.

[25] Il Payment Card Industry Data Security Standard (noto anche come PCI DSS) è uno standard per la sicurezza delle informazioni gestito dal PCI Security Standards Council (https://www.pcisecuritystandards.org/), fondato da American Express, Discover Financial Services, JCB International, MasterCard Worldwide e Visa Inc.

Il PCI DSS si applica a tutte le entità che memorizzano, elaborano o trasmettono dati di titolari di carta (CHD) e/o dati sensibili di autenticazione (SAD), compresi esercenti, elaboratori, acquirer, emittenti e fornitori di servizi.

[26] I report di Service Organization Controls (SOC 26) hanno lo scopo di soddisfare una vasta gamma di requisiti di controllo finanziario per gli organismi di revisione statunitensi e internazionali. L'audit del presente rapporto è condotto in conformità agli International Standards for Assurance Engagements No. 3402 (ISAE 3402) e all'American Institute of Certified Public Accountants (AICPA): AT 801 (ex SSAE 16).

[27] http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows

[28] European Centre for International Political Economy (ECIPE): "The Costs of Data Localization: A Friendly Fire on Economic Recovery,"

http://www2.itif.org/2015-cross-border-data-flows.pdf?_ga=1.8208626.1580578791.1473954628.

[29] http://documents.worldbank.org/curated/en/961621467994698644/pdf/102724-WDR-WDR2016Overview-ENGLISH-WebResBox-394840B-OUO-9.pdf

[30] Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" Information Technology and Innovation Foundation (May 2017) http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.243762501.1722557619.1508762047- 1611916082.1508762047.

[31] Ibid p.4 Conclusioni simili sono state confermante indipendentemente da questo documento.

[32] http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.51021357.566718019.1510350061-1611916082.1508762047

[33.] Ad esempio, sistemi con capacità di GPU generici e Field Programmable Gate Array (FPGA).

[34] L'addendum per l'elaborazione dei dati del GDPR di AWS, che include le clausole modello dell'UE, fa ora parte dei nostri Termini di servizio online. Ciò significa che tutti i clienti AWS a livello globale possono fare affidamento sui termini del GDPR DPA di AWS ogni volta in cui utilizzano i servizi AWS per elaborare dati personali in base al GDPR. Per ulteriori informazioni sull'approccio di AWS sulla conformità con il GDPR è possibile consultare il sito: https://aws.amazon.com/ compliance/gdpr-center/.