The Perfect Storm o la Tempesta Perfetta è un evento dalla portata eccezionale, derivante alla concomitanza di diversi fattori che, se presi singolarmente, hanno un impatto significativo ma che se agiscono in modo combinato, possono dare luogo ad un effetto amplificato e dirompente. Nel campo della moderna *Information & Communication Technology* il primo elemento di questa tempesta è il Cloud Computing, a cui segue la Cybersecurity. Il terzo elemento è il fenomeno in atto da parte di alcuni governi relativo agli aspetti di Cyber Spionaggio. Se non opportunamente gestiti, questi tre elementi possono infatti delineare scenari critici, ma combinati in una strategia integrata possono, al contrario, produrre scenari d'innovazione dirompente.

di Carlo Mauceli

THE PERFECT STORM

***Carlo MAUCELI** è National Digital Officer della filiale italiana di Microsoft. con la responsabilità di promuovere l'innovazione del Paese, gestendo i rapporti con le government élites, i leader accademici e i decisori pubblici e contribuendo alla definizione di una politica tecnologica funzionale alla digitalizzazione del territorio.*

1. Introduzione

Nel campo dell'Information&Communication Technology stiamo assistendo oggi ad un fenomeno nuovo che potrebbe essere paragonato alla **Tempesta Perfetta.**

Sappiamo tutti che la Tempesta Perfetta è un evento dalla portata eccezionale, derivante alla concomitanza di diversi fattori che, se presi singolarmente, hanno un impatto significativo ma che se agiscono in modo combinato, possono dare luogo ad un effetto amplificato e dirompente. È utile analizzare ogni singolo elemento ai fini della comprensione del fenomeno nel suo complesso e della risposta di Microsoft a tale scenario: il Trusted Cloud.

2. Cloud Computing

Il Cloud Computing è, senza dubbio, uno dei più importanti, rivoluzionari e dirompenti trend tecnologici del momento.

Le motivazioni principali per cui molte organizzazioni stanno abbracciando l'idea dell'adozione di modelli cloud sono principalmente tre: **sostanziale riduzione dei costi**, **aumento delle performance** e **maggiore scalabilità**. Di questi tre elementi, indubbiamente, il fattore economico rappresenta il driver principale per garantire una trasformazione radicale e, come sempre è avvenuto in passato, sarà l'artefice di una nuova rivoluzione industriale.

Va considerato, però, che ci sono ancora molte discussioni sui fattori che ne ostacolano l'adozione e, perché no, anche alcune complessità tecniche. Quindi, se da un lato dobbiamo riconoscere che tali preoccupazioni esistono e sono importanti, il fatto di sottolineare gli aspetti economici ha sicuramente un impatto molto forte sulla possibilità di velocizzare l'adozione del cloud stesso.

Sono tre le aree principali attraverso le quali l'utilizzo del Cloud Computing può garantire alle infrastrutture IT di muoversi all'interno dei grandi Datacenter permettendo, così, significativi vantaggi da un punto di vista economico:

- **Risparmi sul fronte dell'offerta**. I Datacenter di grandi dimensioni riducono i costi per singolo server;
- **Aggregazione della domanda**. Aggregare il più possibile la "demand generation per server" permette un aumento della media di utilizzo per singolo server, diminuendo gli sprechi e una variabilità di utilizzo che penalizza l'efficienza;
- **Efficienza multi-tenancy**. Quando ci si orienta verso una soluzione che prevede un modello multi tenant, all'aumentare del numero degli utenti diminuisce il costo di gestione e del server stesso per utente.

Il Cloud Computing offre notevoli opportunità sia nel campo dell'innovazione che in quello dell'imprenditorialità perché garantisce a chiunque, con bassi investimenti, di potere accedere ad una grande quantità di servizi oltre che a potere avviare attività in maniera rapida.

Senza ombra di dubbio, il Cloud Computing è il primo elemento della nostra Tempesta Perfetta.

3. Cybersecurity

La Cybersecurity rappresenta il secondo elemento da tenere in considerazione. Certamente, non si tratta di una sorpresa, anche se in Italia non è da molto tempo che le organizzazioni pubbliche e private hanno posto l'attenzione su un fenomeno che rappresenta, ormai, un vero e proprio business.

In ogni caso, qualcosa ha cominciato a muoversi e molte domande vengono sollevate a riguardo: siamo di fronte ad un nuovo trend? Ci stiamo misurando con un nuovo scenario se lo confrontiamo con quello di qualche anno fa?

La risposta non può che essere affermativa e le ragioni possono essere sintetizzate nei seguenti cinque punti:

1. **Gli attacchi provengono da ogni dove**. Non è più il tempo in cui gli attacchi avevano una specifica motivazione politica o ideologica, per esempio, Oggi una minaccia può arrivare anche dall'interno o da molto vicino.

2. **Gli attacchi sono rivolti a tutti, senza distinzione di luogo, persone o strumenti**. Qualche anno fa la tendenza era, preferibilmente, quella di attaccare le banche, le realtà finanziarie o similari. Oggi, queste minacce non sono scomparse ma, piuttosto, si sono allargate verso il furto di identità, dell'intellectual property delle aziende pubbliche e private.
3. **Gli attacchi, a volte, sono diretti ad aziende specifiche o ad obiettivi specifici**. Stiamo parlando di un fenomeno noto con il nome di **Advanced Persistent Threat** (APT).
4. **Non è più il tempo dei cosiddetti "Script Kiddies"**, meccanismi che appiattivano le reti. Siamo di fronte ad un vero e proprio mercato, generato dalla capacità di sviluppare minacce facendo leva sulle vulnerabilità presenti nei vari sistemi e nei software. Minacce costruite da team di professionisti che fanno del cybercrime un vero e proprio business.
5. **La tecnologia è vulnerabile**. Non esiste nulla che sia sicuro al 100%. Pertanto, non diamo credito a chi afferma il contrario raccontando storie sulla non vulnerabilità dei prodotti e delle soluzioni. L'unica cosa di cui possiamo parlare è la **gestione del rischio**.

È fondamentale, quindi, che ***la sicurezza non venga considerata un costo ma, piuttosto, una necessità e che si parli di sicurezza nella più ampia accezione del termine*** oltre al fatto che ogni azienda debba porsi le seguenti domande:

- Qual è il criterio attraverso il quale sviluppiamo applicazioni sicure?
- Quanto sono flessibili i processi interni per potere rispondere ad incidenti legati alla sicurezza?
- Abbiamo processi e sistemi che garantiscono il testing e l'aggiornamento delle piattaforme?
- Abbiamo processi e tecnologie di sicurezza certificati secondo i criteri ISO?

Ed è a queste domande che ogni ente deve essere in grado di rispondere quando si parla di sicurezza.

4. Cloud Security

Le domande precedenti, comunque, non rappresentano l'unico argomento di discussione quando si parla di Cloud Computing. **Uno dei punti fondamentali riguarda la questione della cosiddetta "Global Trust" ossia la fiducia che una azienda ripone nel proprio provider di servizi.**

E da questo punto di vista diventano fondamentali le risposte che un provider di servizi cloud è in grado di offrire relativamente ai seguenti tre aspetti:

- **Data Privacy**, Quanto l'utilizzo del tuo servizio impatta sulle mie responsabilità di CIO? In maniera più specifica, come mi puoi aiutare perché io risponda in modo corretto ai requisiti che regolano il mantenimento, il controllo e l'accesso dei dati?
- **Security**. In che modo mi aiuti affinché possa garantire la sicurezza dei miei dati sia quando si trovano sui tuoi sistemi che quando sono in transito?
- **Trasparency**. Come mi puoi aiutare dal punto di vista della compliance? Dove sono memorizzati i miei dati? Dove sono processati i dati? Che garanzie mi dai sulla disponibilità del servizio?

È fondamentale ricordare che, in ogni caso, l'adozione del cloud non elimina le responsabilità del CIO e degli altri membri del board esecutivo di un'azienda. L'adozione del cloud significa delegare le attività che riguardano la gestione, l'archiviazione e il mantenimento dei dati ma non elimina le responsabilità che riguardano, appunto, il CIO e le figure del board esecutivo. A questo riguardo bisogna sempre ricordare che:

- **Titolare del trattamento** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualunque altro ente, associazione e organismo cui competono le decisioni in ordine alle finalità, alle modalità di trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
- **Responsabile del trattamento**: è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

A questo punto è utile condividere un elemento che sta sempre più diventando un trend e che riflette la maturità delle discussioni in ambito cloud. C'è una concezione sbagliata secondo la quale le soluzioni cloud talvolta creano discussioni che diventano quasi delle sfide insostenibili relativamente ai temi sulla privacy e la sicurezza. È fondamentale sfatare questo mito. ***Il cloud fornisce un'opportunità alle organizzazioni per migliorare la privacy e la sicurezza dei dati mantenendo la compliance alle leggi***.

È sorprendente come gli argomenti relativi alla sicurezza in ambito cloud vengano utilizzati come estremi opposti della stessa discussione. Ossia, l'argomento della sicurezza viene utilizzato per evitare l'utilizzo del cloud ma, allo stesso tempo, diventa l'elemento principale per scegliere di abbracciare l'utilizzo del cloud. Perché? La ragione è semplice ed è legata al fatto che le aziende usano criteri di valutazione che, dato l'elevato livello di minacce con cui si devono confrontare quando espongono i dati nel cyberspace, le portano a pensare che non avranno mai il livello di conoscenza adeguato e necessario oltre che la capacità di difendere in maniera corretta quei dati. E in una pura logica di risk assessment si pensa che, probabilmente, i dati sono molto più sicuri e protetti nel cloud se fornito da importanti service provider che hanno maggiori skill e migliori forme di protezione di quanto ne possano avere loro.

5. Compliance

È possibile spostarsi sul cloud e continuare ad essere aderente alle regole e le leggi presenti e a cui come azienda si deve rispondere? La risposta è: dipende. Dipende da cosa?

Bisogna essere chiari. Tutto ciò dipende dal service provider e, soprattutto, dal modello di business del service provider. Nel caso di Microsoft, i servizi cloud vengono offerti sia per il mondo consumer (Outlook, Onedrive, Office Web Apps) che nel mondo enterprise (Office 365, Microsoft Azure, Dynamics CRM Online, Windows Intune).

Le infrastrutture sono fisicamente separate e non hanno le stesse caratteristiche in termini di compliance e livello di servizio, questo perché il mondo enterprise necessità di garanzie diverse.

Infine, il modello operativo che abbiamo realizzato nei nostri datacenter, certificato ISO 27001, la risposta pubblica alle iniziative sulla trasparenza come la "STAR Registry" dal Cloud Security Alliance, la nostra capacità di incorporare nei nostri contratti le "EU Model Clauses" per coprire il trasferimento dei dati a livello internazionale, lo specifico "Data processing Agreement" che va, addirittura, oltre le EU Model Clauses, sono solo alcune delle misure che aiutano e sostengono il passaggio al cloud da parte delle organizzazioni. E non è una sorpresa il recente riconoscimento ricevuto dai garanti della privacy della EU (Art. 29 Working Group) relativo all'accuratezza dei nostri contratti in tema di rispondenza agli elevatissimi livelli richiesti dalla EU.

6. Governance Survilliance

Il terzo elemento della nostra Tempesta Perfetta è il fenomeno in atto da parte di alcuni governi relativo agli aspetti di Cyber Spionaggio. Sono tre le strategie con cui Microsoft affronta questa problematica:

- **Espansione dei meccanismi di crittografia a tutti i nostri servizi**. Ciò che Microsoft vuole è che nessuno, al di fuori dei nostri datacenter, acceda ai dati in maniera non conforme alle leggi esistenti;
- **Rafforzamento delle protezioni di carattere legale per i dati dei clienti**;
- **Continuo miglioramento della trasparenza**.

È giusto però essere chiari su un punto: Microsoft non fornisce ad alcun governo l'accesso diretto alle mail o agli "*instant messages*", né le soluzioni tecniche per potere accedere ai dati degli utenti in maniera diretta. Al contrario, qualunque governo deve affidarsi alle procedure legali per potere richiedere a Microsoft informazioni specifiche riguardo ai dati dei clienti.
In ogni caso, relativamente alla richiesta dei governi di accedere ai dati in modo non conforme alla legge, Microsoft ritiene che le attuali leggi in termini di trasparenza abbiano bisogno di essere riviste ed in questo senso molte società, insieme a Microsoft, quali Facebook, Google, Apple, Yahoo, Twitter, AoL, Linkedin si sono accordate per creare una sorta di "**Public Class**" al fine di chiedere una "**Global Governance Surveillance Realm**" (https://www.reformgovernmentsurveillance.com/) riguardo la consistenza delle norme che stabiliscono la trasparenza, la libertà di espressione e la privacy, con l'obiettivo di assicurare che l'applicazione della legge governativa e gli sforzi dell'intelligence vengano regolamentati in maniera chiara.

Microsoft chiede a tutti i governi di appoggiare i seguenti principi e ad attuare riforme che trasformino questi principi nelle seguenti azioni:

1. Limitare l'autorità del governo a collezionare le informazioni relative agli utenti;
2. Supervisione e responsabilità;
3. Trasparenza relativamente alle richieste dei governi di accedere ai dati;
4. Rispetto della libertà dei flussi delle informazioni;
5. Evitare conflitti tra i governi.

Tutto ciò è un ottimo approccio industriale nella speranza, però, che i governi considerino questa richiesta in maniera seria. In ogni caso, parallelamente, come Microsoft stiamo facendo un enorme sforzo di tipo "Crypto" relativamente ai nostri servizi online. Infatti, stiamo lavorando per proteggere i dati in qualsiasi tipo di comunicazione, il che significa:

- **Proteggere i dati in transito tra l'utente ed il servizio;**
- **Proteggere i dati in transito tra i vari Datacenter;**
- **Proteggere i dati anche "a riposo";**
- **Crittografare i dati in modalità end to end a livello di comunicazione**.

Ci teniamo anche ad aggiungere un'ultima osservazione tratta dallo European Cloud Partnership Steering Board riguardo il *Trusted Cloud Europe* sulla "riduzione delle restrizioni sulla localizzazione dei dati". Le norme degli Stati Membri e, in alcuni casi, le leggi nazionali restringono la possibilità di archiviare e di gestire alcune tipologie di dati (specialmente i dati del settore pubblico) al di fuori del territorio. Se si potessero trovare dei requisiti comuni per casi simili, gli Stati Membri potrebbero scegliere di eliminare gradualmente le restrizioni sulla localizzazione dei dati quando ciò non sia ritenuto strettamente necessario. Ciò non implica che i controlli sui dati non debbano più esserci; spesso è possibile e consigliabile rimpiazzare requisiti formalmente legali (come la localizzazione geografica dei dati) con requisiti funzionali corrispondenti (come assicurare l'accesso e la sicurezza dei dati). Allo stato dell'arte, le tecnologie di sicurezza potrebbero essere considerate per alcuni casi specifici come un'alternativa alle restrizioni sulla localizzazione dei dati. Questo approccio è tecnologicamente neutrale per supportare l'innovazione e le nuove tecnologie e fare sì che gli obiettivi di policy, trasparenza e sicurezza vengano raggiunti in maniera sempre più efficace.

7. Conclusione

Nell'attuale scenario moderno, in cui nuove minacce e rischi minano diffusamente la sicurezza, i tre elementi prima descritti possono delineare scenari critici se non opportunamente gestiti.
L'obiettivo deve rimanere, tuttavia, quello di aiutare un sempre maggior numero di aziende pubbliche e private a cogliere le opportunità del Cloud Computing, contribuendo al percorso di crescita dell'intero Paese. I tre elementi, quindi, devono essere combinati in una strategia integrata e così possono, al contrario, produrre scenari d'innovazione dirompente.

Un "Trusted Cloud", cioè un cloud che risponde a tutti i requisiti di sicurezza, privacy e trasparenza, rappresenta la sola risposta alla Tempesta Perfetta e facilita il passaggio al cloud da parte delle organizzazioni, consentendolo loro di dare vita a progetti IT complessi senza preoccupazioni.

Con il "Trusted Cloud" Microsoft intende rivoluzionare la realtà italiana. ©