Come approcciare Business Continuity e Cyber Security sinergicamente

Parte I – Introduzione

Al giorno d'oggi, in un mondo sempre più digitalizzato e in continua evoluzione, un grande pericolo cui tutte le aziende devono far fronte, è rappresentato senza dubbio dagli attacchi informatici verso i propri asset informativi aziendali. È inevitabile quindi il ricorso a strumenti necessari per mitigare, quando non prevenire, il verificarsi di tali attacchi che, se condotti con successo, potrebbero comportare la compromissione dell'integrità, della disponibilità e dalla riservatezza di importanti informazioni aziendali.

Oltre a questa importante sfida, un'azienda deve sicuramente garantire a sé stessa e ai suoi clienti la continuità operativa dei servizi erogati, in qualsiasi situazione. A tal fine, ed anche per compliance normativa, molte aziende si sono dotate da anni di specifiche strategie a garanzia della continuità del business. In molti casi questo piano si è evoluto in un vero piano di *Business Continuity* capace di garantire la continuità operativa anche durante il verificarsi di molteplici situazioni avverse quali eventi naturali, guasti agli impianti, guasti e danni intenzionali, ecc.

Risulta quindi naturale integrare gli scenari di incidenti tipici della sicurezza informatica e più in generale gli scenari di gestione degli attacchi cyber, nel sistema di gestione della *Business Continuity*. Nei paragrafi seguenti viene mostrato come questa integrazione possa aumentare considerevolmente la resilienza complessiva dell'azienda.

Per *Business Continuity (BC)* si intende la capacità di mantenere funzionanti i propri processi di business, i

servizi, le tecnologie ed anche il personale nonostante il manifestarsi di situazioni avverse, pur ammettendo performance differenti rispetto la normale operatività. La BC può, in alcune circostanze, essere intesa anche in ottica ISO 22301 e quindi fare riferimento ad un sistema di gestione per la Continuità operativa. La gestione della continuità operativa, è dunque un processo che ha l'obiettivo di:

- assicurare la "sopravvivenza" di tutte le funzioni essenziali dell'organizzazione;
- identificare gli eventi e gli incidenti di sicurezza potenzialmente in grado di compromettere la continuità del business aziendale;
- organizzare una struttura in grado di reagire tempestivamente in seguito al verificarsi di interruzioni o compromissioni dei processi di business;
- ridurre i rischi correlati alla continuità operativa aziendale, gestendone le conseguenze sul piano gestionale, amministrativo e legale.

Le tre componenti fondamentali di un così detto processo di gestione della Continuità Operativa **BCM** (Business Continuity Management) sono:

- la valutazione degli impatti sul business – **BIA (Business Impact Analysis)** ovvero la mappatura dei processi aziendali, al fine di identificarne criticità e impatto sul business, la tempistica di ripristino (RTO) oltre che le risorse necessarie affinché il processo possa essere ripristinato ai livelli di normale funzionamento;
- il piano di continuità operativa – **BCP (Business Continuity Plan)** ovvero il complesso di procedure formalizzate che guidano le organizzazioni nel rispondere, recuperare, riprendere e ripristinare a un livello predefinito almeno le funzioni organizzative critiche, a seguito di un'interruzione.
- il piano di recupero da situazioni di disastro – **DRP**

(Disaster Recovery Plan), ovvero il processo documentato per recuperare una infrastruttura IT in caso di disastro. Un disastro può verificarsi per cause naturali (come ad esempio una tormenta di neve, una tempesta o un'inondazione) o per danni provocati dall'uomo (come ad esempio atti di terrorismo o attacchi hacker).

La **BIA**, il **DRP** e il **BCP** devono necessariamente tenere conto uno gli uni degli altri al fine di essere integrati correttamente oltre che dei tipici scenari di incidenti di sicurezza

Il NIST definisce la Cybersecurity come:

"The ability to protect or defend the use of cyberspace from cyber attacks". Lo stesso NIST definisce il *Cybespace* come *"A global domain within the information environment consisting of the interdependent network of information systems infrastructuresincluding the Internet, telecommunications networks, computer systems, and embedded processors and controllers*".

La *Cybersecurity* rappresenta la seconda emergenza in Europa, dopo il cambiamento climatico e prima dell'immigrazione: il Presidente della Commissione Europea, Jean-Claude Junker, lo ha sostenuto nel discorso sullo stato dell'Unione del 13 settembre 2017. Da diversi anni i governi di tutto il mondo riservano alla *Cybersecurity* ampio spazio nelle loro agende. Il blocco dell'operatività di aziende, il controllo surrettizio di servizi di infrastrutture critiche, il furto della proprietà intellettuale o di informazioni cruciali per la sopravvivenza di un'azienda sono esempi delle maggiori minacce che un paese deve affrontare.

Nonostante gli attacchi cyber abbiano raggiunto la loro notorietà soprattutto in considerazione della violazione della riservatezza dei dati personali fino a centinaia di milioni di persone è da ricordare anche la capacità distruttiva di questi

attacchi informatici, anche nei confronti della continuità operativa dei sistemi informatici e quindi dell'azienda stessa.

Un caso reale, che ha avuto una grande risonanza mediatica nel giungo 2017 e che può essere considerato un utile caso di studio, è sicuramente quello del gigante danese della logistica Maersk. La società danese, presa di mira da un attacco NotPetya (noto alle cronache *ransomware)*, ha visto messi offline i propri sistemi informatici comportando perdite comprese fra 200 e 300 milioni di dollari, dovuti dalla forzata e significativa interruzione dell'attività.

Le conseguenze dell'incidente per Maersk sarebbero state molto più contenute in presenza di un piano di *Business Continuity* che considerasse l'indisponibilità totale dei propri sistemi informativi per un limitato lasso di tempo.

In situazioni analoghe si ritrovano manager IT in continua difficoltà nella gestione dei *cybersecurity risk* e nella difesa delle proprie aziende da attacchi di vario tipo. Il volume e la complessità degli attacchi è nel tempo cresciuta, ed in seguito ad una violazione di sicurezza le organizzazioni possono registrare considerevoli perdite economiche per via dei costi di ripristino della normale operatività a seguito di un attacco informatico che, non in ultima analisi, spesso comporta anche danni alla reputazione dell'azienda stessa.

Per indirizzare proattivamente le minacce per la cybersecurity, le aziende monitorano continuamente i potenziali *cyber risk* e sviluppano di conseguenza strategie di risposta. E' qui che nasce quasi spontaneamente la necessità di integrare queste risposte strategiche con il piano di continuità operativo dell'azienda, in modo che in caso di eventi avversi l'azienda possa rispondere tempestivamente con un piano d'azione ben coordinato.

Disporre di un BCP può semplificare la vita alle

organizzazioni anche nell'adempiere a requisiti cogenti come ad esempio quelli indicati dal nuovo Regolamento Europeo sulla privacy (GDPR).

Un esempio è certamente la notifica delle violazioni di sicurezza (Art. 33) che le organizzazioni, a breve, dovranno fare all'autorità di controllo entro 72 ore dal momento in cui si viene a conoscenza della violazione di sicurezza sui propri sistemi informativi, pena l'applicazione di sanzioni amministrative e interdittive. Uno scenario di rischio di questo tipo sarebbe sicuramente emerso nel corso di un progetto di BCM, in particolare nelle fasi BIA e Risk Assessment, e quindi opportunamente considerato nella stesura del BCP e nelle procedure di Incident Management.

Uno studio condotto nel 2016 dal Ponemon Institute sul costo di un *data breach*[1], evidenzia come le organizzazioni che legano la *cybersecurity* con il *Business Continuity Management*, hanno ridotto significativamente il tempo medio per affrontare una violazione dei dati, nonché la probabilità di subire nuovamente un incidente analogo nel futuro.

Sempre questo studio riporta come un BCP ben definito contribuisca a ridurre i costi di una violazione dei dati, in media di $9 per record, mantenendo attive e operative le attività aziendali. Oltre alle tradizionali misure correttive attuate in risposta a incidenti di sicurezza, vi è una sempre maggiore necessità di attenzione verso una risposta strategica, snella e rapida. Una risposta a questa sempre più pressante richiesta di attenzione da parte del management aziendale può arrivare muovendosi su due piani differenti: da un lato abbiamo un piano prettamente strategico; dall'altro abbiamo un piano tattico. Le caratteristiche salienti di questi due diversi approcci possono essere sintetizzate in:

- **piano strategico:**
  - coinvolgere il top management nella gestione della strategia di risposta agli eventi;

    - utilizzare un programma di continuità aziendale, eventualmente basato sul Cloud;
    - allineare la strategia di *business continuity* alle prassi di sicurezza delle informazioni attuate in risposta ad eventi avversi;
    - sviluppare un quadro di continuità operativa che includa anche la catena di fornitura (c.d. supply chain);
- **piano tattico**
    - risolvere un eventuale incidente di sicurezza secondo le migliori prassi di riferimento;
    - riportare al management aziendale circa la gestione del rischio informatico includendo piani e test di continuità operativa;
    - elaborare un efficace piano di comunicazione rivolto a tutti gli stakeholder, da attuare in caso di eventi avversi;
    - includere la BIA come parte integrante del processo di gestione del rischio informatico.

In situazioni reali come quella precedentemente descritta per Maersk risulta evidente che l'implementazione congiunta di quanto descritto sopra come piano strategico e piano tattico ovvero l'implementazione del BCM con una prospettiva sulla c*ybersecurity* permetta di reagire in modo strutturato e ad ampio spettro:

- la BIA permette la completa identificazione e valorizzazione dei dati e dei sistemi informatici posti a supporto dei processi vitali dell'azienda;
- il BCP permette di identificare un piano per garantire di operare ad un livello minimo accettabile, anche in assenza di sistemi informatici.
- il DRP deve considerare non solo gli scenari di distruzione fisica, ad esempio del data center, ma anche gli incidenti logici che possono compromettere l'integrità e la disponibilità dei dati e dei sistemi di

produzione.

In conclusione, nell’ottica di aumentare la resilienza complessiva delle aziende è opportuno che queste agiscano contemporaneamente su due aspetti: innanzitutto la definizione e l’implementazione di un sistema di gestione della *cybersecurity*. Parallelamente le aziende, dando per assodato che non è possibile eliminare totalmente il rischio, dovrebbero predisporre un BCP da attuare nella malaugurata eventualità che un avverso evento di *cybersecurity* colpisca i propri sistemi informativi, rendendoli indisponibili.

La combinazione di queste due pratiche, ed il loro continuo esercizio e miglioramento, è certamente capace di garantire la sopravvivenza delle aziende anche nelle condizioni più estreme.

Note

[1] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

A cura di: **Matteo Salvaggio**

https://www.ictsecuritymagazine.com/articoli/come-approcciare-business-continuity-e-cyber-security-sinergicamente/