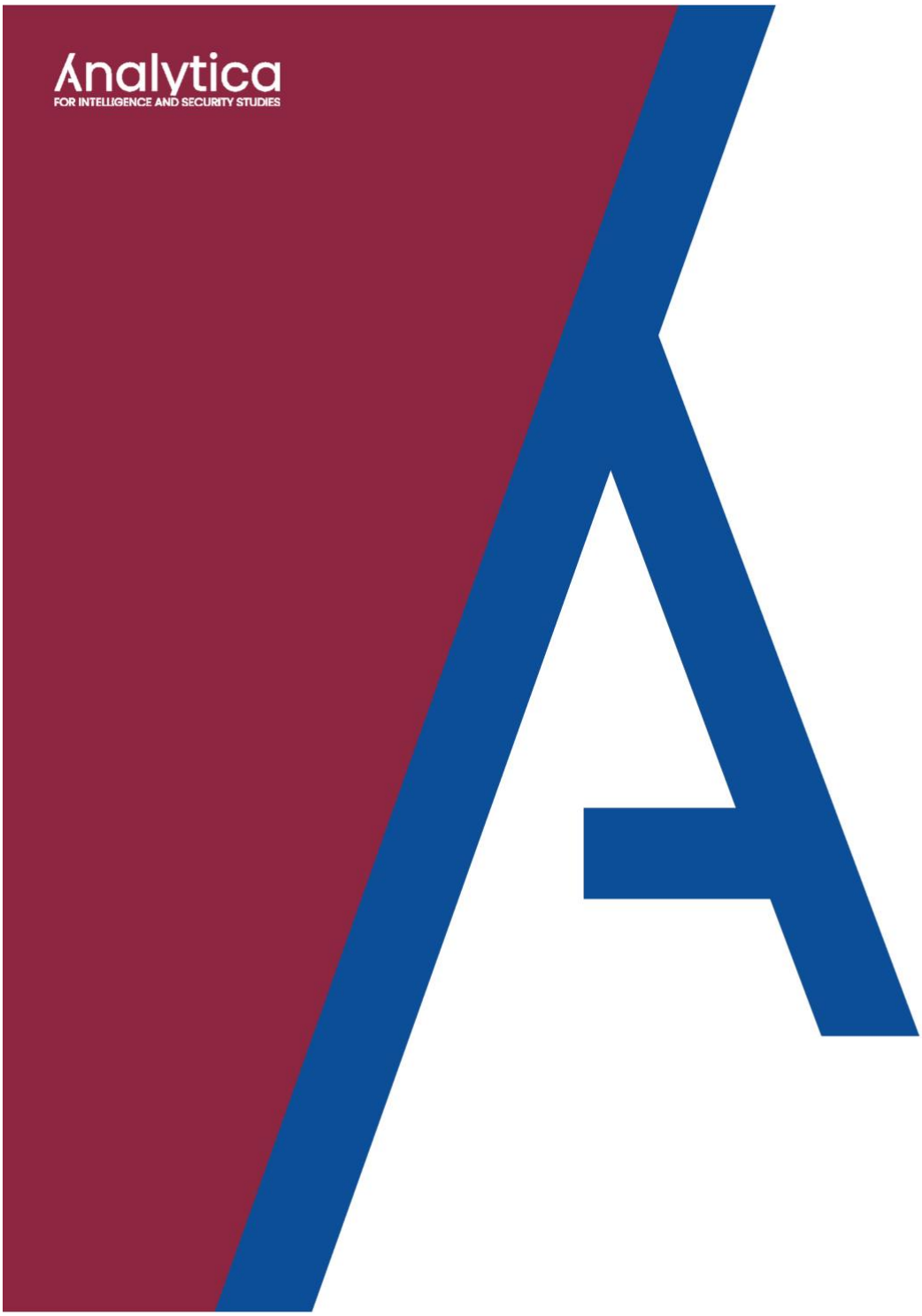

La continuità operativa e l'analisi dei rischi per un sistema resiliente.

Spelta Maurizio
Esterin Kojtari - Benedetto Fucà

Analytica for intelligence and security studies

Paper Cyber-Security

La continuità operativa e l'analisi dei rischi per un sistema resiliente.

Spelta Maurizio
Esterin Kojtari – Benedetto Fucà

Torino, giugno 2021

Prepararsi adeguatamente alle minacce cibernetiche è quanto mai fondamentale sia per il settore pubblico che privato. È necessario elaborare preventivamente piani in modo da non farsi cogliere impreparati di fronte all'interruzione dei servizi e garantire la continuità degli stessi. Le misure da adottare sono diverse; in questo documento l'attenzione verrà posta sull'analisi dei rischi, la Business Continuity, l'Incident Handling & Response e il Disaster Recovery Plan. Anche alla luce di quanto accaduto recente con il service provider OVH, che a seguito di un incendio che ha danneggiato alcuni data center della stessa società. In questo documento, verrà proposto uno scenario di un'ipotetica società che usufruendo dei servizi offerti da OVH dovrà stabilire in che modo dovrà gestire il rischio, garantire una continuità operativa in caso di un incidente e allo stesso tempo ripristinare i propri servizi.

1. Analisi dei rischi

1.1 Obiettivi aziendali

Per un'analisi dei rischi che tenga conto del contesto organizzativo e degli obiettivi strategici di business, è necessario individuare due scopi:

- garantire la continua fruizione dei beni e dei servizi resi dalla società;
- mantenere un servizio efficiente in linea con alti livelli di customer care.

Prendiamo ad esempio una società di e-commerce che, attraverso il cloud provider OVH, offre servizi e beni mediante il proprio sito. Naturalmente, se questo da un lato fornisce ai clienti una maggiore accessibilità, dall'altro espone la società stessa a rischi di varia natura. Questi rischi vanno valutati tenendo conto del contesto aziendale secondo fattori che possono essere di natura fisica, procedurale e informatica.

L'utilizzo di sistemi informativi infatti amplia il perimetro aziendale, ampliando i rischi intrinsechi e l'esposizione dell'azienda alle minacce di varia natura. Per un'attenta valutazione dei rischi, può essere utile prendere come supporto e guida allo standard ISO3100:2018[1] che permette alle organizzazioni di supportare la gestione del rischio nelle attività e nelle fasi più importanti. Questo processo è fondamentale per comprendere il livello di maturità dell'organizzazione rispetto ai rischi che possono comportare un danneggiamento/ inutilizzabilità/perdita continuità dei servizi erogati, andando in ultima istanza ad incidere sugli obiettivi aziendali. Infatti le minacce presenti potrebbero verificarsi, esponendo gli asset ad eventi che potrebbero generare un'incertezza o una distorsione rispetto gli obiettivi aziendale.

[1] Testo originale dello standard consultabile al seguente link: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

L'analisi dei rischi è dunque un processo fondamentale da attuarsi sistematicamente, in modo da comprendere a pieno quali asset sono maggiormente vulnerabili e dunque implementare una strategia atta a prevenire ed eventualmente mitigare i rischi. In particolare, l'analisi dei rischi non è solo necessaria per l'ottimizzazione dei processi aziendali rispetto al rischio generico, ma anche a quello cyber, ma è un obbligo normativo previsto dalla direttiva NIS[2]. Secondo la suddetta normativa, essendo OVH un servizio Cloud, si configura come Fornitore di Servizi Digitali sui quali vi è **l'obbligo** di attivare misure tecnico-organizzative per gestire i rischi e ridurre le conseguenze sia in ambito di un attacco informatico, sia di un evento di altra natura, in base al Regolamento di esecuzione (UE) 2018/151 della Commissione del 30 gennaio 2018[3].

1.2 Individuare gli asset da valutare

L'individuazione degli asset all'interno di un'organizzazione è un processo importante, in quanto permette di mappare e avere una una visione del proprio perimetro aziendale. Individuare ogni singolo asset permette, per l'appunto, di comprendere quale minaccia ciascun asset può subire. Una prima suddivisione va fatta tra asset tangibili (beni materiali) e intangibili (categoria eterogenea che include reputazione, proprietà intellettuale, sistemi informatici e dati aziendali o dei clienti). Rapportandosi al caso concreto di un'azienda di e-commerce, essa può essere composta di asset tangibili come ad esempio server, dispositivi, reti, magazzini, merce e beni intangibili quali sito web, database, layer applicativi, i vari processi aziendali e il know how del personale. Tutti questi asset sono necessari per il business della società. Se uno di questi asset, non fosse operativo o disponibile, la continuità operativa potrebbe rallentare o fermarsi, creando un danno diretto (al business in termini di mancato ricavi) e/o un danno indiretto (reputazionale)

1.3 Rischio

Per meglio definire il concetto di rischio, è utile richiamare lo standard ISO 31000:2018, anche per analizzare in maniera descrittiva e a titolo esemplificativo due tipologie minacce che possono verificarsi. Questa descrizione ci permette di comprendere come si dovrebbe attuare un piano di gestione e trattamento del rischio.

Facendo riferimento alla società di e-commerce, possiamo ipotizzare due minacce.

---

[2]Testo originale della Direttiva consultabile al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016L1148&from=IT

[3] Testo originale del Regolamento consultabile al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32018R0151

Una di tipo ambientale: un incendio che può svilupparsi nel perimetro fisico dell'azienda e può colpire gli asset fisici e allo stesso tempo arrecare danni ad un server, comportando la perdita di dati aziendali conservati in esso.

L'altra tipologia di minaccia è più legata all'ambito cyber: un attacco ransomware. Essi sono una tipologia di malware che può infettare i dispositivi rendendoli inutilizzabili attraverso la cifratura dei sistemi informatici. L'elemento peculiare di questi malware risiede nel fatto che l'attaccante chiede un riscatto dietro pagamento (in criptovalute) per rilasciare una password in grado decriptare i file.

Per analizzare i rischi connessi a queste due minacce è utile prendere a riferimento questi fattori:

- cause ed eventi;
- minacce e opportunità;
- vulnerabilità e capacità;
- cambiamenti nel contesto esterno e interno;
- indicatori di rischi emergenti;
- la natura e il valore dei beni e delle risorse;
- conseguenze e loro impatto sugli obiettivi;
- limiti di conoscenza e affidabilità delle informazioni
- fattori legati al tempo;
- pregiudizi, ipotesi e convinzioni delle persone coinvolte.

Mediante questi fattori, infatti è possibile calcolare il rischio inerente, ossia l'esposizione ad una minaccia. Ovviamente il rischio inerente può essere gestito e mitigato attraverso alcune azioni che portano alla riduzione dell'esposizione del rischio che vedremo più avanti.

1.4 Evento = probabilità x impatto

Fondamentale per comprendere in che modo questi rischi possono andare ad intaccare gli obiettivi aziendali è capire come il verificarsi degli stessi può esporre la società a eventi non previsti, i quali possono arrecare un danno. Per fare ciò è utile richiamare la seguente formula: *Evento= probabilità x impatto*. Utilizzando una scala di valori da 1 a 5 per entrambi le variabili della formula, nella fase di valutazione dei rischi si dovrà calcolare il livello di probabilità e d'impatto che le due minacce potrebbero avere. Per meglio comprendere il processo, si riporta una matrice rappresentativa:

Con riferimento alla prima minaccia (l'incendio) possiamo dare un valore alla probabilità che esso accada uguale a 4 (probabile), supponendo che l'azienda operi in maniera tale da non garantire a

Probabilità	Impatto: Trascurabile	Minore	Moderato	Significativo	Grave
Molto Probabile	Medio-Basso	Medio	Medio-Alto	Alto	Alto
Probabile	Basso	Medio-Basso	Medio	Medio-Alto	Alto
Possibile	Basso	Medio-Basso	Medio	Medio-Alto	Medio-Alto
Possibilità bassa	Basso	Medio-Basso	Medio-Basso	Medio	Medio-Alto
Improbabile	Basso	Medio-Basso	Medio-Basso	Medio	Medio

pieno il rispetto delle normative antincendio e che non sia dotata di adeguati sistemi che possono prevenire il propagarsi dello stesso. Il valore dell'impatto sarà uguale a 5 (grave) in quanto lo stesso potrebbe comportare la distruzione di asset fondamentali per la società. Seguendo la matrice e la formula adottata, il risultato genererebbe un evento con rischio alto.

Seguendo lo stesso ragionamento per la seconda minaccia (ransomware) possiamo assegnare i seguenti valori: probabilità 5 (molto probabile) laddove la società non utilizza sistemi di anti malware e il personale non è stato adeguatamente formato sui rischi cyber. Il valore assegnato all'impatto è 5 (grave) in quanto laddove questa minaccia si verificasse comporterebbe il mancato utilizzo dei dispositivi necessari per l'obiettivo di business della società di e-commerce. L'evento, qualora si realizzasse, si collocherebbe nella fascia di rischio alta (si veda la cella in alto a destra).

Per quanto riguarda la possibilità che si concretizzi un attacco ransomware, le misure di mitigazioni dovranno riguardare gli asset informatici:

- si dovrà valutare quali dispositivi non dispongono più degli aggiornamenti dei vendor e pertanto valutare una loro dismissione sicura (sia fisica che dei dati in essi contenuti);
- valutare con i fornitori se sono previsti aggiornamenti periodici del software e patch delle vulnerabilità note
- prevedere strategie di backup
- piani periodici di Vulnerability Assessment e Penetration Test
- prevedere sistemi di rilevazione, l'analisi e la risoluzione istantanee delle segnalazioni degli utenti su messaggi phishing

Un piano di misure di mitigazione potrà valutare di intervenire prima su alcune aree maggiormente a rischio per poi prevedere ulteriori azioni in aree di minore rischio, questa soluzione si ricollega anche alla fase di monitoraggio e implementazione che verrà descritta più avanti.

1.5 Gestione del rischio appropriato e dinamico

La gestione del rischio consiste nella selezione, in base ai costi e ai risultati attesi, degli strumenti da applicare per rendere il rischio economicamente accettabile. Una gestione del rischio deve essere appropriata e dinamica. Infatti, essa deve ricalcare la propensione al rischio della società e deve tenere conto del perimetro aziendale, partendo da questi due principi, il rischio deve essere gestito in maniera calzante al contesto organizzativo dato dalla società. Inoltre, questa gestione deve essere dinamica, ad ogni cambiamento interno (nuovi dispositivi, nuove policy, nuovo assetto organizzativo) ed esterno (nuove tipologie di minacce cyber) essa deve essere riformulata andando a considerare come questi cambiamenti possono andare ad influenzare direttamente i fattori e quindi alzare o abbassare il valore del rischio inerente.

Attraverso trattamento del rischio, la società quindi adotterà, in base all'ISO 31000:2018, un processo iterativo che comprende:

- la formulazione e selezione delle opzioni di trattamento del rischio;
- la pianificazione e implementazione del trattamento del rischio;
- la valutazione dell'efficacia di tale trattamento;
- la possibilità di decidere se il rischio rimanente è accettabile.

Questo processo permetterà all'azienda di avviare un processo che partendo dalla governance, andrà a coinvolgere tutti gli stakeholder attraverso la scelta e l'attuazione di misure di mitigazione per portare il livello di rischio ad un livello ritenuto accettabile dal management della società e che deve risultare in linea con gli obiettivi che si è data.

1.6 Misure di mitigazione

Quindi dopo aver valutato ed aver effettuato una gestione del rischio, con riferimento alle due minacce, sarà necessario che la società intraprenda azioni aventi come scopo la mitigazione del rischio. Significherà in altre parole, adottare misure che permettono di ridurre il rischio inerente.

La società dovrà quindi decidere quali azioni intraprendere in base alla propria capacità economica, effettuando una scala di prioritizzazione degli asset da salvaguardare per rispettare i propri obiettivi aziendali, una particolare attenzione in entrambe le minacce dovrà essere dato al fattore umano: una corretta preparazione del personale lavorativo dei comportamenti da intraprendere al fine di limitare

i rischi dovrà essere tenuta in considerazione. Molto spesso, comportamenti imprudenti o dettati da negligenza aumentano il rischio. Predisporre policy, procedure e stabilire processi, stabilire azioni di formazione e training al fine far prendere conoscenza e praticità con le nuove misure introdotte.
Con riferimento alla minaccia che possa scaturire un incendio dovrà pertanto creare, monitorare e implementare processi compliance con la normativa sulla sicurezza dei luoghi di lavoro andando ad installare sistemi di allarmi antincendio, prediligendo soluzioni più efficaci secondo un approccio non solo di prioritizzazione ma che tenga conto degli asset con maggiore rischio inerente. alisi dei rischi, Business Continuity Plan, Incident Handling & Response e Disaster Recovery Plan. Questi sono piani finalizzati a garantire la continuità dei servizi di un'organizzazione anche a seguito di incidenti di qualunque entità e natura.

1.7 Rischio residuo

Tutte le azioni che si vanno ad intraprendere per mitigare il rischio sono tese ad abbassare il livello dello stesso. Rimane sempre valore di rischio che prende il nome di rischio residuo. Esso è quello che rimane anche dopo che è sono state adottate le misure di mitigazione. In questa fase, qualora la società decidesse, potrebbe valutare il trasferimento di tale rischio ad un'assicurazione mediante polizze di cyber risk.

1.8 Monitoraggio e implementazione

A monte della valutazione dei rischi, la società dovrà continuare a monitorare e dovrà, inoltre prevedere un piano di implementazione del rischio. Il monitoraggio sarà necessario per valutare che la gestione del rischio risulti sempre in linea con gli obiettivi aziendali, dall'altro lato dovrà prevedere che le azioni prese per mitigare il rischio siano rispettate.Qualora avvenisse un cambiamento interno ed esterno esso dovrà essere valutato (gestione del rischio dinamico), andando a configurare un'implementazione necessaria per mantenere il rischio ad un livello tollerabile.

2. Business Continuity Plan[4] (BC)

2.1 Identificare l'obiettivo del piano

Il Business Continuity Plan è fondamentale per garantire la continuità delle funzioni chiave della propria Organizzazione. Per far ciò, bisogna garantire il corretto funzionamento e la continuità delle aree fondamentali del proprio business, analizzate di seguito nell'elaborato. Priorità verrà data a determinate funzioni che permettono ad un'organizzazione di continuare il proprio business.

[4] Riferimento ISO22301:2019 - https://www.iso.org/standard/75106.html

2.2 Creare un Business Continuity team

In primo luogo, bisogna identificare il personale e le infrastrutture necessarie per il business. Nel caso preso in considerazione questa è un'azienda di e-commerce, il business è diviso in: risorse umane (comprende area marketing, l'area operation che si occupa della logistica e servizio clienti e quella commerciale dell'assortimento pricing e informazioni catalogo); sistemi informativi (come il sito web, i servizi cloud, le applicazioni e i servizi di pagamento); infrastrutture fisiche (il magazzino, gli uffici e le infrastrutture fisiche informatiche); la documentazione (sia contratti che i dati personali dei lavoratori, dei fornitori dei servizi e dei clienti).

2.3 Identificare le aree fondamentali per il business

Di seguito bisogna identificare le aree fondamentali per il business, ovvero gli strumenti e le infrastrutture per poter continuare la propria attività commerciale. In questo caso, fondamentale sono la continuità dei propri sistemi informatici: il sito web deve essere raggiungibile sia dei clienti che hanno effettuato già un acquisto, sia dai futuri clienti. Data la natura del business dell'azienda in esame, la priorità verrà data al servizio di post-vendita ovvero il servizio di spedizione per i clienti che hanno effettuato acquisti pre-disaster. Devono essere garantite le possibilità di osservare lo status dell'ordine, contattare direttamente l'azienda e il vettore di spedizione. Nel caso in cui i sistemi informatici siano offline, bisognerà nel tempo minore possibile di trovare una soluzione alternativa come indicato nel Disaster Recovery Plan. Bisognerà dare massima priorità al ripristino dei sistemi informatici. I servizi di pagamento sono affidati ad una banca esterna e per tale ragione non rientrano nel progetto di business continuity. La privacy dei clienti, dei lavoratori e dei fornitori dei servizi deve essere garantita e protetta. Nel caso di compromissioni bisognerà effettuare l'iter legislativo ed azienda propriamente indicato. Deve essere garantita la continuità delle infrastrutture fisiche come il magazzino, perché imprescindibile per la parte finale del business. Nel caso di problematiche varie, bisognerà trovare una soluzione alternativa con un magazzino in loco. Il funzionamento del servizio trasporti è la conclusione del ciclo commerciale dell'azienda, bisogna assicurare il corretto funzionamento del servizio, anche attraverso appalti esterni a quelli già effettuati dall'azienda, fatta un'analisi costi-benefici. Per tutte le aree fondamentali è indicato il valore di *Recovery Point Objective* (RPO, ovvero il tempo tollerante per la messa in sicurezza dei dati informatici) e del *Recovery Time Objective* (RTO, il tempo necessario per il pieno recupero dei dati informatici). Questi valori sono indicati in giorni lavorativi.

Funzione	RPO	RTO
SISTEMI INFORMATICI	1	3
CRM	1	2
FATTURAZIONE	2	5
MAGAZZINO	2	3

Analizzando la tabella soprastante, possiamo concludere che priorità del disaster recovery sarà la messa in sicurezza e nel recupero dei sistemi informatici e dei dati dei clienti, fornitori dei servizi e dei lavoratori. La tollerabilità nei confronti di queste due aree è molto bassa perché inciderebbe in modo dominante all'interno del ciclo commerciale dell'azienda. Maggior tollerabilità invece è data alle infrastrutture fisiche e sui trasporti poiché entrerebbe nelle casistiche eccezionali previste dal ciclo produttivo.

2.4 Identificare l'interdipendenza dei processi e delle aree fondamentali:

L'interdipendenza tra le varie aree dell'e-commerce analizzate nel punto 2.4 è estremamente alta. Senza un corretto funzionamento dei sistemi informatici, viene meno l'intero business model dell'azienda e-commerce. Problematiche relative al magazzino e/o al sistema dei trasporti inciderebbe sull'efficienza dell'azienda e sulla fiducia dei clienti. Molti clienti potrebbero effettuare il reso e/o annullare ordini già conseguiti pre-disaster. Questo porterebbe ad un danno economico, non solo dal punto di vista dei costi da sostenere per i resi e/o annullamenti ma soprattutto sulla fiducia dei clienti e dei futuri clienti.

2.5 Determinare il Maximum Recovery Time Objective (MRTO)

Il Maximum Recovery Time Objective indica è la quantità massima di tempo accettabile per poter ripristinare i dati e per poter riprendere il lavoro. Per determinare il **MRTO** bisogna prima analizzare il bilancio economico dell'azienda -commerce. Nel nostro caso, l'azienda presenta un ricavo giornaliero di 100€ e dei costi totali giornalieri di 10€. Il totale del patrimonio aziendale è di 1000€. L'azienda e-commerce, nel caso di un shutdown totale dei propri servizi potrebbe garantire la copertura dei costi totali per cento giorni dall'evento avverso. Il MRTO, quindi, dovrebbe essere uguale o inferiore a 100: empiricamente dovrà essere inferiore poiché parte del patrimonio sarà utilizzato per sostenere i costi dovuti alla gestione e risoluzione del problema.

2.6 Priorità e fattori esogeni

La priorità di una azienda dell'e-commerce post-disaster è quella di finalizzare tutti gli ordini effettuati pre-disaster in modo da garantire la fiducia del consumatore finale. A tal ragione, bisogna attivare un servizio clienti adeguatamente strutturato, garantendo un'informazione esaustiva riguardo alle problematiche che possono portare ritardi nelle consegne. Bisogna inoltre, rassicurare il consumatore sulla salvaguardia dei suoi dati personali, quelli di pagamento e del rispetto della legislazione in essere.

2.7 Multi-cloud e strategie di business continuity

Attuare una strategia di business continuity basata su un'architettura multi-cloud è fondamentale per affrontare rischi e problematiche di ogni genere. Il multi-cloud beneficia l'azienda evitando la dipendenza da un unico fornitore. Il multi-cloud permette inoltre di dividere i dati e le applicazioni tra i due provider oppure di utilizzare il secondo come sito di backup nel caso il primo abbia problemi. Inoltre, permette di minimizzare i costi, scegliendo di volta in volta il servizio tramite un'analisi costi-benefici tra i due o più cloud.

3. Incident Handling & Response

I Team di Incident Handling & Response (IH&R) si occupano della gestione degli incidenti che riguardano
la cyber security o altri tipi di incidente. Questo significa definire che l'azienda deve definire le strutture, il personale adeguato e formato e tutte le procedure necessarie per gestire gli incidenti. Secondo alcune ricerche, ci vogliono mediamente più di 100 giorni per scoprire un attacco informatico e a seconda della gravità più di 40 giorni per contenerlo e mitigarlo. Questo perché circa il 76% delle organizzazioni non prevede efficienti piani per il recupero da incidenti. Dunque, le procedure di IH&R sono fondamentali.
Dotarsi di un Team IH&R e degli strumenti necessari alla detection fa diminuire questi valori in modo significativo.

3.1 Incident triage

Una volta che si verifica un incidente e viene assegnato ad un team, si procede in 3 fasi:

- *L'analisi* dell'incidente e la sua *validazione* serve a capire di che tipo di incidente stiamo esaminando; un cyber-attacco? un problema di software o di hardware? o altro...

- La *classificazione.* Il Team IH&R deve trovare la fonte dell'incidente, analizzare i log e la correlazione degli eventi e vedere su che tipologia di asset c'è stato l'incidente, in modo da poterlo classificare.
- La *prioritizzazione*, che si articola su 4 livelli: critico (L4), alto (L3), medio (L2), basso (L1). Questa scala dipende dall'impatto che l'incidente sta avendo sugli asset e dunque sul business aziendale. Se si rischia una perdita di dati, bisogna determinare la sensibilità di questi (riguarda i clienti? si rischiano grosse perdite finanziarie? sono dati personali? o particolari?). Chiaramente, maggiore la criticità maggiore dovrà essere la prontezza nella risposta.

Nel caso di OVH che subisce un incendio, stiamo dunque parlando sicuramente di perdita di asset fisici e potenzialmente di dati nel caso non ci siano strutture di backup apposite; se si trattasse di un ransomware, sono a rischio sia i dati personali della società che quelli dei clienti. Nel caso di un incendio che pregiudica la continuità del servizio (ad esempio l'indisponibilità di più sistemi contemporaneamente), la priorità sarà alta o critica; nel caso di un ransomware, a seconda della sua ampiezza e complessità può variare (alcuni possono essere risolti subito e bloccano porzioni ristrette di dati, altri bloccano l'intero sistema).

In seguito l'incidente va notificato a chi è competente per gestirlo internamente (per esempio l'IT o al dipartimento di crisis management) ed eventualmente al top management che dovrà a norma di Direttiva NIS comunicare l'incidente all'autorità nazionale preposta (in Italia essa è lo CSIRT[5]) in caso di perdita di dati personali avviare la procedura di data breach e comunicarla al garante entro i tempi stabiliti dalla norma. Determinare chi deve venire a conoscenza dell'incidente è fondamentale, sia che si tratti di persone interne alla struttura che esterne (in caso fossero colpite), in modo da poter assegnare il giusto ruolo a chi si occupa di mitigare. Prima ancora di mitigare però, bisogna adoperarsi per *contenere* l'incidente. Questo deve avvenire istantaneamente, soprattutto se si tratta per esempio di un incendio, per evitare danni irreparabili. Il contenimento serve a "limitare la diffusione" e quindi da il tempo per poi raccogliere tutte le informazioni necessarie, specialmente se si tratta di un attacco informatico. Queste informazioni, per esempio di tipo forense, servono sia per analizzare l'accaduto e rispondere adeguatamente, ma anche per eventuali procedimenti legali. Se si è sotto attacco malware o similari, è necessaria un'accurata analisi in modo da non solo identificare la fonte del problema ma anche ogni possibile "traccia" dell'attacco.

[5] Acronimo di Computer Security Incident Response Team, incardinato presso il Dipartimento delle Informazioni per la Sicurezza della Presidenza del Consiglio.

Il processo di *eradicazione* serve dunque a "ripulire" il sistema dopo che l'incidente è stato contenuto. Ciò significa anche disabilitare account compromessi. A seguito di ciò i Team IH&R devono procedere con la fase di *recupero*, che consiste soprattutto nel controllare che le vulnerabilità siano state risolte in maniera che non possano essere più sfruttate e, conseguentemente, assicurarsi che tutti processi riprendano normalmente.

Quando l'incidente è stato risolto va preparata una documentazione in merito. Questa deve servire a definire bene il "cosa" e il "come" dell'incidente, in modo da prepararsi adeguatamente ad una situazione simile. Per quanto le tattiche dei cybercriminali siano in continua evoluzione, non va sottovalutato il rischio di "ricaderci", soprattutto se non si è implementato un piano IH&R adeguato. Questo discorso vale anche per incidenti fisici; le strutture avevano adeguate misure di sicurezza? Sono conformi alle normative? Dunque, va prodotto un assessment sull'impatto che questo incidente ha avuto sull'organizzazione. Questo può comprendere la tipologia e quantità di dati perduti, danni materiali e i costi sostenuti per ripristino. La documentazione e l'assessment servono a verificare, a seconda della gravità dell'accaduto, se è necessaria una riforma delle politiche e pratiche interne all'organizzazione. Se l'incidente è avvenuto per mancanze gravi nell'organigramma o nelle misure, è necessario rivedere le *policies* in modo da non farsi trovare impreparati in seguito. La non conformità con regolamenti nazionali ed europei come il GDPR o la direttiva NIS hanno gravi conseguenze sull'immagine dell'organizzazione e possono comportare sanzioni di un certo calibro. Quanto tutto è stato risolto, è tempo di chiedersi se rilasciare informazioni in merito all'incidente e come farlo. Bisogna dunque valutare che tipo di informazioni, che grado di sensibilità hanno e a chi comunicarle. Non notificare ai diretti interessati non è corretto, al contempo è preferibile rilasciare solo ed esclusivamente le informazioni necessarie sull'accaduto, in modo da non danneggiare l'immagine dell'organizzazione che subisce l'incidente.

4. Disaster Recovery Plan[6] (DR)

Abbiamo finora analizzato i rischi che minacciano il nostro servizio e ne abbiamo definito le strategie di Business Continuity, cosa accade invece quando l'incidente si verifica e produce un impatto tale da interrompere la continuità operativa? Il Disaster Recovery Plan è una procedura che stabilisce le azioni da attuare al fine di proteggere l'azienda dagli effetti negativi degli incidenti al fine di permetterle un rapido recupero a seguito di un evento negativo.

[6] Riferimento ISO22301:2019 - https://www.iso.org/standard/75106.html

Qualora si verificasse un incidente, e se la gravità è tale da costringere l'azienda ad attuare il piano di DR. Alla luce di quanto indicato, un piano di Disaster Recovery, dovrebbe prevedere: un ripristino dei servizi essenziali che ne permettono di riprendere le attività nel breve tempo possibile in accordo con il piano di BC. Una strategia di Disaster Recovery dovrà prevedere un Data Center alternativo per il ripristino, qualora l'azienda si sia appoggiata su un'infrastruttura cloud, come nel nostro caso, dotarsi di una strategia multi cloud sarebbe la scelta migliore sotto molti aspetti. infine, dotarsi di una strategia ben dettagliata che permetta alla società di individuare quali sono gli asset fondamentali che devono avere priorità in un piano di ripresa della continuità operativa è una scelta strategica, quali dati sono necessari, il personale che deve operare e una strategia di backup dei dati, questo permetterebbe di ottimizzare i costi di un piano di DR.

4.1 Tecniche di Disaster Recovery

Sistemi e dati considerati importanti vengono ridondati in un "sito secondario" o "sito di Disaster Recovery" per far sì che, in caso di un disastro di qualsiasi natura sia tale da rendere inutilizzabili i sistemi informativi del sito primario, sia possibile attivare le attività sul sito secondario al più presto e con la minima perdita di dati possibile. Ci sono svariate tecniche per far ciò:

- **Replica sincrona**: presenza di dati in due siti paralleli, utilizzandole come strumento di ripristino così da ottimizzare i tempi.
- **Replica asincrona:** attraverso la lontananza geografica per permettere al business di poter reagire anche nel caso disastri in larga scala, come per esempio un terremoto.
- **Tecnica mista:** utilizzando sia la replica sincrona che quella asincrona per ottimizzare il disaster recovery.
- **Adozione di un servizio multi-cloud:** attraverso l'attivazione di più servizi di hosting cloud al fine di poter riprendere il servizio qualora uno dei cloud non fosse disponibile.

4.2 Virtualizzazione e Cloud Computing[7]

Esistono soluzioni tecnologiche che permettono il recupero dei dati in situazioni di crisi, rispettando l'integrità, la confidenzialità e la sicurezza di quest'ultimi. La *virtualizzazione* permette di emulare tramite un software un ambiente fisico. Questa strategia permetterebbe di ridurre i costi e i tempo. Il *cloud* permette la possibilità di usufruire dei dati "on-demand" da un provider che offre dei servizi ben specifici (chiamati *Infrastructure as a service*). Il backup tramite Cloud permette di rispettare sia il RTO che RPO.

[7] https://www.agid.gov.it/sites/default/files/repository_files/linee_guida/linee-guida-dr.pdf

La flessibilità dei contratti potrebbe costituire un ottimo vantaggio economico per l'azienda, poiché permetterebbe di acquistare solo un servizio specifico, modellato ad-hoc. La scelta di un provider Web Hosting deve essere fatta tramite un'analisi scrupoloso dei contratti: nel caso del "Disastro OVH", nelle condizioni generali di contratto si declina ogni responsabilità sulla corretta esecuzione del backup, affidandola all'azienda stessa. Non avendo previsto un Disaster Recovery Plan, i dati dell'azienda potrebbero essere stati eliminati per sempre (si possono ipotizzare anche possibili ripercussioni a livello di privacy secondo la normativa EU679/2016). Bisogna sempre porre attenzione sulla centralità di effettuare backup, direttamente o indirettamente tramite i provider scelti.

Conclusioni

Con questo percorso è stata delineata una strategia di gestione del rischio nel riguardo di un'azienda e-commerce cliente di OVH. Attraverso l'analisi dei rischi si è cercato di individuare le problematiche che possono causare un disservizio dei sistemi informativi aziendali, ponendo l'accento di quanto ogni rischio possa incidere sul business dell'azienda. Attraverso la strategia di Business Continuity si è cercato di ipotizzare strumenti e metodi per garantire la continuità dell'azienda, identificando le aree fondamentali del business e il tempo massimo per poter garantire il corretto ripristino di queste ultime. Con l'incident handling invece, abbiamo presentato un modello per poter gestire l'incidente di qualunque natura esso sia, dal punto di vista strategico che organizzativo. Infine, abbiamo formulato alcune ipotesi di Disaster Recovery basate sulle tipologie di backup e l'adozione di strategie multi-cloud.

Ponendo come esempio il caso OVH e le problematiche che esso ha generato a migliaia di imprese, le quali potevano essere evitate, dotandosi di un piano descritto in questo documento.