Unit 3 week 1

Giorno 1- cyber security and operation

1. Introduzione

In questo modulo ci focalizzeremo sugli aspetti operativi della sicurezza informatica nel mondo enterprise, introducendo il concetto di “**security operation**”.

**Affronteremo i seguenti argomenti legati:**

* Al monitoraggio degli eventi di sicurezza e alla gestione di eventuali “alert”.
* Alla gestione completa degli incidenti di sicurezza;
* Alle azioni preventive che possono essere implementate per evitare gli incidenti di sicurezza;
* Alle azioni per ripristinare gli asset, le applicazioni critiche a valle di un incidente di sicurezza.

**Dopodiché ci concentreremo sullo studio delle tecniche utilizzate per le analisi dei malware, sempre in ottica di Security Operation.**

Durante le attività pratica e durante la build week analizzeremo codice di malware proveniente dal “mondo reale”, ovvero software scritto intenzionalmente per arrecare danno a cose o persone.

Affronteremo l’analisi statica, dove i malware verranno analizzati senza eseguirli, e l’analisi dinamica, dove bisogna fare attenzione in quanto a livello pratico si utilizzeranno dei tool che prevedono l’esecuzione real-time dei malware.

Uno degli scopi principali della sicurezza informatica è **mettere al sicuro le informazioni e i dati.**

La **sicurezza di un ambiente informatico viene parametrata sulla base di “principi fondamentali”.** Uno dei principi cardine e più importanti per valutare lo stato della sicurezza delle informazioni di un dato ambiente è il “**CIA principle**”**, dove:**

* **C** sta per **Confidentiality**, ovvero la riservatezza del dato;
* **I** sta per **Integrity**, ovvero l’integrità del dato;
* **A** sta per **Availability**, ovvero la disponibilità del dato.

Generalmente, i controlli di sicurezza sono valutati in base al loro impatto sulle componenti del “CIA principle” (detto anche **CIA triade**)**.**

**Confidentiality**

Il primo principio della **triade CIA** è la “**confidentiality**” **o riservatezza.**

Questo principio si concentra su quello che è l’accesso al dato, **che deve essere garantito solamente agli utenti autorizzati.**

La protezione della riservatezza ha di fatto lo scopo di prevenire o minimizzare gli accessi non autorizzati a determinate informazioni.

C’è un ampio spettro di controlli di sicurezza che impattano positivamente sulla riservatezza del dato, come ad esempio la **cifratura, e le tecniche di controllo degli accessi.**

**Integrità**

Il secondo principio della **triade CIA** è l’**Integrità, ovvero il concetto di proteggere l’affidabilità e la correttezza del dato.**

In altre parole, la protezione dell’integrità previene modifiche non autorizzate al dato in modo tale che ad esempio in una comunicazione tra due parti, il dato ricevuto dal destinatario risulti esattamente quello inviato dal mittente.

I controlli di sicurezza che impattano positivamente sull’integrità sono molteplici, come ad esempio meccanismi di controllo accessi ed autenticazione oltre ai meccanismi di verifica degli hash (MD5, hash1, hash2.6) o checksum.

**L’integrità del dato dipende dalla riservatezza del dato.**

Ad esempio, se un attaccante riuscisse ad intercettare una comunicazione tra due parti, sarebbe di conseguenza in grado di alterare il contenuto di un dato.

**Availability (disponibilità)**

Il terzo ed ultimo principio della triade CIA è la disponibilità del dato, che deve essere garantita in ogni momento e per i soli utenti autorizzati ad accedere alla risorsa in oggetto.

La disponibilità deve essere garantita in ogni situazione, anche in situazioni critiche, ad esempio, in caso di errore a livello applicativo o “crash” dei sistemi.

Le misure di sicurezza che impattano sulla disponibilità del dato sono ad esempio: meccanismi di anti-denial of service, backup, ridondanza dell’infrastruttura, e tutte quelle altre misure di sicurezza che garantiscono la disponibilità dei servizi/dati in situazioni di criticità.

La possibilità che un evento possa accadere causando danni parziali o totali a dati, informazioni oppure asset prende il nome di “**rischio**”.

Il rischio può essere gestito in diversi modi, tra i quali:

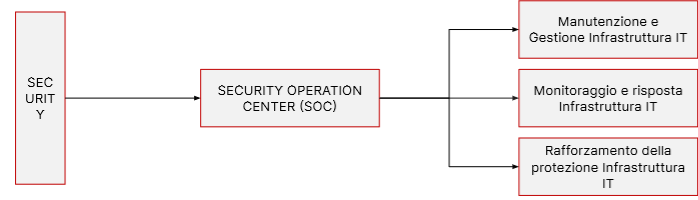
* **Riduzione del rischio:** introducendo delle “**security remediation action**”**,** ovvero delle azioni di rimedio per ridurre/eliminare il rischio;
* **Accettazione del rischio:** accettando il rischio residuo.
* **Rimozione del rischio:** rimuovendo l’asset (laddove non critica) soggetta al rischio.

1. **Security Operation**

All’interno delle moderne compagnie, la Security sta acquisendo un ruolo sempre più centrale e, soprattutto negli ultimi anni, sta cambiando il modo di vedere la security da parte delle aziende: infatti, non è vista più come un costo per il business ma piuttosto come un asset a supporto del business stesso.

Il **Security Operation Center (SOC)** è un **sotto-dipartimento all’jnterno del dipartimento di Sicurezza** che eroga servizi finalizzati alla protezione dei sistemi informatici, quali:

* **Servizi di gestione:** in questa categoria ricadono tutte quelle attività di gestione e manutenzione dell’infrastruttura IT delle compagnie, come ad esempio, la manutenzione dei server, degli switch di rete, degli applicativi ecc.
* **Servizi di monitoraggio e risposta:** questa sezione comprende tutte quelle attività erogate al fine di monitorare in tempo reale tutte le componenti dell’infrastruttura IT della compagnia. Il monitoraggio ha lo scopo di individuare tempestivamente eventuali “minacce” (anche chiamate “**security threats**”) ed in caso
  + **Minacce “avversarie”:** da parte di individui, gruppi oppure organizzazioni che tentano di minare la sicurezza di una compagnia. I nemici possono essere gruppi di hacker, impiegati scontenti, competitors ecc.
* **Minacce “strutturali o infrastrutturali”:** si verificano quando un device, un asset (come un software o altro), o una componente infrastrutturale non supera determinati test, come ad esempio: una componente infrastrutturale che è diventata obsoleta, e non più supportata dal vendor, un software deve essere aggiornato in quanto è fermo ad una versione datata che potrebbe introdurre vulnerabilità, ecc.
* **Minacce “ambientali”:** eventi di natura ambientali come uragani, maremoti, terremoti, incendi, assenza di corrente elettrica e tutti quegli eventi che si possono verificare che non sono sotto il controllo della compagnia.
* **Minacce “accidentali”:** eventi che occorrono quanto un individuo, magari un impiegato della compagnia, svolgendo i suoi compiti giornalieri, esegue un errore delle azioni che possono minare la sicurezza della compagnia, come ad esempio inviare un file con informazioni confidenziali ad un indirizzo email errato.
* **Servizi proattivi:** i servizi includono tutte quelle attività che hanno lo scopo di migliorare il livello di sicurezza generale o protezione della compagnia da eventuali attacchi interni o esterni, come ad esempio i Vulnerability Assessment, i penetration test, ecc.

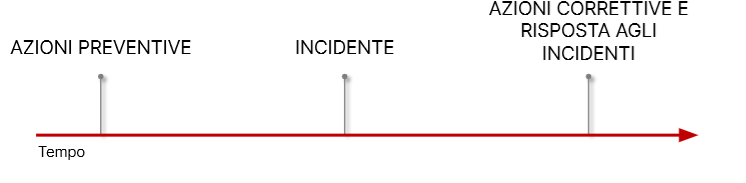


I servizi di “**Security Operation**” possono anche essere definiti secondo una logica temporale in relazione al verificarsi di una situazione particolare che viene detta “**incidente di sicurezza**”. Prima di vedere la classificazione temporale, definiamo il concetto di “**incidente di sicurezza**”.

Sebbene possa sembrare scontato, un “**incidente di sicurezza**” si riferisce ad un evento che ha un impatto negativo sulla riservatezza, integrità o disponibilità di una data risorsa, come risultato di un attacco esterno oppure di un azione volutamente dannosa proveninete dall’interno (ad esempio da un impiegato). Mentre con il termine generico “**incidente**”, si includono all’interno di casistiche considerate prima, anche gli eventi ambientali e accidentali.

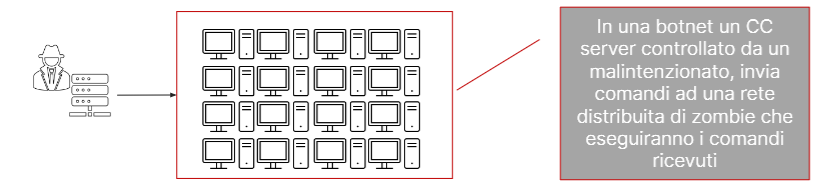
Possiamo identificare delle classi di azioni a seconda del loro posizionamento temporale rispetto ad un incidente/incidente di sicurezza. Distinguiamo:

* **Azioni preventive:** includono tutte quelle azioni di sicurezza che vengono adottate ed implementate anticipatamente e preventivamente per ridurre i rischi di eventi negativi.
* **Azioni correttive e di risposta agli incidenti:** contiene al suo interno tutte le azioni di rimedio a stretto giro per risolvere gli incidenti e ripristinare il corretto funzionamento dei sistemi informativi quanto prima possibile.



1. **Le minacce Cyber**

I professionisti della Security hanno la necessità di essere a conoscenza dei comuni vettori di attacco al fine di individuare le migliori misure preventive da adottare. Tra i vettori di attacco più comuni troviamo:

* **Botnets:** sono reti di computer dove un’entità centrale, che prende il nome di “**control-and command server**” (CC server), invia istruzioni a una rete distribuita di computer, che prendono il nome di “Zombie”, precedentemente infettati tramite virus/malware. Lo scopo di una botnet è effettuare attacchi simultanei contro target in maniera centralizzata, causando impatti negativi sulla disponibilità dei servizi. La figura sotto mostra una botnet, pensate che non è raro trovare botnet con 40000+ macchine.
* **Denial-of-service (DoS):** gli attacchi DoS hanno lo scopo di mettere fuori uso un servizio in esecuzione su un sistema, come potrebbe essere un’applicazione web, un sito web. Una delle forme più comune di attacco DoS è la trasmissione di un numero ingente di pacchetti ad un server al fine di saturare la CPU, dove si intende che la CPU è al 100% di utilizzo e non può di conseguenza processare altre richieste. La forma più comune di DoS è il Distributed DoS (DDoS), ovvero un attacco di tipo denial-of-service che viene inviato contemporaneamente verso un target da sorgenti multiple.
* **Zero-day Exploit:** gli attacci 0-day (zero-day) si riferiscono a tutti quegli attacchi che sfruttano per la prima volta una vulnerabilità ancora sconosciuta ad altri, ovvero una vulnerabilità non ancora nota. Gli exploit 0-day sono motivo ed oggetto di ricerca da parte di un numero elevato di ricercatori di sicurezza/penetration tester, che appunto testano un sistema per scovare le vulnerabilità ancora non note prima che esse vengano sfruttate da malintenzionati.
* **Man-in-the-Middle:** gli attacchi di tipo man-in-the-middle (MITM) si verificano quando un utente malintenzionato riesce ad ottenere accesso ad una comunicazione posizionandosi tra il mittente ed il destinatario. Si possono distinguere due tipi di attacchi MITM:
  + 1) lo **sniffing**, dove un attaccante riesce ad intercettare il traffico su un canale e ne legge il contenuto;
  + 2) **store-and-forward-proxy**, dove un attaccante riesce a posizionarsi nel mezzo di una comunicazione, ricevere il traffico dal mittente per poi spedirlo al destinatario. La differenza in questo secondo caso è che il traffico viene processato dalla macchina dell’attaccante durante l’attacco MITM.

1. **Security Operation: le azioni preventive**

Le ***azioni preventive*** possono essere viste come l'insieme dei controlli di sicurezza che vengono adottati da una compagnia per aumentare il livello di protezione perimetrale ed interno al fine di ridurre il rischio di potenziali attacchi.

Vediamone alcuni casi:

* **Controlli Network**:

Come visto in precedenza, le reti sono il primo punto di accesso per eventuali attacchi. Al fine di mitigare il rischio, ci sono diversi controlli che possono essere messi in campo come:

1. **NAC**: network access control. Sono soluzioni di sicurezza che aiutano le compagnie a controllare gli accessi alla propria rete, limitando di fatto l'accesso solo agli utenti autorizzati ed assicurando che i sistemi che accedono alla rete soddisfino determinati requisiti di sicurezza.
2. **Firewall**: aiutano a ridurre gli attacchi dall’esterno. Utilizzano un approccio basato su «regole o policy» che automatizzano la gestione di una particolare comunicazione. Ci sono diverse categorie di firewall che variano a seconda delle funzionalità come:

* Packet Filtering Firewall, che si «limitano» al semplice controllo del pacchetto in base alle policy;
* Stateful Inspection Firewall, che oltre al controllo sul singolo pacchetto, mantengono informazioni sullo stato dell'intera connessione che passa attraverso il firewall;
* *Next Generation Firewall (NGFW)*, che includono ancora più funzionalità di analisi, e permettono l'analisi dei flussi basati sull'utente che effettua la connessione, sull'applicativo utilizzato e così via.
* *Web Application Firewall*, dei dispositivi di sicurezza dedicati per proteggere le applicazioni quali SQL Injection e Cross Site Scripting (XSS).

1. **Segmentazione di rete**: la rete può essere segmentata in zone di rete per rendere inaccessibili le aree della rete interna che ospitano gli applicativi critici. Il principio della segmentazione «assegna» diversi livelli di sicurezza alle diverse aree della rete, come ad esempio ***DMZ***, ovvero l'area della rete che espone i servizi accessibili da internet, ***Internal Network***, ovvero l'area delle rete che ospita i server che erogano i servizi accessibili dall'interno e cosi via.
2. **IPS / IDS**: i sistemi di prevenzione e rilevamento intrusioni servono ad individuare preventivamente potenziali attacchi alle reti ed alle macchine. Mentre il sistema di rilevamento (IDS) si occupa solo del monitoraggio di determinati eventi di sicurezza in tempo reale alla ricerca di «anomalie sospette», il sistema di prevenzione (IPS) supporta anche delle azioni automatiche per fermare la potenziale intrusione.

* **Controlli sugli end-point**:

La sicurezza degli end-point quali laptop, PC, smartphone, o server è un tema critico per le aziende.

Vediamo alcuni controlli che mirano a ridurre i rischi sugli end-point:

1. **Hardening dei sistemi e delle configurazioni**: indica l'insieme delle azioni di configurazione di un sistema e delle sue componenti che hanno lo scopo di migliorare la sicurezza complessiva.

Tra queste attività ricadono attività come la disabilitazione di eventuali porte non utilizzate, la rimozione di utenti non necessari sui sistemi operativi, la riduzione dei privilegi degli utenti laddove non necessari e così via. *Vedete l'hardening come un modo di rafforzare la sicurezza di un sistema mediante la sua corretta configurazione*.

1. **Patching dei sistemi**: la «patch» indica un frammento di codice scritto per aggiornare o migliorare la sicurezza di un programma.

Ad esempio, quando su un sistema operativo o su un software viene identificata una vulnerabilità il vendor generalmente rilascia una patch che deve essere subito implementata per evitare che la vulnerabilità venga sfruttata. Il processo di implementazione della patch e di monitoraggio successivo viene detto «**patch management**» e fa parte delle attività preventive per ridurre i rischi su un sistema.

1. **Group policy**: le policy di gruppo consentono agli amministratori di reti e sistemi di gestire la sicurezza degli endpoint in maniera centralizzata. Le GPO (group policy object) infatti, permettono di applicare centralmente configurazioni standard per tutti i PC che sono all'interno di uno stesso workgroup, dominio, oppure di differenziare le configurazioni di sicurezza in base al ruolo della macchina.
2. **Penetration testing**: da un punto di vista della security operation, un Penetration Testing aiuta la riduzione del rischio su un sistema a valle dell'implementazione delle «remediation action».

Di conseguenza, le compagnie generalmente impiegano cicli e sessioni di PT sugli end-point per valutare il loro stato di sicurezza e coprire eventualmente le debolezze, implementando le azioni di rimedio.

* **Controlli sul software**:

Così come i server e gli apparati di reti, il software fa parte di quello che viene definito all’interno di una compagnia e deve essere conseguentemente protetto da minacce esterne.

1. **Code analysis**: la «code analysis», letteralmente analisi del codice, si riferisce a quelle tecniche di analisi del codice sorgente di un software al fine di identificare bug nel codice / errori di programmazione o durante l'esecuzione. Possiamo distinguere due tipi di analisi del codice:

**I) *Analisi del codice statica***, dove le righe del codice sorgente vengono analizzate senza eseguire il software;

**II) *Analisi del codice dinamica***, dove il codice sorgente viene eseguito ed il suo comportamento viene analizzato da uno speciale software.

1. **Reverse engineering**: «l'ingegneria inversa» è quell'insieme di tecniche e procedure che permettono di «risalire» al codice sorgente di un determinato software, utilizzando dei tool in base al linguaggio di programmazione utilizzato per scrivere il software stesso. In linea di massima «l'ingegneria inversa» risulta più semplice per i software sviluppati con linguaggi interpretati (come ad esempio Python), mentre risulta più complicato per i software scritti con linguaggi compilati (come ad esempio C, C++).

Vedremo successivamente le tecniche di ingegneria inversa in lezioni dedicate all'analisi dei malware.

* **Logging e Monitoring**:

Logging e Monitoring, letteralmente «registrazione e monitoraggio» è quell'insieme di procedure e tecniche che permettono di tracciare tutte le azioni su un determinato sistema da parte degli utenti, come ad esempio il login, il logout, la modifica delle impostazioni ed altri eventi significativi. Ciò aiuta le compagnie ad identificare preventivamente e tempestivamente eventuali eventi dannosi.

**Logging**: le applicazioni, i servizi, i sistemi e gli altri asset infrastrutturali generano «log» di default, o hanno la possibilità di farlo se correttamente configurati. I «**log**» sono dei file contenenti gli ***eventi e le attività*** che si verificano su un dato sistema, che includono altri dati quali: *la data e l'ora in cui l'evento si è verificato, l'utente che ha eseguito l'azione ed il sistema sul quale si è verificato l'evento*.

Possiamo identificare diversi tipi di log, sulla base delle attività, degli eventi catturati.

1. **Log di sicurezza**: i log di sicurezza includono tutti quegli eventi come accessi alle risorse, ai sistemi, ai file ed alle stampanti. Tramite i log di sicurezza un amministratore può tracciare tutti gli accessi ai propri sistemi, risalire a chi ha modificato o cancellato un determinato file. Generalmente i log di sicurezza sono abilitati di default per salvare gli eventi più significativi che si verificano su un sistema.
2. **Log di sistema**: registrano gli eventi di sistema quali: start e stop del sistema, riavvio, spegnimento. Ciò consente di monitorare eventuali eventi dannosi, come potrebbe essere il tentativo di spegnere un sistema da parte di un malintenzionato per farlo successivamente ripartire da chiavetta USB / CD allo scopo di rubare i dati. Ad esempio, i sistemi Linux salvano i log di sistema nella directory «**\var\log**».
3. **Log applicativi**: registrano le informazioni per determinate applicazioni web, come stabilito in fase di sviluppo dagli sviluppatori, come per esempio accesso a database, modifiche a determinate «table».
4. **Log dei Firewall**: i log dei firewall includono tutti quegli eventi che sono relativi al traffico che li attraversa, sia per quei flussi che sono permessi, sia per i flussi non permessi. Generalmente vengono salvate tra le altre info: IP sorgente; IP destinazione; porta sorgente; porta destinazione; l'azione effettuata sul flusso (accept / deny).
5. **Log dei proxy**: un proxy server serve ad aumentare il grado di protezione delle connessioni da rete interne verso indirizzi su internet. Nei log proxy si trovano info quali:

II) IP / URL visitati dagli utenti;

II) tentativi di connessione verso siti proibiti.

Data l’importanza del file di log, essi vengono spesso inviati a quello che prende il nome di «**log collector**» centralizzato che ha appunto il compito di centralizzare tutti i log e salvarli per utilizzo futuro.

Spesso essi vengono inviati ad un sistema centralizzato chiamato **SIEM - Security Information Event Management**, che ha il compito di correlare le informazioni provenienti da diverse sorgenti ed automatizzare il monitoraggio.

**Monitoring**: il monitoraggio degli eventi raccolti ha lo scopo principale di identificare

preventivamente comportamenti anomali sulla rete o sui sistemi da parte di un dato utente.

Quando si parla di monitoring, si introduce il concetto di «accountability», ovvero di

«responsabilità». Un utente non può negare di aver effettuato una determinata azione se dimostrata dagli eventi acquisiti su quel sistema. È importante sottolineare come il monitoraggio sia un processo continuo che assicuri che tutti gli eventi siano strettamente controllati.

Per aumentare i livelli di automatismo, spesso si implementano delle policy di sicurezza che in presenza di determinati eventi anomali fanno scattare degli «alert di sicurezza».

1. **Cenni di SIEM e SOAR**

**SIEM:** la maggior parte delle organizzazioni utilizzano un accentratore di log, un’infrastruttura dedicata alle attività di “**logging & monitoring**”. I **SIEM** sono dei tool che mettono a disposizione delle compagnie analisi del log in real-time, di fatto garantendo un livello di protezione ottimale contro minacce interne/esterne.

I **SIEM** sono generalmente costituiti da un’architettura Client-Server, dove la parte client è svolta da un “agent”, ovvero un programma installabile su un end-point che permette la comunicazione e l’invio dei log dall’end-point al server centrale.

Tra i punti di forza di un SIEM troviamo:

* **La capacità di ricevere in ingresso i log da diverse sorgenti** come Firewall, Proxy, sistemi e altro ancora, di fatto estendendo la visibilità del SIEM su tutti gli asset aziendali.
* **La capacità di correlazione dei dati tra diverse fonti.**
* **La capacità di monitoraggio real-time su tutti gli asset aziendali.**
* **La possibilità di definire preventivamente degli alert configurabili.** Ovvero, si potrebbe creare una policy di sicurezza per allertare il responsabile di un dato sistema, qualora fossero evidenziati accessi anomali alla macchina.

**SOAR:** il SOAR (**Security orchestration, automation and response**) può essere visto come un complemento ad un sistema SIEM. Mentre il SIEM si focalizza sul salvataggio ed il monitoraggio degli eventi di sicurezza, il SOAR aggiunge delle funzionalità di risposta automatica a determinati eventi, aggiungendo “**workflow**” (flussi di lavoro) complessi ed automatizzati.

Generalmente un SOAR è costituito da tre componenti principali:

* **Gestore delle vulnerabilità e delle minacce:** include e supporta workflow per tool quali Vulnerability Scanner, tool di reportistica e collaborazione.
* **Gestore delle risposte agli incidenti:** include i framework ed i tool per condurre l’analisi post-incidente di sicurezza end-to-end, ovvero dal momento in cui si verifica l’incidente fino al completo ripristino dei sistemi.
* **Gestore dell’automazione delle Security Operations:** il modulo che si occupa di tutta la parte di gestione e correlazione dei tool di sicurezza integrati con il SOAR.

Giorno 2- Business continuity & disaster recovery

**1. Introduzione**

Nonostante le misure di sicurezza, alcuni eventi esterni possono impattare negativamente sulla sicurezza delle compagnie, come può essere un evento catastrofico oppure un attacco.

Le compagnie resilienti predispongono di conseguenza piani e procedure per ridurre gli effetti dell’evento ed assicureare la continuità operativa, queste pratiche prendono il nome di “**business continuity plan**” e “**disaster recovery**”.

**2. Business continuity plan (BCP)**

Il “**business continuity plan”, piano per la continuità del business**, ha lo scopo principale di dettagliare la policy e le procedure per minimizzare gli impatti negativi sull’operatività di una compagnia a valle di un evento catastrofico/attacco, e ad assicurare la continuità delle operazioni svolte dalla compagnia anche in situazioni di emergenza.

Esempio: ospedale che eroga servizi indispensabili per la comunità e la salute del cittadino. Cosa succede se manca l’elettricità in tutta la città?

L’ospedale non può smettere di funzionare e qui viene in aiuto la pianificazione strategica preventiva della **business continuity**, che dettaglierà come gestire la casistica (esempio: tramite l’installazione preventiva di generatori autonomi ed indipendenti).

Il **“business continuity plan” (BCP)** si compone di 4 step principali:

* Pianificazione e scopo
* Business impact assessment (**BIA**), ovvero valutazione degli impatti sul business
* Business planning, ovvero piano di continuità operativa
* Approvazione ed implementazione
* **Pianificazione e scopo**

Come ogni pianificazione di business formale, lo sviluppo del BCP richiede un approccio strutturato e l’utilizzo di una metodologia comprovata. In questa fase è necessario:

* **Un’analisi strutturata dell’organizzazione e del business dell’organizzazione:** un’analisi strutturata dell’organizzazione e del business è il primo passo nella stesura di un piano di continuità. In questa fase lo scopo è quello di dettagliare e “mappare” i dipartimenti interni di una compagnia e gli individui con i servizi critici erogati dalla compagnia stessa. Infatti, in ottica di evento catastrofico, un piano d continuità ben strutturato dovrà come prima priorità ridurre gli impatti su quelli che sono i “servizi core”, ovvero i servizi principali erogati dalla compagnia. Per l’implementazione delle “**remediation action**” si riprende anche in questo contesto il concetto di “**priorità**”: gli asset critici, relativi al business hanno sempre la priorità.
* **La creazione di un team/ gruppo di lavoro responsabile del BPC che deve essere approvato dai dirigenti della compagnia stessa:** il secondo step nello sviluppo di un piano d’azione per la continuità del business è l’identificazione delle persone responsabili del business continuity plan (BCP). Questa fase è molto importante, in quanto bisogna che tutti i dipartimenti di una compagnia siano consapevoli dell’esistenza di un piano di continuità. Pertanto, nella pianificazione del team di lavoro bisognerà includere:
  + **Un rappresentante di ogni dipartimento dell’organizzazione che si occupa di erogare servizi critici.**
  + **un esperto di servizi IT (Information Technology)** **con competenze tecniche nelle aree coperte del BCP.**
  + **Un membro del team di Cyber Security,** che abbia competenze del processo BCP.
  + **Un membro del team di sicurezza fisica**
  + **Membri del team legale,** che abbiano competenze sulle regolamentazioni, leggi e contratti in essere.
  + **Membri del team delle risorse umane (HR- human resources),** per la gestione di eventuali impatti sullo staff, o su impiegati
  + **Un rappresentante dei dirigenti che abbia potere decisionale,** al fine di definire la priorità e allocare eventualmente risorse.
* **Una valutazione delle risorse ed asset disponibili che saranno incluse nelle attività di business continuity:** una volta che il team responsabile del BCP è stato definito, è il momento di definire le risorse richieste dal BCP. Si possono definire le risorse definite per le tre fasi di seguito del BCP:
  + **Sviluppo del BCP**: per lo sviluppo del piano di continuità le risorse coinvolte e di conseguenza l’effort (il costo) è imputabile a capitale umano come il team coinvolto nel processo di BCP ed eventualmente il costo dello staff esterno richiesto a supporto (se necessario).
  + **Test, manutenzione e training per gli impiegati:** il BCP deve essere testato, manutenuto, ma soprattutto bisogna organizzare delle sessioni di training/lezioni per gli impiegati al fine di mostrare il funzionamento di BCP. Pertanto, l’effort richiesto da questa fase, oltre al capitale umano, è anche in parte imputabile a costi software/hardware da mettere a disposizione soprattutto per le fasi di training degli impiegati.
  + **Implementazione del BCP:** infine, in caso di disastro, il BCP deve essere attuato il che richiede non solo capitale umano, ma anche un uso di risorse e mezzi. In questa fase, è molto probabile che per un periodo limitato una buona porzione della compagnia sia impegnata nell’implementazione del piano di continuità. Di conseguenza, bisogna avere particolare cautela nell’utilizzo del piano di continuità, valutando preventivamente se la situazione di disastro può essere tenuta sotto controllo diversamente.

In linea di massima la maggior parte dell’effort per le attività relative al BCP sono imputabili a capitale umano, con una porzione minore dedicata a risorse quali software ed hardware per garantire continuità dei servizi.

* + **Un’analisi delle leggi e regolamentazioni che la compagnia deve rispettare. Ad esempio, potrebbero essere in vigore delle leggi che stabiliscono quali servizi devono essere sempre erogati anche in situazioni critiche di una data compagnia:** capita frequentemente, che le compagnie sono in qualche molto legate a leggi statali o regolamentazioni che governano l’implementazione dei piani di continuità. Questo succede spesso nel mercato del “**Financial Services**”, ovvero il mercato di quelle compagnie che erogano servizi finanziari come banche e assicurazioni. In questi casi, le regolamentazioni pongono dei limiti o degli obblighi nello sviluppo dei piani di continuità operativa, ed è di conseguenza fondamentale capire il contesto giuridico nel quale si posiziona la compagnia al fine di sviluppare un piano che sia in linea con le leggi e le regolamentazioni in vigore.
* **Business impact analysis (BIA):**

Una volta completato il primo step della pianificazione, bisogna affrontare il **Business Impact analysis (BIA)**, ovvero l’analisi degli impatti di determinate minacce sul business. Il BIA ha lo scopo principale di **identificare le risorse critiche di una compagnia e le potenziali minacce alle quali esse sono esposte.** Inoltre, il BIA ha lo scopo di misurare la probabilità che tali minacce possano verificarsi e l’impatto che esse potrebbero avere sul business. Il BIA e conseguentemente la sua “misurazione” può seguire due approcci:

* + - **Qualitativo:** per il calcolo degli impatti di determinate minacce sul business NON si prendono in considerazione parametri misurabili, o numerici, ma bensì l’analisi è guidata da fattori non numerici.
    - **Quantitativo:** il calcolo degli impatti sul business prende in considerazione solamente parametri numerici o quantificabili con un numero.
  + **Identificazione delle priorità:** il primo task da eseguire quando ci si prepara ad affrontare un BIA è l’**identificazione delle priorità del business.** Questo fattore dipende ovviamente da quello che è lo scopo principale, o il business principale della compagnia.
    - da un punto di vista **qualitativo**, si potrebbero identificare le priorità in base alla loro criticità relativamente al business, dove agli asset a supporto del business viene assegnata una priorità superiore.
    - Da un punto di vista **quantitativo**, si potrebbe invece creare una lista contenente tutti gli asset della compagnia ed assegnare ad ognuno di essi un valore monetario, chiamato “asset value”(AV) e successivamente assegnare una priorità in base al valore.

All’interno di questa fase si definiscono altri due valori quantitativi:

* **Maximum tolerable downtime (MTD):** definito come il limite massimo di tempo durante il quale un business può non essere operativo senza causare danni irreparabili al business stesso.
* **Recovery time objective (RTO):** definito come l’ammontare di tempo necessario a recuperare un sistema o una funzionalità di esso in caso di disastro.

Lo scopo del BCP è di assicurare che **RTO<= MTD**, ovvero che il tempo per recuperare un sistema o una funzionalità critica in caso di disastro sia minore del tempo limite “sopportabile” dal business, e superato il quale si avrebbero conseguenze permanenti sul business stesso.

* **Identificazione dei rischi:** una volta completata la fase di identificazione delle priorità, bisogna stimare il rischio che impatterebbe l’organizzazione in caso di disastro. Possiamo dividere i rischi in due grosse categorie:
  + **Disastri naturali:** ricadono all’interno di questa categoria tutti questi fenomeni che non sono causati direttamente dall’uomo in prima persona, come ad esempio terremoti, maremoti, valanghe, eruzioni vulcaniche.
  + **Disastri causati dall’uomo:** in maniera complementare sono inclusi nei disastri causati dall’uomo tutti quei fenomeni che vedono l’uomo commettere un’azione in prima persona come atti terroristici, esplosioni ecc.
* **Valutazione della probabilità:** una volta identificati i rischi che possono impattare sull’organizzazione, ad ognuno di essi si associa la probabilità che l’evento si verifichi. Se la probabilità è stimata in numero di volte che l’evento si è verificato nel corso di un anno, si parla di “**annualized rate of occurence**” (ARO), ovvero **tasso annuale di occorrenza.** I dati storici e le statistiche messe a disposizione degli enti pubblici possono sicuramente supportare la valutazione delle probabilità per quanto riguarda i disastri naturali.
* **Valutazione degli impatti:** a valle dell’identificazione dei rischi e delle probabilità che essi si verifichino, si può procedere con la fase di valutazione degli impatti. Il risultato della fase di valutazione degli impatti è una misura qualitativa (basso, medio, alto) o quantitativa (e quindi espressa in forma monetaria) degli impatti su business legati ad un determinato evento.
  + **Da un punto di vista quantitativo**: si assegna ad ogni asset quello che viene chiamato “**exposure factor**” (EF), misurato come la percentuale di asset che verrebbe impattato a seguito del verificarsi di un determinato evento, e si introduce il concetto di “single loss expectancy” (SLE), che ci dà una misura monetaria della perdita che si subirebbe al verificarsi dell’evento, calcolato il prodotto tra il valore dell’asset (AV) e la percentuale impattata in caso di evento (EF):

**SLE = AV x EF**

Esempio pratico:

Ipotizziamo di essere il CEO di una compagnia. Possediamo un edificio che vale 500000 euro (asset value) e stimiano un exposure factor del 70% rispetto all’evento “incendio”, ovvero se dovesse mai capitare un incendio perderemmo il 70% dell’edificio.

Seguendo la precedente formula, si avrebbe un SLE= AV x EF= 500000 x 0,70= 350000

Se volessimo ora il valore della perdita subita in un arco di tempo di un anno, chiamato **ALE** (**annualized loss expectancy**), dovremmo moltiplicare il valore del SLE per il numero di volte stimato dell’evento in un anno (ARO)

**ALE = SLE x ARO**

**Ad esempio, stimando un incendio ogni 30 anni, quindi ARO= 0,03/anno, la perdita annuale al nostro edificio a causa di incendi è di 1050 euro/anno.**

**ALE= 350000 x 0,03 = 10500 euro**

Da un punto di vista qualitativo, bisognerebbe considerare tutti gli impatti “non numerici” sul business, come ad esempio:

* Pubblicità negativa (es. banca che non riesce ad assicurare servizio agli intestatari dei conti corrente);
* Sfiducia dei clienti;
* Responsabilità etica e sociale dell’organizzazione ecc.

A differenza dell’analisi quantitativa, l’analisi qualitativa non restituisce un numero in valuta, ma una stima degli impatti sul business di un dato evento.

* **Business continuity planning:** le prime due fasi del BCP si focalizzano sulla pianificazione del BCP e sull’identificazione delle priorità e dei rischi per il business. La fase del continuity planning ha invece lo scopo di sviluppare ed implementare una strategia per la riduzione dell’impatto dei rischi sugli asset protetti. Possiamo identificare all’interno della fase di continuity planning, le seguenti sottofasi:
  + **Sviluppo della strategia:** lo sviluppo della strategia è un’attività complementare all’identificazione delle priorità, discussa nella fase di BIA. Infatti, se nella BIA si identificano rischi ed asset prioritari, nella fase di sviluppo strategia si decidono i rischi che verranno gestiti all’interno del BCP. In questa fase il managenement deciderà quali rischi potrebbero essere accettabili, e quali invece no, quali rischi sono da evitare e quali da inserire all’interno del BCP.
  + **Stesura dei processi:** all’interno di questa fase vengono dettagliati i processi e le procedure da seguire per la salvaguardia degli asset critici: personale, edifici ed infrastrutture. È bene ricordare che le persone sono sempre “l’asset” più significativo di una compagnia e pertanto devono essere dettagliati i processi per assicurare l’incolumità durante un emergenza.
* **Approvazione ed implementazione:** una volta completate le fasi precedenti, è il momento di sottoporre il piano all’attenzione della dirigenza per revisione ed approvazione, prima di passare alla fase di implementazione, dove il team responsabile del BCP deve assicurarsi che tutte le risorse necessarie siano disponibili e che è stato organizzato, o erogato un piano di training per tutti gli impiegati che prendono attivamente parte al BCP. Infine, tutte le fasi precedenti devono essere ampiamente documentate e rese disponibili per eventuale consultazione da parte degli impiegati.

**3. Disaster recovery (DR)**

Abbiamo visto fin qui il BCP, che ha lo scopo di supportare le organizzazioni nella riduzione degli impatti sugli asset prioritari a valle di un evento critico. Il Disaster recovery planning (DRP) può essere visto come il complemento tecnico al BCP e, mentre da un lato il BCP copre le tematiche di governance, pianificazione e gestione, il disaster recovery planning include i controlli tecnici da implementare per la riduzione del rischio e per il recupero dei servizi a valle di un evento catastrofico. Insieme, il BCP ed il DRP, servono da guida durante i momenti di crisi o emergenza per recuperare l'operatività del business quanto prima così da impattare gli utenti fruitori del servizio quanto più lievemente possibile.

La tabella in calce include alcuni degli eventi catalogati come «disastri naturali» e «disastri causati dall'uomo», da considerare quando si pianifica un disaster recovery planning:

|  |  |
| --- | --- |
| DISASTRI NATURALI | DISASTRI CAUSATI DALL’UOMO |
|  |  |
| Terremoti | Atti di terrorismo |
| Inondazioni | Esplosioni |
| Temporali | Interruzioni di corrente |
| Maremoti | Guasti infrastrutturali o di rete |

Nello sviluppo di un piano di disaster recovery, vi sono dei ***documenti che devono essere presenti***:

* ***Executive summary***, ovvero un documento che andrà al management al cui interno sarà presente una vista globale sul piano di disaster recovery.
* ***Un documento tecnico*** per il personale IT responsabile dell'implementazione e della manutenzione dei sistemi.
* ***Un piano d'azione*** per tutte le persone ingaggiate nel piano di disaster recovery.
* ***Copie complete del piano di disaster recovery*** per i responsabili primari dell'implementazione e attuazione del piano.

***Tecniche e controlli*** utilizzati in fase di disaster recovery:

* **Resilienza dei sistemi**: i controlli tecnici che aumentano la resilienza di sistemi impattano positivamente sulla disponibilità di sistemi e servizi, uno dei principi cardine della triade CIA. Si definisce *resilienza di un sistema la sua capacità di far fronte a determinati eventi critici*. L'obiettivo primario dei controlli in esame è di eliminare i cosiddetti «single point of failure» (SPOF), intesi come quei componenti del sistema che possono causare anomalie o cessazione dell'intero sistema.
* **Tolleranza agli errori**: la tolleranza agli errori, chiamata in inglese «fault tolerance», è la capacità di un sistema di continuare ad essere operativo nonostante un errore. Essa si può aumentare *aggiungendo ad esempio componenti ridondanti* all'interno dell'architettura, come ad esempio un disco in più per il salvataggio dei dati.
* **Protezione dei dischi**: la tolleranza agli errori e la resilienza di un sistema possono essere rinforzate come abbiamo visto aggiungendo ridondanza, *per esempio eliminando SPOF causati da dischi rigidi unici*, tramite l'inserimento di dischi aggiuntivi secondo la configurazione RAID. Un vettore RAID infatti, include 2 o più dischi per garantire continuità di servizio anche quando uno dei dischi non risulta più disponibile.
* **Configurazioni RAID**: tra le configurazioni RAID più comuni troviamo:

1. **RAID-1**: questa configurazione utilizza 2 dischi, entrambi contenenti gli stessi dati. Se uno dei due dischi smette di funzionare, il sistema non è impattato, in quanto il secondo disco ne assicura l'operativita.
2. **RAID-5**: questa configurazione utilizza 3 o più dischi, e tramite un tecnicismo chiamato «parità» implementa una soluzione che consente al sistema di funzionare anche se uno qualsiasi dei dischi smette di funzionare. La «parità» infatti rende possibile recuperare i dati sul disco non funzionante cosi da garantire continuità di servizio.

Il ***concetto di ridondanza*** può essere applicato a tutti gli asset critici, dove la ridondanza può dare un valore aggiunto al sistema. Quando parliamo di server, il concetto di ridondanza trova applicazione pratica nel «**failover cluster**», dove con cluster si intende un gruppo di computer che svolge generalmente lo stesso ruolo e che sono tra di loro sincronizzati, i singoli computer vengono chiamati anche nodi del cluster.

Il «failover cluster» include due o più server e permette 'operatività dell'intero sistema anche a fronte di un errore su uno dei due server. Quando il server attivo smette di funzionare, il secondo server prende il suo posto come server attivo tramite un processo che viene chiamato appunto «failover».

Immagine che contiene testo

Descrizione generata automaticamente

Il concetto di «failover cluster» può essere applicato a vari tipi di server ad esempio: web server che erogano servizi su internet, application server, database e cosi via.

* **Disponibilità elettrica**: la tolleranza agli errori può essere applicata anche ai sistemi elettrici mediante l'utilizzo di generatori di corrente autonomi. Questi sistemi sono fondamentali per assicurare l'erogazione di elettricità anche in caso di disastro.
* **Backup**: un piano di disaster recovery deve assolutamente prevedere una strategia preventiva di backup. Ovvero una strategia di come copiare i dati, i sistemi e le configurazioni attualmente in produzione al fine di recuperare l'operatività a fronte di un disastro. Tra le strategie di backup troviamo:

1. **Full backup**: in una strategia di full backup i dati e le configurazioni di un sistema vengono copiate completamente. Può essere utilizzata in contesti con alta disponibilità di spazio per salvataggio dei dati. Non è una strategia di ottimizzazione spazio.
2. **Incremental backup**: la strategia del backup «incrementale», invece, utilizza un approccio diverso. Solo i dati che sono stati modificati dall'ultimo backup incrementale vengono copiati e salvati.
3. **Differential backup**: solo i dati che sono stati modificati dall'ultimo full backup vengono copiati e salvati sul mezzo di salvataggio scelto.

* **Migration to cloud**: negli ultimi anni si sta diffondendo sempre più il fenomeno tecnologico della migrazione dei server da on-premise (utilizzo di server fisici) al cloud. Ad oggi, ci sono molti cloud service provider (CSP) come Google, Amazon, Microsoft che mettono a disposizione servizi in Cloud per le compagnie. Di consequenza la stesura di un piano di disaster recovery deve anche considerare l'approccio adottato. Una compagnia potrebbe avere una parte dell'infrastruttura nei propri datacenter e quindi gestirne la sicurezza e il piano di disastro ed una parte completamente demandata al cloud provider, che in tale caso sarebbe anche parte responsabile delle politiche di disaster recovery.

Per quanto riguarda le ***metodologie di disaster recovery***, possiamo identificare quattro diversi scenari:

* **Cold site**: questa modalità di ripristino prevede un secondo sito (una seconda sede) attrezzata con gli strumenti e le dotazioni per l'operatività del business da attivare a valle del disastro. Prevede dei costi di gestione sicuramente minori rispetto ad altre soluzioni, ma tra i contro troviamo i tempi di recupero piuttosto alti e il disallineamento dei dati rispetto al sistema primario.
* **Hot site**: al contrario del «cold site», «l'hot site» è un sito sempre attivo, e dunque dispone dei dati sempre aggiornati. Lo spostamento da un sito primario ad un sito secondario in caso di disastro non comporta discontinuità di servizio. Tuttavia, tra i contro troviamo gli alti costi di gestione.
* **Virtualizzazione**: un altro approccio piuttosto comune nelle compagnie è l'adozione di ambienti virtuali in sostituzione ai server fisici. I motori di virtualizzazione mettono a disposizione delle compagnie tecnologie per replicare completamente l'ambiente informatico virtualizzato quali server, sistemi operativi, dischi per salvataggio di dati, applicazioni, database e così via.
* **Disaster recovery as a service (DRaaS)**: i cloud provider mettono a disposizione delle compagnie un modello di cloud chiamato «disaster recovery as a service», dove il cloud provider mette a disposizione un'infrastruttura in cloud che viene immediatamente attivata in caso di disastro sul sito primario della compagnia. Tra gli svantaggi troviamo i tempi di latenza per lo «switch» dal sito primario al sito secondario. Tuttavia, in termini di ottimizzazione budget è spesso la soluzione migliore considerato che si pagherebbe il servizio solo in caso di effettivo utilizzo.

**Link utili:**

* <https://www.juniper.net/it/it/research-topics/what-is-802-1x-network-access-control.html>