Co-funded by the Erasmus+ Programme of the European Union

Moduli di formazione InCyT

Sicurezza delle informazioni per manager **N. unità (modulo) e n. settimana: Unità-2 Settimana-4** **Nome dell'unità (modulo): Gestione della sicurezza delle informazioni -2**	
Attività di apprendimento	❑ **Webinar** ❑ **Esercizi** ❑ **Workshop** ❑ **Presentazione** ❑ **Altro** Webinar in streaming, testo, esercizi di autovalutazione, esercizi con risposte su forum di discussione e discussione con il formatore/mentore.
Apprendimento responsabile	• Fatma Gökdemir • Ali Gökdemir
Obiettivi dell'attività di apprendimento	1. Valutazione delle minacce e delle vulnerabilità 2. Gestione delle minacce e delle vulnerabilità 3. Tipi di valutazione della vulnerabilità 4. Continuità delle operazioni informatiche 5. Attività informatica 6. Valutazione dell'efficacia delle politiche di sicurezza informatica
Competenze da acquisire	• IS 1 • IS 3 • SM 5
Durata dell'attività di apprendimento	2 settimane
Apprendimento requisiti	***Cosa serve?*** • Competenze informa intermedie

Co-funded by the
Erasmus+ Programme
of the European Union

Brevi informazioni sul modulo

Descrizione
La gestione degli asset occupa un posto importante nell'ambito del Sistema di gestione della sicurezza delle informazioni ISO 27001. In effetti, l'identificazione e la classificazione degli asset informativi è una delle prime fasi dell'impostazione della sicurezza delle informazioni. L'identificazione e l'assegnazione del valore agli asset di un'organizzazione è una fase fondamentale del processo di analisi dei rischi. Per assegnare il valore agli asset si prepara un inventario degli asset. Prima dell'inventario dei beni è necessario condurre uno studio esplorativo su tutti i dipendenti. Con questo studio, l'inventario degli asset del reparto viene esplorato ed elencato con i possibili rischi e il grado di riservatezza. L'inventario dei beni deve essere effettuato uno per uno sulla base dei processi coperti. Durante la preparazione dell'inventario degli asset, vengono determinati il gruppo di asset, l'ambiente in cui si trova l'asset specificato, il codice di classificazione e viene calcolato il valore dell'asset (riservatezza, integrità, accessibilità). In base al risultato del calcolo, si determina lo stato di priorità e si prendono decisioni di intervento. Al termine del lavoro di inventario degli asset, viene preparato un elenco dettagliato degli inventari software-hardware rilevati. Le condizioni/controlli relativi alla gestione degli asset nella norma ISO27001 sono raccolte nell'Allegato A.8. In questo modulo esamineremo i termini per la responsabilità degli asset definiti in A.8.1.

Contenuto del materiale didattico

1. Valutare la gestione della sicurezza delle informazioni

Nella prima fase della gestione del patrimonio, sarebbe utile innanzitutto rivelare ed elencare i beni di cui disponiamo. È necessario innanzitutto conoscere ciò che un'istituzione possiede o non possiede. Poi occorre definirne la proprietà. Nessuna attività o transazione dovrebbe essere lasciata incustodita. Infine, si devono determinare le regole per l'utilizzo di questi beni.

Per i dettagli dell'argomento, è necessario esaminare la norma ISO27002. Le aspettative relative alla gestione delle risorse nella norma ISO27002 sono incluse nell'ottavo articolo della norma:

Gestione delle attività e responsabilità per le attività

Scopo: identificare gli asset dell'organizzazione e definire le responsabilità di protezione appropriate.

1. Inventario dei beni

Controllo: I beni relativi alle informazioni e alle strutture di elaborazione delle informazioni devono essere identificati e deve essere redatto e mantenuto un inventario di tali beni.

Guida all'applicazione: Un'organizzazione deve identificare le risorse rilevanti nel ciclo di vita delle informazioni e documentarne l'importanza. Il ciclo di vita delle informazioni deve comprendere la creazione, l'elaborazione, l'archiviazione, la trasmissione, la cancellazione e la distruzione. La documentazione deve essere mantenuta in conformità con gli inventari esistenti o in modo specifico.

Inventario dei beni; deve essere aggiornato, coerente, accurato e compatibile con altri inventari.

La proprietà del bene deve essere assegnata per ogni bene identificato (cfr. articolo 2) e deve essere determinata la sua classe.

Altre informazioni: L'inventario dei beni contribuisce a fornire una protezione efficace e può essere necessario anche per altri scopi, come la salute e la sicurezza, l'assicurazione o motivi finanziari (gestione dei beni).

Lo standard ISO/IEC 27005[11] fornisce esempi di asset che possono essere presi in considerazione dall'organizzazione nell'identificazione degli asset. Il processo di compilazione dell'inventario degli asset è un importante prerequisito per la gestione del rischio (vedi ISO/IEC 27000 e ISO/IEC 27005[11]).

2. Proprietà dei beni

Controllo: Per tutti i beni in inventario devono essere assegnati i proprietari.

Guida all'applicazione: Possono essere designati come proprietari dell'asset gli individui e le altre entità con responsabilità di gestione approvata per il ciclo di vita dell'asset.

Spesso si utilizza un processo per garantire che la proprietà delle risorse sia determinata in modo tempestivo. La proprietà deve essere determinata quando le risorse vengono create o trasferite all'organizzazione. Il proprietario dell'asset deve essere responsabile della corretta gestione dell'asset per tutto il suo ciclo di vita.

Il proprietario del bene deve:

a) assicurare la registrazione dell'inventario dei beni,

b) assicurare che le attività siano classificate e protette in modo appropriato,

c) definire e rivedere periodicamente le restrizioni di accesso alle attività significative e la loro classificazione, tenendo conto della politica di controllo degli accessi applicabile,

d) garantire che vengano intraprese azioni appropriate per la cancellazione o la distruzione degli asset.

Altre informazioni: Può essere un individuo o un'entità con l'approvazione per la responsabilità gestionale di controllare un asset per tutto il suo ciclo di vita. Il proprietario identificato non ha alcun interesse di proprietà nell'asset.

I compiti di routine possono essere delegati (ad esempio, un custode che si occupa di un bene su base giornaliera), ma la responsabilità resta al proprietario del bene.

L'identificazione di gruppi di asset all'interno di sistemi informativi complessi può essere utile per fornire funzioni congiunte. In questo caso, il proprietario del servizio è responsabile dell'erogazione del servizio, compreso il funzionamento degli asset.

3. Uso accettabile delle risorse

Controllo: *Le regole* relative all'uso accettabile delle informazioni e delle risorse relative alle strutture di elaborazione delle informazioni devono essere determinate, documentate e attuate.

Guida all'applicazione: I dipendenti e gli utenti esterni che utilizzano o hanno accesso alle risorse dell'organizzazione devono essere informati dei requisiti di sicurezza delle risorse dell'organizzazione associate alle strutture e alle risorse informatiche e di elaborazione delle

informazioni. Questi utenti devono essere responsabili dell'uso di tutte le risorse di elaborazione delle informazioni e di qualsiasi uso che avvenga sotto la loro responsabilità.

4. Ripristino delle attività

Controllo: Tutti i dipendenti e gli utenti di soggetti esterni devono restituire tutti i beni aziendali in loro possesso al termine del rapporto di lavoro, del contratto o dell'accordo.

Guida all'applicazione: Il processo di cessazione deve essere formulato in modo da includere la restituzione della proprietà di tutti i beni fisici ed elettronici dell'organizzazione precedentemente concessi.

Quando un dipendente o un utente esterno acquista o utilizza le apparecchiature dell'organizzazione, vengono seguite procedure per garantire che tutte le informazioni rilevanti vengano trasferite all'organizzazione e cancellate in modo sicuro dalle apparecchiature.

Se un dipendente o un utente esterno dispone di informazioni importanti per le operazioni in corso, queste devono essere documentate e trasferite all'organizzazione.

Durante il periodo di preavviso di licenziamento, l'organizzazione deve controllare la copia non autorizzata di informazioni correlate, come la proprietà intellettuale, da parte dei dipendenti e degli appaltatori licenziati.

2. Valutazione e gestione delle minacce e delle vulnerabilità

Quasi tutte le organizzazioni hanno beni sensibili e preziosi che devono essere protetti. Tuttavia, non tutte le organizzazioni dispongono di una strategia completa e ponderata per la protezione di questi beni. Nella cybersecurity, le strategie di gestione delle vulnerabilità sono il fondamento di una difesa forte. In genere, le strategie di gestione delle vulnerabilità sono progettate per aiutare i sistemi, le reti, le applicazioni e così via di un'organizzazione. Queste vulnerabilità vengono quindi identificate, valutate e risolte il prima possibile.

Le minacce e le tendenze in materia di sicurezza sono in continua evoluzione e richiedono sforzi efficaci e preventivi per gestire le minacce e le vulnerabilità che potrebbero compromettere i vostri dati. Per identificare tutti i potenziali obiettivi di una violazione o di un attacco, è necessario innanzitutto mitigarne il rischio effettuando un inventario delle risorse. Gli obiettivi devono poi essere classificati e monitorati costantemente per individuare nuove potenziali vulnerabilità. A questo punto è necessario sviluppare e testare un modello di minaccia che identifichi gli asset più preziosi e ad alto rischio dell'organizzazione. Lo scopo principale del processo di verifica delle minacce e delle vulnerabilità (assessment) è quello di comprendere al meglio la criticità degli

asset, le vulnerabilità di tali asset e ridurre le misure necessarie per proteggere efficacemente tali asset.

2.1. La valutazione della vulnerabilità

La valutazione delle vulnerabilità è il processo di identificazione, individuazione, classificazione e prioritizzazione delle vulnerabilità nei sistemi informatici, nelle applicazioni e nelle infrastrutture di rete.

Le valutazioni di vulnerabilità forniscono inoltre a un'organizzazione le conoscenze, la consapevolezza e il background di rischio necessari per comprendere e rispondere alle minacce al proprio ambiente. Un processo di valutazione delle vulnerabilità mira a identificare le minacce e i rischi che esse comportano. Spesso prevede l'uso di strumenti di test automatizzati, come gli scanner di sicurezza di rete, i cui risultati sono elencati in un rapporto di valutazione delle vulnerabilità.

Le organizzazioni di qualsiasi dimensione, anche quelle individuali a maggior rischio di attacchi informatici, possono trarre vantaggio da una qualche forma di valutazione delle vulnerabilità, ma le grandi organizzazioni e altri tipi di organizzazioni esposte ad attacchi continui trarranno i maggiori benefici dall'analisi delle vulnerabilità.

Poiché le vulnerabilità possono consentire agli hacker di accedere ai sistemi e alle applicazioni IT, è fondamentale per le organizzazioni identificare e risolvere le vulnerabilità prima che vengano sfruttate. Una valutazione completa delle vulnerabilità, unita a un programma di gestione, può aiutare le aziende a migliorare la sicurezza dei loro sistemi.

2.2. L'importanza delle valutazioni di vulnerabilità

Per comprendere meglio l'importanza della valutazione della vulnerabilità, consideriamola attraverso gli occhi del proprietario di un immobile. Se possedete un edificio di valore, probabilmente adottate una serie di misure per proteggerlo: Lo sottoponete a manutenzione, lo assicurate, vi assicurate che le porte e le finestre siano chiuse a chiave e che gli allarmi siano attivati. Tutte queste misure possono essere definite come gestione del rischio per l'immobile e il suo contenuto.

Cosa succederebbe se poteste assumere qualcuno per testare e riferire sui vostri allarmi e sulle vostre difese esterne? Le vulnerabilità della sicurezza informatica vengono affrontate in modo simile. La gestione delle vulnerabilità è una strategia globale e continua, mentre le valutazioni

delle vulnerabilità sono uno strumento specifico utilizzato in questa strategia di gestione più ampia.

Una valutazione delle vulnerabilità fornisce a un'organizzazione informazioni dettagliate su eventuali punti deboli della sicurezza nel suo ambiente. Fornisce inoltre indicazioni su come valutare i rischi associati a tali punti deboli. Questo processo consente all'organizzazione di comprendere meglio le proprie risorse, le falle nella sicurezza e il rischio complessivo, riducendo la probabilità che un criminale informatico violi i sistemi e colga l'azienda di sorpresa.

2.3. Tipi di valutazione della vulnerabilità

Le valutazioni di vulnerabilità scoprono diverse vulnerabilità di sistema o di rete. Ciò significa che il processo di valutazione prevede l'utilizzo di una serie di strumenti, scanner e metodologie per identificare vulnerabilità, minacce e rischi.

Alcuni dei diversi tipi di scansioni di valutazione della vulnerabilità includono (Figura 1):

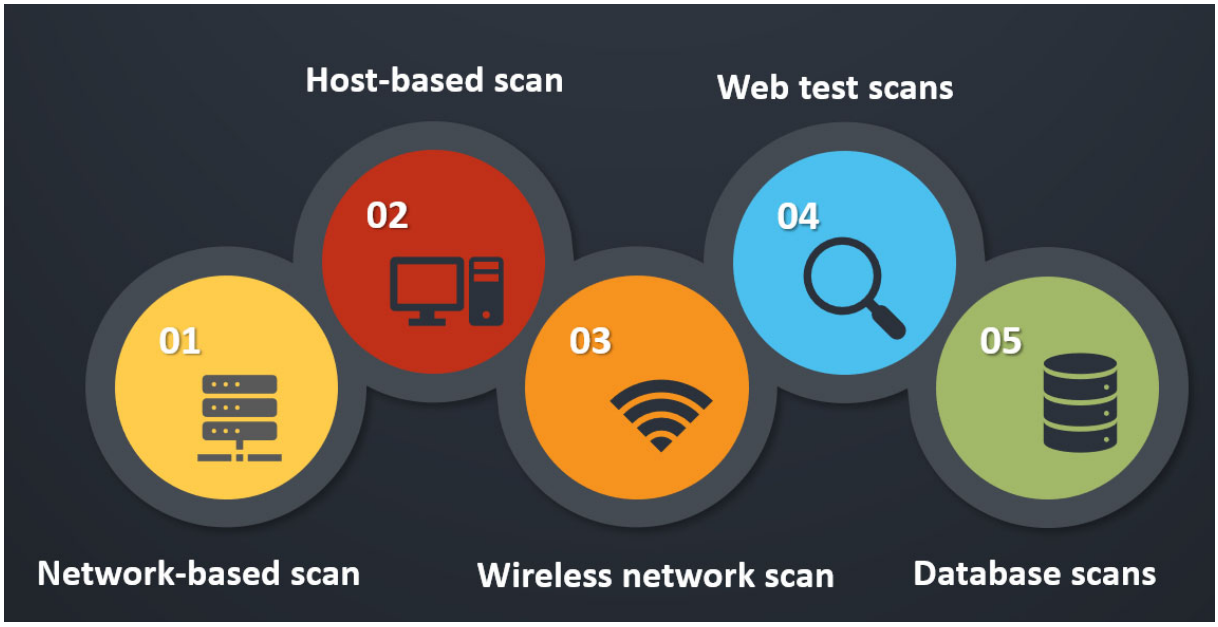

Figura 1. Tipi di valutazione della vulnerabilità

- **Le scansioni basate sulla rete** sono utilizzate per identificare potenziali attacchi alla sicurezza della rete. Questo tipo di scansione può anche rilevare sistemi vulnerabili su reti cablate o wireless.
- **Le scansioni basate su host** sono utilizzate per trovare e identificare le vulnerabilità nei server, nelle workstation o in altri host di rete. Questo tipo di scansione esamina solitamente porte e servizi, che possono essere visti anche nelle scansioni basate sulla

rete. Tuttavia, offre una maggiore visibilità sulle impostazioni di configurazione e sulla cronologia delle patch dei sistemi sottoposti a scansione, compresi i sistemi legacy.

- **Le scansioni delle reti** Wi-Fi di un'organizzazione si concentrano spesso sui punti di attacco dell'infrastruttura di rete wireless. Oltre a individuare i punti di accesso non autorizzati, la scansione della rete wireless può anche verificare che la rete aziendale sia configurata in modo sicuro.
- **Scansione Web di** siti di **test** per rilevare vulnerabilità software note e configurazioni errate in applicazioni, reti o applicazioni Web.
- **Le scansioni del database** possono identificare i punti deboli di un database per prevenire attacchi dannosi, come gli attacchi SQL injection.

2.4. Valutazioni di vulnerabilità e test di penetrazione

Una valutazione delle vulnerabilità spesso include una componente di penetration test per identificare le vulnerabilità nel personale, nelle procedure o nei processi di un'organizzazione. Le valutazioni delle vulnerabilità condividono molte delle stesse caratteristiche dei test di penetrazione, perché entrambe consentono alle organizzazioni di esaminare rigorosamente le proprie difese. Queste vulnerabilità non vengono normalmente rilevate dalle scansioni di rete o di sistema. Il processo viene talvolta definito Vulnerability Assessment/Penetration Testing (**VAPT**).

Tuttavia, il test di penetrazione non è sufficiente come valutazione completa della vulnerabilità ed è in realtà un processo separato. Una valutazione della vulnerabilità mira a scoprire le vulnerabilità di una rete e a suggerire una mitigazione o un rimedio appropriato per ridurre o eliminare i rischi.

Una valutazione delle vulnerabilità utilizza strumenti di scansione automatica della sicurezza di rete. I risultati sono elencati nel rapporto di valutazione delle vulnerabilità, che si concentra sul fornire alle organizzazioni un elenco di vulnerabilità da correggere. Tuttavia, questo viene fatto senza valutare obiettivi o scenari di attacco specifici.

Le organizzazioni devono eseguire regolarmente test di vulnerabilità per garantire la sicurezza delle loro reti, soprattutto quando vengono apportate modifiche. Ad esempio, i test dovrebbero essere eseguiti quando si aggiungono servizi, si installano nuove apparecchiature o si aprono porte.

I test di penetrazione, invece, consistono nell'identificazione delle vulnerabilità di una rete e nel tentativo di sfruttarle per attaccare il sistema. Anche se a volte vengono eseguiti insieme alle valutazioni di vulnerabilità, lo scopo principale dei test di penetrazione è quello di verificare

l'effettiva esistenza di una vulnerabilità. Inoltre, i test di penetrazione cercano di dimostrare che lo sfruttamento di una vulnerabilità può danneggiare l'applicazione o la rete.

Mentre una valutazione delle vulnerabilità è solitamente automatizzata per coprire un'ampia gamma di vulnerabilità non patchate, i test di penetrazione spesso combinano tecniche automatizzate e manuali, aiutando i tester a indagare ulteriormente sulle vulnerabilità e a sfruttarle per ottenere l'accesso alla rete in un ambiente controllato.

2.5. Gestione delle vulnerabilità e dei rischi

Mentre la gestione delle vulnerabilità è un processo continuo di gestione delle vulnerabilità, la gestione del rischio ha una visione più ampia di tutto ciò che può rappresentare una minaccia per un'organizzazione. Una solida strategia di gestione del rischio consente di identificare, analizzare e mitigare efficacemente i rischi. Questo approccio aiuta le organizzazioni a comprendere non solo le vulnerabilità esistenti, ma anche l'entità dei danni che possono verificarsi in caso di abuso. Una valutazione dei rischi e delle vulnerabilità condotta nell'ambito della gestione del rischio può fornire una prospettiva particolarmente ampia sulla solidità della postura di sicurezza di un'organizzazione.

3. Continuità delle operazioni informatiche

Per aumentare la resilienza contro le minacce di malware distruttivo è necessario conoscere la postura di sicurezza attuale, pianificare e coordinare le azioni difensive principali e allineare correttamente le risorse difensive chiave.

Anche gli incidenti informatici hanno messo a dura prova gli sforzi di pianificazione della continuità di base. Sebbene molte giurisdizioni dispongano di attrezzature e strategie per identificare, rilevare e proteggere dagli attacchi informatici, molte meno hanno affrontato la dura realtà della continuità delle operazioni in caso di attacco reale. Quando i cyberattacchi colpiscono, molte giurisdizioni colpite scoprono che i loro piani COOP di base non reggono. Sebbene i piani siano adeguati per la transizione verso un luogo di lavoro alternativo, hanno molto meno da offrire quando si tratta di lavorare senza accesso ai sistemi e ai dati di cui il personale ha bisogno per svolgere le proprie funzioni essenziali. I piani esistenti mancano anche della specificità necessaria per guidare la risposta, e i principali stakeholder, come i membri del personale IT, spesso non sono integrati nelle strutture di risposta. Inoltre, i piani non vengono testati con un'esercitazione o un incidente reale.

I piani COOP tradizionali non riescono a garantire la continuità durante gli incidenti informatici in diversi modi (Figura 2):

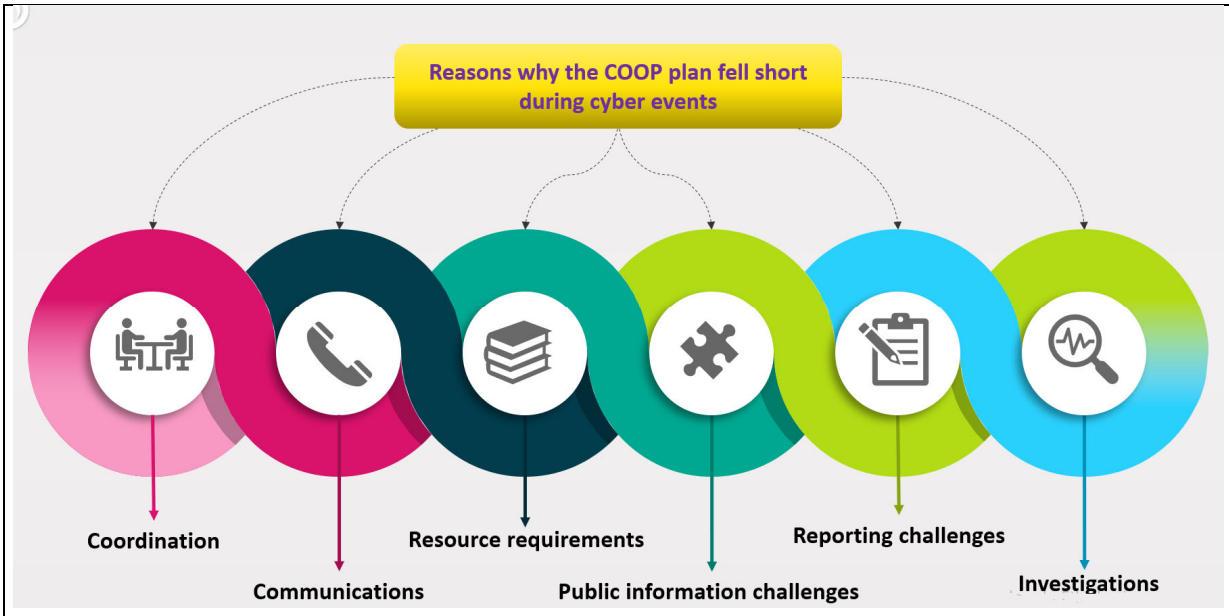

Figura 2. Motivi per cui i piani COOP sono insufficienti per la continuità durante gli eventi informatici

Coordinamento: chi è coinvolto nel processo decisionale quando si tratta di ransomware, decisioni di mettere offline i sistemi e decisioni di attivare il Centro operativo di emergenza della giurisdizione. Inoltre, la maggior parte delle amministrazioni locali non ha chiari livelli di escalation per un attacco, né le azioni associate per ciascun livello. Anche la leadership della risposta e il personale possono essere poco chiari; le competenze necessarie per guidare una comunità attraverso un incidente informatico sono diverse da quelle necessarie per un evento meteorologico estremo.

Comunicazioni: includere il modo in cui i manager locali forniranno rapidamente informazioni al personale quando un attacco informatico ha gravemente compromesso le comunicazioni. Questo include sia le comunicazioni immediate che spiegano cosa fare quando inizia l'attacco, sia le comunicazioni continue, come ad esempio le modalità di erogazione degli stipendi entro il giorno di paga. Entrambe le cose sono fondamentali per la risposta, ma potrebbero dover essere trasmesse senza il beneficio dei tipici sistemi di comunicazione di emergenza.

Requisiti delle risorse: Che possono essere molto diverse da quelle di una risposta più tradizionale. Ad esempio, il personale potrebbe aver bisogno di computer puliti, server puliti, stampanti locali e persino fax e carta. È importante notare che il fabbisogno di personale può aumentare ancora di più durante il recupero rispetto alla risposta, poiché i dipartimenti e le agenzie lottano per replicare i dati mancanti o sospetti.

Sfide per l'informazione pubblica: Tra cui funzionari dell'informazione pubblica con poca o nessuna formazione o esperienza in materia di cybersecurity, mancanza di messaggi prestabiliti e disaccordo sul momento in cui le informazioni sull'attacco devono essere rese pubbliche. Fornire informazioni al pubblico è fondamentale perché i cittadini si preoccupano dei loro dati e dell'affidabilità di sistemi democratici fondamentali come il voto e la giustizia.

Problemi di segnalazione: Questo può ritardare la risposta, poiché le interruzioni non vengono segnalate in modo coerente, lasciando i reparti IT senza il quadro operativo comune necessario per identificare rapidamente un attacco. Inoltre, le linee di segnalazione sono spesso poco chiare e poche persone al di fuori dell'IT capiscono quali sistemi sono collegati sia all'interno che all'esterno della giurisdizione.

Indagini: Si tratta di una scatola nera per molte località. Il coinvolgimento di una o più organizzazioni federali e i limiti che le indagini pongono agli sforzi di bonifica non sono ben compresi o pianificati. Questo rende estremamente difficile la pianificazione della continuità, perché c'è incertezza su come e quando la bonifica possa iniziare.

3.1. Priorità per un'azione immediata con una difesa coordinata

1) Sviluppare una "Go Bag" informatica con le procedure e le informazioni essenziali.

- Assemblare kit di strumenti mobili per la sicurezza informatica che includano procedure per stabilire, implementare, mantenere e consentire la continuazione di TTP resilienti dal punto di vista informatico all'interno di una struttura designata COOP.

2) Sviluppare, testare e convalidare playbook, ruoli, responsabilità e strumenti.

- Designare ruoli informatici specifici, responsabilità associate e strumenti informatici che possono essere impiegati per garantire l'attuazione della COOP informatica.
- Definire le rappresentazioni standard della COOP cibernetica per l'esecuzione individuale o da parte di una squadra cibernetica, utilizzando strumenti cibernetici "Go Bag" e TTP elastici.
- Condurre diversi tipi di esercitazioni informatiche (ad esempio, esercitazioni di tipo mini-table top) utilizzando la "Go Bag" informatica e il libro dei giochi.

3) Definire i processi di collaborazione e acquisire strumenti per i difensori informatici e i risponditori agli incidenti.

- Garantire che i processi COOP informatici, sia mobili che fissi, includano la comunicazione e il coordinamento per promuovere un'adeguata gestione delle difese informatiche, la sinergia

tra tutte le attività di risposta e la riduzione delle lacune nella copertura della sicurezza durante le attività di recupero.

Sebbene i piani COOP di base abbiano favorito la preparazione locale per molte delle minacce che le giurisdizioni si trovano ad affrontare, essi risultano insufficienti in situazioni che creano un ambiente molto diverso dalla norma. Mentre i dipartimenti informatici di tutto il Paese continuano a rendere i sistemi e i dati il più sicuri possibile, spetta ai gestori delle emergenze sforzare la propria immaginazione e pianificare gli attacchi informatici che hanno un grave impatto sui sistemi e sui dati critici.

3.2. Priorità di azione immediata con il riallineamento

1) Identificare le dipendenze delle missioni e delle funzioni aziendali dalle risorse informatiche.

- Determinare gli scopi della missione delle risorse, in modo da identificare ed eliminare gli usi che aumentano il rischio senza alcun beneficio corrispondente per la missione.
    - Identificare e rimuovere o sostituire le connessioni e i flussi di dati per i quali i rischi superano i benefici.
- Considerare le interdipendenze tra le funzioni aziendali e le organizzazioni di missione e non, che condividono ruoli critici nella fornitura delle capacità NEF.
    - Riallocare le risorse o riassegnare le responsabilità amministrative e gestionali in base al rischio per la missione e la funzione aziendale.

2) Identificare le dipendenze non legate alla missione e alle funzioni aziendali o l'utilizzo delle risorse informatiche.

- Utilizzare l'analisi del flusso delle missioni, l'analisi delle dipendenze delle missioni, le esercitazioni tabletop e il Red Teaming per scoprire le dipendenze non documentate delle missioni.
- Rivedere e correlare la missione e le funzioni aziendali con la mappatura del modello di dipendenza e le attività e i risultati dell'analisi d'impatto.
- Identificare i sistemi, le applicazioni e i processi delle funzioni non mission critical e le risorse che li supportano.
    - Valutare queste funzioni rispetto a una strategia di implementazione fluida della Cyber COOP, per soddisfare le operazioni prioritarie e migliorare l'utilizzo o l'eliminazione delle dipendenze.

4. Gestione delle risorse informatiche, delle modifiche e delle configurazioni

- **Asset:** iniziamo con la definizione di asset. Secondo la definizione del dizionario, un asset è una cosa o una persona utile o di valore. Allo stesso modo, gli asset di un fornitore di servizi IT sono gli strumenti, le applicazioni, gli elementi di configurazione e qualsiasi altro elemento di valore che aiuta a fornire servizi ai clienti o all'azienda. Gli asset sono una parte della gestione delle risorse e delle configurazioni dei servizi.

- **Elemento di configurazione: Un elemento di** configurazione è qualsiasi componente che deve essere gestito per fornire un servizio IT. Esempi di elementi di configurazione sono servizi IT, hardware, software, edifici, persone e documentazione formale. In breve, qualsiasi componente o elemento che contribuisce a fornire un servizio IT al cliente viene classificato come elemento di configurazione. Le informazioni su ogni elemento di configurazione sono registrate in un Record di Configurazione all'interno del Sistema di Gestione della Configurazione e queste informazioni sono mantenute durante il ciclo di vita dalla Gestione della Configurazione.

- **Database di gestione della configurazione:** Il database di gestione della configurazione è abbreviato in CMDB. Il CMDB è un database utilizzato per archiviare i record di configurazione durante il loro ciclo di vita. Il CMDB archivia le informazioni sulle vostre CI, ognuna contraddistinta da un identificatore unico, comprese le informazioni identificative come il numero di serie, l'indirizzo MAC o l'indirizzo IP, la versione corrente, la posizione, le informazioni sul fornitore e sui fornitori.

- **Sistema di gestione della configurazione: Il** sistema di gestione della configurazione, abbreviato in CMS, è un insieme di strumenti e database utilizzati per gestire i dati di configurazione di un fornitore di servizi IT. I dati relativi agli elementi di configurazione sono memorizzati in record di configurazione e i record di configurazione sono inclusi nei database del sistema di gestione delle configurazioni. Il CMDB di un fornitore di servizi IT per gestire i dati di configurazione è incluso nel processo di gestione degli asset e della configurazione del servizio. Il Configuration Management System include anche informazioni su incidenti, problemi, errori noti, modifiche e rilasci, dipendenti, fornitori, sedi, business unit, clienti e utenti. In sintesi, tutte le informazioni necessarie sugli elementi di configurazione e sugli asset IT sono incluse nel Configuration Management System. Quando necessario, queste informazioni vengono acquisite dal CMS e utilizzate rispettivamente**.**

La gestione della configurazione, definita fondamentalmente come il processo di identificazione, controllo, monitoraggio e verifica delle modifiche apportate, è una parte fondamentale di un solido programma di sicurezza. La gestione delle modifiche e delle configurazioni all'interno di

un'organizzazione ha forti legami con i requisiti di audit di quasi tutti i framework e le normative di sicurezza.

La gestione della configurazione si basa sul controllo e sul rilascio delle varie versioni dei prodotti. Le configurazioni predefinite per i sistemi operativi e le applicazioni sono generalmente orientate alla facilità di distribuzione e di utilizzo, non alle best practice di cybersecurity. Oggi la gestione della configurazione è una disciplina molto richiesta con implicazioni significative per la cybersecurity, soprattutto perché le organizzazioni passano da configurazioni predefinite out-of-the-box a configurazioni di applicazioni e hardware più sicure.

Oggi la gestione della configurazione ha significati diversi per persone diverse. In alcune implementazioni, si riferisce al modo in cui vengono configurati i dispositivi di rete. In altre, si riferisce alla versione di un'applicazione che un team sta eseguendo. A volte gli addetti ai lavori confondono la gestione delle risorse IT con la gestione delle modifiche e della configurazione. Pur essendo simili e ugualmente importanti per l'azienda, non sono la stessa cosa. Le soluzioni di gestione IT monitorano, ottimizzano e gestiscono le risorse lungo l'intero stile di vita delle risorse. Nel frattempo, il CM raccoglie, archivia, gestisce, aggiorna e analizza tutti gli elementi di configurazione.

Sebbene molte organizzazioni abbiano programmi di CM immaturi, essi sono fondamentali per il moderno panorama della cybersecurity e la loro importanza è destinata a crescere con la continua evoluzione del panorama delle minacce.

4.1. Gestione della configurazione e Disaster Recovery

Quando si parla di disaster recovery moderno, la gestione della configurazione è essenziale. In caso di disastro di cybersecurity (il 76% delle organizzazioni ha subito un incidente di cybersecurity IoT), può essere impossibile ripristinare la configurazione più recente se non esiste una documentazione della stessa.

Lo stesso vale per la sicurezza informatica: è impossibile per i team sapere se qualcosa non va se non c'è un modo standardizzato di configurare, modificare e documentare l'ambiente digitale.

4.2. Gestione del cambiamento

La gestione del cambiamento è parallela alla gestione della configurazione, anche se le due cose *non sono* la stessa cosa. Le persone le confondono continuamente.
Mentre la gestione della configurazione è il processo di identificazione e documentazione dei componenti hardware e software e delle relative impostazioni, la gestione delle modifiche è una funzione sottostante al più ampio processo di gestione della configurazione. La gestione delle modifiche si riferisce ai processi associati e cerca di creare stabilità all'interno di un sistema e di prevenire modifiche incontrollate o casuali o di documentare i processi di modifica in caso di

turnover all'interno dell'organizzazione. In altre parole, consente alle aziende di pianificare i cambiamenti, anziché limitarsi a reagire ad essi.

4.2.1. Il processo di gestione del cambiamento

Oggi, un processo di gestione del cambiamento ben strutturato comprende quanto segue:

- Presentazione delle richieste di modifica
- Valutazioni del rischio e dell'impatto
- Approvare/rifiutare le funzioni di modifica
- Test
- Funzioni di programmazione/ notifica agli utenti/ formazione
- Implementazione
- Convalida
- Documentazione

Uno dei luoghi in cui la gestione del cambiamento prospera è in caso di decisioni di emergenza, quando è necessario apportare modifiche. Una volta implementata, la modifica deve essere reinserita nel processo di gestione delle modifiche, dove beneficerà dei protocolli di convalida e documentazione già stabiliti.

4.3. Gestione degli asset di cybersecurity

La gestione delle risorse di cybersecurity è il processo di raccolta dei dati sulle risorse (dispositivi, istanze cloud e utenti) per rafforzare le funzioni di sicurezza fondamentali, tra cui:

- **Rilevamento e risposta:** Garantire che le capacità di rilevamento e risposta forniscano una copertura in tutta l'azienda.
- **Gestione delle vulnerabilità:** Comprendere quali asset possono essere vulnerabili agli exploit e garantire che tutti gli asset siano valutati per le vulnerabilità.
- **Sicurezza del cloud:** Garantire che le istanze cloud siano sicure e configurate per evitare diritti di accesso troppo permissivi, anche quando vengono messe in funzione e dismesse rapidamente.
- **Risposta agli incidenti:** Utilizzo di dati arricchiti e correlati sugli asset per accelerare le indagini di risposta agli incidenti e la bonifica.
- **Monitoraggio continuo dei controlli:** Identificare quando i controlli di sicurezza sono mancanti e devono essere applicati.

5. Valutazione dell'efficacia delle politiche di sicurezza informatica

Lo sviluppo di un sistema informativo passa attraverso diverse fasi distinte, dall'analisi del problema all'implementazione del sistema. Nel corso di questo processo, ogni fase viene documentata attraverso una serie di documenti che vanno dallo studio di fattibilità ai manuali di formazione e alla documentazione del sistema. Nello sviluppo di una politica di sicurezza questo processo di autodocumentazione generalmente non si verifica.

Molte politiche sviluppate attualmente cercano di far rientrare tutto nella politica di sicurezza: la giustificazione dell'importanza e le istruzioni e le descrizioni specifiche del sistema. Certamente, la politica di sicurezza in sé è già abbastanza prolissa, senza avere dettagli su come è stato creato il documento, su chi è stato consultato nella sua produzione o su come si è arrivati alla formulazione della politica. Non ci sarà nemmeno una documentazione sui problemi politici che possono essersi verificati durante l'implementazione della politica, o su come formare le persone sulla politica. Con l'uso di tecniche di documentazione durante lo sviluppo della politica, tuttavia, una politica di sicurezza potrebbe tornare ad essere un documento di principi. Altre questioni che non riguardano i principi della politica di sicurezza verrebbero documentate altrove, insieme alla giustificazione della politica.

L'informazione più importante che spesso manca o è semplicemente inadeguata quando si cerca di valutare una politica di sicurezza in un'organizzazione è la documentazione dei requisiti. Senza una chiara comprensione dei requisiti, la valutazione della qualità di una politica di sicurezza è quasi impossibile. L'analisi dei rischi e delle minacce che l'organizzazione deve affrontare è solo una parte dei requisiti necessari per lo sviluppo di una politica di sicurezza. Gli obiettivi dell'organizzazione e altre questioni politiche che influenzano lo sviluppo, l'implementazione e l'accettazione della politica di sicurezza sono altrettanto importanti. La disponibilità di un'ampia documentazione che includa i risultati di un'approfondita analisi dei requisiti consentirà di valutare la politica di sicurezza in modo più approfondito, anziché limitarsi a una valutazione superficiale del prodotto finale. Per esempio, invece di concentrarsi solo sull'implementazione della politica in una particolare area, la valutazione può ora considerare anche come quell'area è stata sviluppata all'interno della politica. Le prove documentali potrebbero essere valutate per determinare se la politica copre adeguatamente tutte le questioni identificate nell'ambito dello sviluppo senza annacquarne nessuna. Tuttavia, le politiche di sicurezza variano notevolmente a seconda del contesto dell'organizzazione e ci si aspetterebbe che anche il loro sviluppo vari. Esistono alcuni punti in comune tra le politiche, anche se le aree di destinazione si discostano. A differenza della valutazione dei prodotti, tuttavia, molti criteri nella valutazione delle politiche di sicurezza saranno di natura soggettiva. Ciò è dovuto alla natura soggettiva dello sviluppo di una politica e dell'ambiente in cui essa viene implementata.

5.1. Mantenere l'efficacia delle politiche di sicurezza informatica

L'informatica, o IT, è probabilmente la tecnologia del secolo. Ha sicuramente trasformato il mondo. Con tutti i vantaggi dell'IT, tuttavia, anche molti rischi per la sicurezza sono penetrati nelle nostre vite. Le organizzazioni devono progettare efficaci politiche di sicurezza informatica per garantire che le loro operazioni commerciali rimangano al sicuro da intrusi malintenzionati e da ladri di dati. Ironia della sorte, un modo eccellente per mantenere l'efficacia delle politiche di sicurezza contro il mutevole panorama dei rischi informatici è quello di utilizzare maggiormente l'IT.

Ecco alcuni dei modi in cui l'IT può mantenere l'efficacia delle politiche di sicurezza:

- **Migliore valutazione del rischio: La** valutazione dei rischi per la sicurezza è un primo passo essenziale nella progettazione di qualsiasi politica di sicurezza delle informazioni. Per affrontare le minacce derivanti dalla rapida evoluzione del settore IT, l'informatica è l'unico antidoto. Poiché i rischi cambiano costantemente, l'informatica è un elemento indispensabile per tenere sotto controllo le nuove minacce. Permette di scoprire facilmente nuovi rischi sulla base dei precedenti record di conformità, di classificare i fattori di rischio e di valutare i danni che possono causare. È quindi importante imparare dai nuovi sviluppi, positivi o negativi, dell'IT. In questo modo migliorerete la valutazione dei rischi e la vostra preparazione in caso di minaccia imminente.
- **Migliore conformità**: L'IT vi aiuta a monitorare la conformità dei dipendenti e dei responsabili dell'organizzazione alle autorità di regolamentazione e alle politiche di sicurezza specifiche dell'organizzazione. Attraverso un unico software, è possibile tenere sotto controllo le autorizzazioni di accesso, la condivisione insicura dei dati, la navigazione web non sicura, la crittografia dei dati insufficiente e innumerevoli altri fattori che possono compromettere gravemente la sicurezza.
- **L'aggiornamento costante è d'obbligo**: Poiché il mondo dell'IT cambia a ogni respiro, è necessario essere costantemente alla ricerca di nuovi cambiamenti che potrebbero danneggiare il sistema. Monitorate gli sviluppi nel mondo dei rischi informatici, della criminalità informatica e della sicurezza informatica. Aggiornate frequentemente e regolarmente le vostre politiche di sicurezza informatica e il vostro software di sicurezza, perché possono diventare obsoleti molto rapidamente. In questo modo, potrete mantenere l'efficacia delle vostre politiche di sicurezza.
- **Attenuazione rapida**: Se la vostra organizzazione si trova di fronte a un'imminente minaccia alla sicurezza che può portare a una potenziale perdita o furto di dati, dovete avere a portata di mano un piano di mitigazione o di rimedio. L'IT vi aiuta a pianificare la mitigazione in modo semplice ed efficiente. Con l'IT è possibile assegnare e collegare le fasi di mitigazione del rischio ai diversi rischi potenziali quando si progettano le politiche

di sicurezza. Questo renderà la mitigazione tempestiva e più efficace, mantenendo così l'efficacia delle politiche di sicurezza.

- **Miglioramento della responsabilità**: Nessuna politica sulle informazioni può rimanere efficace se le persone non sono ritenute responsabili e responsabili dei rischi, della conformità e della mitigazione. L'IT rende più facile garantire la responsabilità delle azioni correttive. Può migliorare notevolmente la visibilità dei rischi e la valutazione della maturità, la conformità e le misure di rimedio intraprese dall'organizzazione. Ciò significa che i vostri dipendenti saranno più tempestivi e più responsabili nei confronti dei passi elencati nelle vostre politiche di sicurezza delle informazioni.

5.2. Valutazione dei rischi per la sicurezza

Valutazione del rischio, dopo aver determinato quali asset informativi saranno protetti, si seleziona il metodo di valutazione del rischio e si definiscono i rischi. In base al metodo di valutazione del rischio scelto, le risorse informative vengono posizionate sulla mappa del rischio mostrata in figura. Una volta effettuata la valutazione, la mappa dei rischi comprende i processi di miglioramento e controllo dei rischi per le minacce ad alto impatto e probabilità. Poiché la posizione delle risorse informative nella mappa dei rischi può cambiare, la mappa dei rischi deve essere aggiornata regolarmente e devono essere prese le precauzioni necessarie.

Il rischio è definito come la combinazione delle probabilità di un evento e del suo esito. La valutazione del rischio, che è una fase della gestione del rischio, è un processo in cui vengono definiti i rischi e vengono determinati gli effetti e le priorità di questi rischi identificati. La gestione del rischio consiste nel determinare un livello di rischio accettabile, nel valutare il rischio attuale, nell'adottare le misure necessarie per ridurlo a un livello accettabile e nel mantenere tale livello. Le informazioni e gli altri asset, le minacce a questi asset, le vulnerabilità del sistema esistente e i controlli del sistema di sicurezza sono i componenti che determinano il rischio attuale. L'identificazione delle informazioni o degli asset da proteggere, la determinazione del valore di questi asset per l'azienda, la rivelazione di quali minacce note e possibili a questi asset si cercherà di prevenire, l'indagine su come potrebbero verificarsi le possibili perdite, l'identificazione dell'entità delle possibili minacce a ciascun asset, l'esame di ciò che si può fare in primo luogo per ridurre l'entità e la probabilità delle perdite che possono verificarsi in questi asset e la pianificazione delle misure da adottare per mantenere le minacce prospettiche a un livello minimo sono alcune fasi della valutazione del rischio. Il costo del sistema di sicurezza da stabilire e implementare come risultato della gestione del rischio è un'altra questione importante da considerare. Il costo del sistema di sicurezza deve essere limitato dal valore delle informazioni protette e dal rischio determinato dall'esame delle possibili minacce. Oltre al principio che non esiste una sicurezza al 100%, la configurazione ideale della sicurezza delle informazioni si realizza

attraverso tre processi. Questi processi sono la prevenzione, il rilevamento e la risposta (risposta o reazione).

Prevenzione **-** è il processo su cui i sistemi di sicurezza si concentrano e lavorano maggiormente. Sono state sviluppate diverse misure per isolare il sistema dalle minacce e dagli attacchi contro i sistemi informatici, come le misure di sicurezza utilizzate nella vita quotidiana, quali la recinzione del giardino di una casa e l'utilizzo di una porta d'acciaio. Per quanto riguarda la sicurezza del personal computer, è difficile valutare le password utilizzate, è necessario installare programmi di scansione dei virus, eseguire questi programmi e i service pack del sistema operativo e la correzione degli errori e gli aggiornamenti a intervalli regolari, utilizzare uno screen saver protetto da password sul computer, abbandonare il sistema dopo essere stati lontani dal computer per molto tempo, è difficile stimare le password utilizzate, è necessario mantenere queste password riservate e cambiarle a intervalli regolari, è necessario prestare attenzione alla condivisione dei dischi, prestare attenzione ai file scaricati da Internet o inviati per posta elettronica, proteggere i documenti importanti con una password o mantenerli crittografati, inviare per posta elettronica informazioni riservate o importanti, siti senza certificati di sicurezza. Alcune misure che possono sembrare semplici, ma che salvano la vita, come ad esempio non farsi inviare tramite mezzi non sicuri, spegnere l'accesso a Internet quando non lo si usa, fare backup regolari di informazioni e documenti importanti. Le misure di prevenzione da attuare per la sicurezza informatica negli ambienti aziendali sono più ampie e complesse. Alcune delle cose che vengono fatte per la prevenzione in questi sistemi in cui lavorano esperti di sicurezza:

- Esaminare periodicamente i service pack e gli aggiornamenti del sistema operativo e del software,
- Mantenere i diritti degli utenti al minimo, non eseguire protocolli, servizi, componenti e processi inutilizzati,
- Tecniche di crittografia nella trasmissione dei dati, scanner di vulnerabilità,
- Utilizzo della rete privata virtuale,
- L'uso dell'infrastruttura a chiave pubblica e della firma elettronica può essere annoverato tra i sistemi basati sulla biometria.

Infatti, se i progressi determinati nel processo di prevenzione potessero essere perfetti, non sarebbero affatto necessari ulteriori processi. Tutti gli attacchi sarebbero stati prevenuti nel peggiore dei modi. Ma nessun prodotto di sicurezza è perfetto o completo. Inoltre, quasi ogni giorno vengono rilevate diverse vulnerabilità nei sistemi di trasmissione, nei servizi Internet, nelle tecnologie web e nelle applicazioni di sicurezza. Da questo punto di vista, l'utilizzo dei processi di rilevamento e abbinamento aumenta.

Determinazione - la sicurezza non è solo una questione di prevenzione. Ad esempio, il fatto che un museo sia ben protetto, che sia circondato da recinzioni, che le porte siano chiuse e bloccate, non rende necessario l'uso di guardie notturne in quel museo. Allo stesso modo, aumenta l'uso

di metodi per rilevare i tentativi di attacco ai sistemi informatici. La prevenzione consiste nel costruire una barriera che renda gli attacchi più forti (ma non impossibili) o che scoraggi (ma non distrugga) gli aggressori. La prevenzione senza rilevamento e risposta può avere un beneficio limitato. Se fosse sufficiente la sola prevenzione, la maggior parte degli attacchi non sarebbe nemmeno nota. Con il rilevamento, gli attacchi già noti o appena emersi possono essere segnalati e ricevere risposte adeguate. Il primo e più elementare passo per il rilevamento consiste nel monitorare l'intero stato e i movimenti del sistema e nel registrare queste informazioni. In questo modo, si raccolgono anche dati e prove per l'analisi post-attacco. Firewall, sistemi di rilevamento delle intrusioni, monitor del traffico di rete, scanner di porte, utilizzo di honeypot, strumenti di protezione in tempo reale da virus e spyware, programmi di controllo del checksum dei file e sensori Sniffer di rete sono alcuni dei metodi più comuni utilizzati nel processo di rilevamento.

AnswerBack **-** Così come un luogo dotato di guardie, cani, telecamere di sicurezza, sensori può attirare l'attenzione dei ladri, anche i sistemi informatici con sistemi di rilevamento in tempo reale sono attraenti per hacker e aggressori. La risposta rapida emerge come un elemento essenziale che completa il sistema di sicurezza per respingere questi attacchi. La risposta può essere definita come l'esecuzione di azioni che rispondono immediatamente o il prima possibile ai tentativi di attacco che non possono essere affrontati dal processo di prevenzione e determinati dai processi di rilevamento. I sistemi di rilevamento delle intrusioni possono avere senso se c'è qualcuno o un sistema che risponde a questo rilevamento. Altrimenti, la situazione non va oltre il vantaggio di un allarme per auto che nessuno sente e di cui nessuno si preoccupa. In questo senso, la reciprocità è un anello importante che completa il processo di sicurezza. Anche se l'attacco non viene completamente impedito, consente al sistema di tornare al suo stato normale, di identificare le cause dell'attacco, di catturare l'aggressore, quando necessario, di identificare le vulnerabilità del sistema di sicurezza e di riorganizzare i processi di prevenzione, rilevamento e risposta. Pianificando in anticipo le azioni da intraprendere quando viene rilevato un attacco, si garantisce che questo processo funzioni in modo efficace e non comporti perdite di tempo e denaro. Il disaster recovery è in prima linea tra i principali piani per i casi peggiori intrapresi in questa fase.

Domande:

Domande di autovalutazione.

- Che cos'è la vulnerabilità dei sistemi IT
- Spiegare e fornire esempi di gestione delle vulnerabilità e del rischio.

Allegati (presentazione PowerPoint, dispense, stampe, link, video...):

Riferimenti:

1. Valutazione dello sviluppo delle politiche di sicurezza IS S.B. Maynard1 & A.B. Ruighaver2 Dipartimento di Sistemi Informativi Università di Melbourne Australia
2. https://www.bizzsecure.com/how-it-can-maintain-the-effectiveness-of-security-policies/
3. https://blog.masterofproject.com/service-asset-and-configuration-management/
4. https://www.apptega.com/blog/change-configuration-management-cybersecurity
5. https://cam.scmagazine.com/it-service-management-vs-cybersecurity-asset-management/
6. http://www2.mitre.org/public/industry-perspective/documents/06-ar-cyber-coop-planning.pdf
7. https://icma.org/articles/pm-magazine/cyber-continuity-planning-go-big-or-go-home
8. https://www.kroll.com/en/services/security-risk-management/security-consulting/threat-vulnerability-assessments
9. https://www.xmcyber.com/blog/what-is-the-difference-between-vulnerability-assessment-and-vulnerability-management/
10. https://www.techtarget.com/searchsecurity/definition/vulnerability-assessment-vulnerability-analysis