**CYBERYOUTH**

**Formazione non formale per la sicurezza informatica e la resilienza delle organizzazioni giovanili e dei giovani**

***Accademia online per la cybersecurity giovanile***

****

**Procedure e linee guida per la risposta agli incidenti**

Indice

[Introduzione](#_heading=h.fpb3yt6tcffi)

[Potrebbe essere successo a te...](#_heading=h.c7zxm1r80lor)

[Cosa imparerai](#_heading=h.bd1t10x6k115)

[Perché è importante](#_heading=h.1fqj6c1n3ygs)

[Come può aiutarti nella vita di tutti i giorni](#_heading=h.bddh90wxykhs)

[Quale carriera puoi intraprendere](#_heading=h.l25siuf1d90q)

[Pre-requisiti](#_heading=h.obikvf4haym5)

[Materiale](#_heading=h.wlxlanfpyu9n)

[5.1 Valutazione della Sicurezza Organizzativa](#_heading=h.2yz7x8bu8zb5)

[Auto-valutazione](#_heading=h.nfq2guswx59)

[Consultazione esterna](#_heading=h.qycpsfx2oc3y)

[Conoscere le tue Debolezze](#_heading=h.ilmmnwqn61ww)

[Tattiche di Prevenzione](#_heading=h.lzulet6qo51l)

[Conclusioni](#_heading=h.q7y4utybp22l)

[5.2 Politiche e Procedure per la Risposta agli Incidenti](#_heading=h.wv8lmqsplpdd)

[Damage Mitigation](#_heading=h.se3v82rotiu3)

[Data Protection](#_heading=h.xa9iyn2x8esy)

[Prevenzione di Futuri Incidenti](#_heading=h.3uw9tlbm0qe0)

[Conclusioni](#_heading=h.jn7khpgf6mc9)

[5.3 Data investigation](#_heading=h.g98km9urykdd)

[Organisational Investigation](#_heading=h.d7j3sia9a2ue)

[External Investigation](#_heading=h.4rgr0sqkydi2)

[Cosa cercare](#_heading=h.uu16mwe9cyzf)

[Conclusioni](#_heading=h.ostdn54761l3)

[5.4 Tecniche di Mitigazione](#_heading=h.7pii0khen2cd)

[Isolazione](#_heading=h.byj2zirdlb0u)

[Contenimento](#_heading=h.orqrn6qc565u)

[Segmentazione](#_heading=h.pr0uebiv6hju)

[Conclusioni](#_heading=h.8fgh3pvuc4s3)

[5.5 Forense Digitale](#_heading=h.azw51npc11fy)

[Aspetti Principali](#_heading=h.ucvhdpx4godb)

[Le 4 Fasi dell’Informatica Forense](#_heading=h.rpetdaosatfp)

[Collezione](#_heading=h.ureo4tm4v2uf)

[Esaminazione](#_heading=h.e3rsgig0mbwl)

[Analisi](#_heading=h.h1zlr3q64b6h)

[Reporting](#_heading=h.33k06le0uda3)

[Conclusioni](#_heading=h.scbfee5behhv)

[L’angolo del Geek](#_heading=h.floxyjcfjlz3)

[Conclusioni](#_heading=h.umqq3lf4f2yk)

[Quiz](#_heading=h.35btfg6prjdy)

[Fonti](#_heading=h.ioedg3ublhq7)

#

# **Introduzione**

## **Potrebbe essere successo a te...**

Nel maggio 2022, Cisco, un'azienda multinazionale di comunicazioni digitali, ha scoperto la presenza di un attaccante all'interno della loro rete. Dalle indagini interne è emerso che l'attaccante aveva condotto una serie di sofisticati attacchi di phishing vocale per accedere all'account Google di un dipendente di Cisco. Poiché le credenziali del dipendente erano sincronizzate in un browser, l'attaccante poteva facilmente accedere ai sistemi interni di Cisco. Dopo aver ottenuto l'accesso iniziale, l'attaccante ha cercato di rimanere nella rete di Cisco il più a lungo possibile e aumentare il proprio livello di accesso. Tuttavia, il team di sicurezza di Cisco è riuscito con successo a rimuovere l'attaccante dalla rete. Successivamente, il gruppo di ransomware Yanluowang ha pubblicato file rubati sul proprio sito web. Secondo Cisco, questa violazione non ha avuto alcun impatto sulle loro operazioni aziendali.

In incidenti come questo, la politica di risposta è fondamentale, come si può vedere dal fatto che Cisco ha reagito rapidamente ed è riuscita a risolvere il problema ed evitare un disastro. È quasi impossibile non subire un attacco, ma è molto possibile evitare conseguenze gravi avendo una rigorosa politica di risposta!

Fonte:<https://www.ekransystem.com/en/blog/top-10-cyber-security-breaches>

## **Cosa imparerai**

Questo modulo coprirà una vasta gamma di argomenti relativi alla risposta agli incidenti, con un focus principale sulle politiche e le procedure che un'organizzazione può implementare per migliorare la loro reazione a potenziali violazioni e attacchi, come strumenti di rilevamento e raccolta di informazioni, investigazione dei dati e tecniche per mitigare i danni causati da un attacco, nonché i punti chiave della scienza forense digitale per apprendere e migliorare da potenziali incidenti.

## **Perché è importante**

Questo modulo è essenziale per una maggiore comprensione di come prevenire e evitare incidenti, nonché per comprendere come reagire a possibili attacchi o violazioni. Gli incidenti di sicurezza informatica non scompaiono una volta verificatisi; molti sono progettati per infiltrarsi in una rete e rimanere finché non vengono gestiti nel modo appropriato. Comprendendo le politiche e le procedure per la risposta agli incidenti, è possibile migliorare le proprie capacità di reagire agli incidenti e agli attacchi, nonché sviluppare una solida conoscenza su come individuare possibili incidenti in anticipo ed evitarli del tutto. Le politiche e le procedure costituiscono una parte molto ampia e importante della sicurezza informatica e della salvaguardia della propria organizzazione e includono una vasta gamma di argomenti, che vanno dalla ricognizione e rilevamento della rete al recupero di dati e informazioni persi o danneggiati.

## **Come può aiutarti nella vita di tutti i giorni**

Il materiale discusso in questo modulo mira a offrire un'esperienza di apprendimento che non solo ti preparerà nel campo della risposta agli incidenti di sicurezza informatica, ma mostrerà anche preziose abilità di preparazione e reazione che possono essere trasferite a molteplici aspetti della vita quotidiana. Con la crescente connessione digitale tra tutti noi, gli incidenti stanno diventando sempre più comuni ogni giorno, il che significa che la necessità di avere una politica e una procedura per rispondere e evitarli sta diventando sempre più importante ogni giorno. Questo vale sia per la sicurezza delle organizzazioni che per la vita digitale quotidiana, poiché le minacce dei crimini informatici non riguardano solo le aziende o le organizzazioni; dobbiamo fare attenzione anche noi.

## **Quale carriera puoi intraprendere**

Dopo aver completato questo modulo, avrai acquisito una comprensione di base dei fondamenti della sicurezza informatica. Questa conoscenza ti fornirà un punto di partenza per esplorare diverse carriere nell'industria della sicurezza informatica. Alcune potenziali carriere di livello base includono:

* Specialisti in Sicurezza Informatica
* Revisori IT
* Responsabili dell'Infrastruttura
* Leader della Risposta agli Incidenti

## **Pre-requisiti**

Tutti i moduli del nostro corso offriranno informazioni preziose anche se studiati singolarmente, ma ti incoraggiamo a completare i quattro moduli precedenti prima di affrontare questo modulo. Sono progettati per essere seguiti in ordine, e ciascun modulo ti offrirà una maggiore comprensione del successivo fornendoti conoscenze e contesti situazionali.

#

#

# **Materiale**

## **5.1 Valutazione della Sicurezza Organizzativa**

Nel mondo moderno, avere adeguate misure di sicurezza in qualsiasi organizzazione è fondamentale per la sicurezza degli utenti, nonché dei membri dell'organizzazione stessa. Per mantenere queste misure di sicurezza ai massimi standard, è necessario capire come valutare e individuare possibili problemi nella sicurezza di un'organizzazione. Comprendere come valutare le politiche e le procedure di cibersicurezza dell'organizzazione è fondamentale per prevenire, reagire e mitigare eventuali attacchi informatici o violazioni. Valutando e comprendendo le debolezze o i punti ciechi nella nostra organizzazione, li trasformiamo in punti di forza implementando politiche e quadri che li tengano in considerazione e proteggano queste vulnerabilità.

### **Auto-valutazione**

Il primo passo da compiere nella valutazione della sicurezza è realizzare una valutazione interna. Un punto chiave nell'autovalutazione è assicurarsi di capire cosa stiamo cercando, così come gli errori comuni e le debolezze. Per questo motivo, è sempre meglio coinvolgere vari membri del team addestrati con background in IT e sicurezza, in modo da offrire prospettive diverse ma informate.

Il processo di autovalutazione della sicurezza di un'organizzazione può essere leggero o approfondito a seconda delle esigenze, ma è sempre meglio effettuare una verifica completa di qualsiasi possibile vulnerabilità, non solo dal lato digitale e tecnologico, ma anche dal lato umano, assicurandosi che tutti i membri dell'organizzazione siano ben preparati e comprendano le procedure e le strategie di sicurezza nell'organizzazione.

### **Consultazione esterna**

Oltre a una valutazione interna, può essere vantaggioso essere valutati da un'organizzazione esterna specializzata in sicurezza informatica e sicurezza organizzativa. Molte volte, un nuovo set di occhi può individuare cose che potremmo aver trascurato! Molte aziende di sicurezza informatica offrono un servizio di ispezione o consulenza come parte del loro business, con molte di esse che offrono persino di gestire completamente il vostro programma di sicurezza.

### **Conoscere le tue Debolezze**

L'obiettivo di una valutazione della sicurezza, che sia interna o esterna, è comprendere la situazione della sicurezza informatica della vostra organizzazione, nonché aiutare a identificare possibili punti deboli o vulnerabilità, capire dove potrebbero verificarsi attacchi o violazioni e sviluppare un piano di prevenzione, nonché una politica di risposta agli incidenti nel caso di una violazione o di un attacco.

### **Tattiche di Prevenzione**

Anche se non direttamente collegato alla risposta agli incidenti, un piano di prevenzione con tattiche dettagliate è strettamente correlato all'idea di risposta agli incidenti, poiché avere un piano di prevenzione sviluppato può aiutare a sviluppare un piano di risposta agli incidenti tenendo conto delle metodologie già utilizzate nel piano di prevenzione.

Tattiche comuni di prevenzione e, di conseguenza, casi comuni di incidenti che richiedono un piano di risposta, possono essere concetti come:

* Autenticazione a più fattori: ciò garantisce che la persona che accede sia effettivamente la persona autorizzata. L'autenticazione a più fattori è uno dei principali metodi di prevenzione degli incidenti, ma non garantisce la sicurezza in casi come il furto di proprietà o l'accesso non autorizzato a un edificio o a una posizione.
* Controllo degli accessi: tattiche come schede chiave, badge RFID, ecc. Queste sono una buona opzione per squadre più piccole, ma possono diventare difficili da monitorare in caso di squadre più grandi, il che significa che il furto o la perdita possono verificarsi senza che il team di sicurezza se ne accorga.

Queste tattiche di prevenzione aiutano a evitare incidenti e possono anche essere implementate come linee guida per lo sviluppo di un piano di risposta agli incidenti robusto, tenendo conto delle comuni violazioni a cui queste tattiche possono essere soggette e guidando la creazione di una risposta specifica per ciascuna di esse.

### **Conclusioni**

Una delle chiavi per sapere come mantenere sicura un'organizzazione è capire da dove potrebbero provenire minacce o attacchi possibili. Le valutazioni di sicurezza regolari sono un vantaggio per la sicurezza dell'organizzazione, poiché le condizioni possono cambiare, rendendo quindi la sicurezza obsoleta o inutile contro possibili attacchi. Oltre a essere preparati per prevenire gli attacchi, attraverso valutazioni di sicurezza regolari e approfondite, le organizzazioni possono capire meglio come risolvere i problemi se dovesse verificarsi un attacco o un incidente, sottolineando l'importanza della corretta valutazione del contesto e della situazione di sicurezza dell'organizzazione.

## **5.2 Politiche e Procedure per la Risposta agli Incidenti**

Indipendentemente da quanta preparazione mettiamo in atto, la probabilità di subire un incidente di cibersicurezza è molto alta, specialmente nel mondo digitale moderno. Studi hanno dimostrato che l'80% delle aziende ha subito qualche forma di incidente di cibersicurezza durante l'operatività, il che significa che la prevenzione è il miglior metodo, ma, cosa dovremmo fare se succede qualcosa nonostante i nostri migliori sforzi?

In casi come questo, è importante avere un piano. Avendo una procedura da seguire in caso di incidente, un'organizzazione può evitare di lasciare decisioni importanti sulla sicurezza a un singolo membro o dipendente, offrendo loro il supporto e gli strumenti necessari per rimanere al sicuro e il quadro con cui risolvere eventuali violazioni o problemi. Avere una politica di risposta agli incidenti non è solo per la sicurezza dell'organizzazione e dei suoi dati, ma anche per la sicurezza dei suoi membri e/o dipendenti, poiché fornendo quadri chiari e rigorosi e passaggi in caso di incidente, l'organizzazione sta proteggendo loro dal dover prendere decisioni potenzialmente insicure o pericolose, che siano digitali o meno.

### **Damage Mitigation**

Uno dei punti chiave in qualsiasi piano di risposta deve essere la riduzione dei danni causati da un attacco o da un incidente. Se si verificasse un incidente, il primo passo, una volta valutati i danni, è ridurli, limitando l'effetto che possono avere sul funzionamento dell'organizzazione. I dati e la sicurezza sono le principali preoccupazioni in caso di incidente, ma un'altra forma di danno causato da violazioni o problemi di cibersicurezza è la perdita di produttività dovuta a servizi o dati non disponibili che l'organizzazione potrebbe necessitare nell'uso quotidiano.

Alcuni dei fattori chiave nella mitigazione dei danni da un attacco o una violazione possono includere azioni come:

1. Se la violazione o l'attacco è avvenuto a causa di malware, assicurarsi che questo non possa diffondersi ad altri membri o dispositivi, utilizzando tecniche di mitigazione (discusse in seguito al punto 5.4).

2. Nel caso in cui password o chiavi di sicurezza siano state compromesse a causa della violazione, rigenerare le chiavi e/o cambiarle immediatamente. Anche se nessun tentativo di utilizzarle è stato effettuato, potrebbe verificarsi in qualsiasi momento e la procedura per cambiarle è uno sforzo minimo per mantenere al sicuro i dati.

3. In caso di una violazione fisica (persona o dispositivo non autorizzato), individuare la violazione e applicare tecniche di mitigazione simili all'area interessata.

4. Lasciare che il responsabile della sicurezza/sicurezza designato prenda le decisioni. È sempre meglio che una persona qualificata prenda decisioni potenzialmente pericolose o ad alta pressione.

5. Se il responsabile della sicurezza lo ritiene necessario, contattare le autorità di polizia o le forze dell'ordine. La parte più importante della mitigazione dei danni è la sicurezza dei dipendenti e/o dei membri del team.

### **Data Protection**

Nella maggior parte delle violazioni di sicurezza informatica, il bersaglio è costituito dai dati dell'organizzazione. Questi dati possono essere dati dei dipendenti, dati dei clienti o persino dati privati sensibili di utenti minorenni nel caso di molte organizzazioni giovanili. Ecco perché proteggere questi dati è di massima importanza in qualsiasi situazione; ma la protezione può assumere vari significati. Dobbiamo proteggere i dati dal furto e assicurarci che altri non possano accedervi, ma dobbiamo anche assicurarci che siano al sicuro in caso di cancellazione, corruzione o qualsiasi incidente fisico imprevisto.

In termini di protezione da furti o attacchi, alcuni dei fattori chiave per mantenere i nostri dati al sicuro possono essere metodi come:

1. **Crittografia di tutti i dati:** Idealmente, tutti i dati con cui operiamo dovrebbero essere crittografati per tenerli al sicuro dagli attaccanti. Abbiamo discusso della crittografia in altri moduli, quindi siamo familiari con i metodi e la loro efficacia, ma nonostante l'efficienza, qualsiasi crittografia è meglio di nessuna!

2. **Separazione dei dati:** Nella stessa ottica della crittografia dei dati, le organizzazioni dovrebbero sempre cercare di mantenere la separazione dei dati in fase di gestione, ad esempio i dati contabili dovrebbero essere conservati in una cartella separata e crittografata rispetto ai dati utente o dei dipendenti, il che ci porta al nostro punto successivo.

3. **Controllo dell'accesso:** Un altro punto chiave per mantenere al sicuro i dati è assicurarsi che l'accesso ad essi sia controllato. I dati dovrebbero essere accessibili solo ai membri del team o ai dipendenti che ne hanno bisogno. Non solo è inutile che un membro del team del dipartimento contabile possa accedere a password e informazioni rilevanti solo per il dipartimento IT, e viceversa, ma costituisce anche un ulteriore possibile punto di attacco per una violazione. Se George, un contabile della nostra organizzazione, viene attaccato e un hacker ottiene accesso al suo dispositivo, è molto più sicuro che l'hacker possa accedere solo alla cartella Contabilità, piuttosto che a ogni dato disponibile per l'organizzazione.

In termini di integrità dei dati e per garantire che un incidente o una circostanza imprevista non comporti una perdita totale, alcune azioni importanti da intraprendere sono:

* Eseguire regolari backup e ripristino di tutti i dati. Questi backup dovrebbero essere crittografati e conservati sul cloud o persino in un'unità locale fuori sede.
* Seguire il metodo 3-2-1: 3 copie dei dati, in 2 diversi formati multimediali, con almeno 1 copia conservata fuori sede.

### **Prevenzione di Futuri Incidenti**

Ora che abbiamo esaminato come mantenere al sicuro i nostri dati e mitigare i danni in caso di attacco, un altro punto chiave nella risposta agli incidenti è la prevenzione di ulteriori incidenti e attacchi. In caso di attacco, un modo efficace per garantire che non si verifichino ulteriori incidenti è rintracciare le cause della violazione o dell'incidente e attuare una soluzione specifica per il problema. Come regola generale da seguire, dopo aver subito un incidente, le organizzazioni dovrebbero seguire una procedura simile a quando indagano per la prevenzione, tenendo presente il contesto dell'attacco avvenuto. Oltre a una verifica e audit generale della situazione di sicurezza informatica dell'organizzazione, è consigliabile offrire formazione aggiuntiva ai membri interessati, mettendo a disposizione risorse e workshop per garantire che tutti abbiano informazioni e contesti aggiornati. Questo è particolarmente vero per la vittima iniziale dell'attacco, a cui dovrebbe essere offerta formazione senza farla sentire meno per aver commesso l'errore in primo luogo. Per riassumere, i punti chiave nella prevenzione di ulteriori incidenti dopo un attacco sono:

* **Risoluzione dei fattori causali dell'incidente**
* **Revisione e verifica dettagliata della sicurezza a livello aziendale**
* **Ulteriore formazione e preparazione dei dipendenti per una maggiore cybersicurezza**
* **Formazione della vittima dell'attacco (se applicabile)**

### **Conclusioni**

In conclusione, i passaggi più importanti nello sviluppo di una procedura per la risposta agli incidenti consistono nel stabilire confini e ruoli corretti e appropriati prima che possa verificarsi un incidente, poiché molti dei punti che impediranno ulteriori danni o problemi durante una violazione sono gli stessi punti enfatizzati nella maggior parte della cibersicurezza e della sicurezza in generale. Dobbiamo sempre tenere a mente la sicurezza dei dati e dei dipendenti quando redigiamo una policy, rendendola il più chiara e concisa possibile per evitare errori nella sua implementazione.

## **5.3 Data investigation**

Dopo aver subito un incidente, una parte importante della risposta è la comprensione. Senza capire cosa è successo e perché, come possiamo risolvere un problema? Con questo in mente, l'indagine dei dati è fondamentale per capire il come e il perché di un attacco. Esaminiamo alcuni dei principali fattori nell'indagine di un attacco o di una violazione.

### **Organisational Investigation**

La più importante e primaria indagine di un incidente dovrebbe essere condotta internamente, da parte degli specialisti IT/cybersecurity dell'organizzazione, per comprendere meglio il contesto dell'incidente e come risolverlo. Alcuni dei principali passi da compiere in casi come questi sono:

1. Se la violazione proviene da una fonte o causa sconosciuta, controllare i registri (logs) dei dispositivi interessati o del server principale, a seconda degli effetti della violazione.

2. Se la fonte e/o la causa sono già note, analizzare come si è verificato l'attacco e il funzionamento del software utilizzato per l'attacco. È importante capire le differenze, poiché la risposta a un ransomware è molto diversa da un attacco Man-in-the-Middle e dovrebbe quindi essere trattata come incidenti molto diversi.

3. Se si sospetta che l'attacco sia avvenuto tramite una persona o un dispositivo non autorizzato nella rete, è possibile utilizzare software di mappatura o tracciatura della rete, come Wireshark, per individuare la fonte dell'attacco.

Oltre all'indagine tecnica, è importante investigare i membri e i dipendenti. No, non preoccupatevi, non dobbiamo interrogarli! Con "indagine", intendiamo un breve controllo delle postazioni di lavoro per vedere se potrebbero essere stati anch'essi colpiti, nonché un'indagine sulla loro conformità alle politiche dell'organizzazione per assicurarsi che comprendano le principali misure di sicurezza adottate. Facendo ciò, agevoliamo una migliore comprensione da parte di tutti i membri del team e dei dipendenti, dalle vittime al team di indagine, fino ad altri possibili soggetti interessati.

### **External Investigation**

Molto spesso saremo in grado di indagare su tutti gli incidenti internamente e risolvere i problemi senza l'assistenza esterna, ma in alcuni casi, soprattutto in organizzazioni non governative o organizzazioni giovanili, potremmo avere bisogno dell'assistenza di una società specializzata in sicurezza informatica o protezione dei dati per risolvere il nostro problema, specialmente se l'origine dell'attacco ci è sconosciuta e l'attacco è di tipo ricorrente (un attacco che ferma la produttività o impedisce all'organizzazione di lavorare può essere un problema serio, specialmente se non viene risolto il prima possibile). A tal fine, abbiamo varie opzioni:

* **Contattare le forze dell'ordine non di emergenza per segnalare il crimine e richiedere assistenza e un'indagine:** a causa della natura digitale, molte persone non tengono conto del fatto che i reati informatici sono proprio questo: reati! Gli agenti di polizia dovrebbero essere in grado di assistervi, e in molte città e località, dispongono persino di reparti dedicati alla sicurezza informatica.
* **Richiedere l'aiuto di specialisti esterni:** se le forze dell'ordine non possono aiutarti, un'altra opzione efficace è cercare società di sicurezza informatica vicino a te o che possano assistere la tua organizzazione nella risoluzione dei problemi. L'ostacolo per questo tipo di consulenza in molte organizzazioni è di natura finanziaria, quindi non è sempre un'opzione, ma più una "soluzione estrema" se la polizia non può aiutare con il problema.

### **Cosa cercare**

Nella maggior parte dei casi, in un contesto di risposta agli incidenti, dovremmo cercare qualsiasi cosa "strana" o al di fuori della normale routine e procedura. Questo potrebbe essere qualsiasi cosa, dal ricevimento di una strana email da parte di un dipendente, fino a un attacco più estremo come un attacco man-in-the-middle che prende il controllo della nostra rete, individuato mappando la rete e controllando tutti i dispositivi.

Non esiste un singolo elemento universale da cercare in un'indagine di risposta agli incidenti, da qui la necessità di personale preparato con la conoscenza per condurre le indagini e che sa cosa aspettarsi. Il numero di variabili in qualsiasi operazione digitale è troppo elevato per individuare una singola chiave da cercare. Ecco perché è importante che le indagini interne riescano a raccogliere e comprendere i processi in corso in un'organizzazione per individuare poi le deviazioni o le variazioni.

### **Conclusioni**

Per riassumere questa sezione, un'indagine su tutte le informazioni relative a un attacco o a una violazione è fondamentale per risolverlo. Se l'indagine non porta a risultati, l'attacco potrebbe persistere o ripresentarsi e colpire l'organizzazione a un livello ancora più profondo. Nella maggior parte dei casi, si preferisce un'indagine interna, ma molte volte è importante contattare le forze dell'ordine e informarle se potrebbero essere stati commessi reati gravi, o soprattutto se persone sono in pericolo.

## **5.4 Tecniche di Mitigazione**

Una delle chiavi della risposta agli incidenti in tempo reale (e, come discusso in precedenza, della riduzione dei danni) è la mitigazione dell'attacco mentre si sta verificando. L'idea alla base di ciò è quella di impedire che l'attacco si diffonda ad altri dispositivi e causi un problema ancora più grande di quanto inizialmente accada. Ci sono alcuni metodi principali di mitigazione, quindi diamo un'occhiata!

### **Isolazione**

L'isolamento è un metodo estremo ma rapido per garantire che il malware di qualsiasi tipo non possa diffondersi ad altri dispositivi nella rete o connessi in alcun modo. La procedura standard per l'isolamento comporterebbe la disconnessione completa del dispositivo interessato dalla rete per interrompere i contatti con altri dispositivi e assicurarsi che non possa diffondere il malware che lo sta influenzando ad altre macchine o persino al nostro server principale. Possiamo pensare all'isolamento come a impedire a una persona malata di diffondere la sua malattia ad altre persone tenendola separata.

### **Contenimento**

La contenimento può essere simile all'isolamento, ma offre una gamma più complessa di risposte. Può variare dall'isolamento e dalla chiusura di un sistema, ma spesso è visto più come il controllo dell'accesso o del controllo di determinati sistemi per evitare che l'attacco si diffonda. Se l'isolamento è il separare qualcuno per assicurarsi che nessun altro si ammali, la contenimento è più simile a cambiare le serrature di casa se ti rubano le chiavi. Molte volte, la contenimento può essere considerata preferibile all'isolamento, poiché attraverso il controllo dell'accesso non dobbiamo incapacitare il dispositivo o la macchina interessata.

### **Segmentazione**

A differenza della contenimento o dell'isolamento, la segmentazione mira a mitigare i danni di un attacco prima che si verifichi un incidente. In questo senso, è più un metodo predittivo di mitigazione dei danni, ma spesso viene combinato con altri metodi se si verifica un incidente. La segmentazione segue i principi della creazione di "cluster" da VLAN o altri metodi, suddividendo la rete di un'organizzazione in reti più piccole e gestibili, consentendo loro di essere trattate in modo diverso in termini di controllo dell'accesso, punti di accesso e mitigazione dei possibili danni a un cluster, impedendo che si diffondano agli altri. In questo senso, l'isolamento viene spesso utilizzato se un cluster subisce un attacco per impedire che gli altri membri del cluster vengano infettati da malware.

### **Conclusioni**

Per riassumere come mitigare i danni in caso di attacco, se volessimo stabilire un ordine in cui impiegare questi metodi, potremmo iniziare dalla Segmentazione, guardando avanti nel caso in cui subissimo un attacco, e poi passare alla Contenimento, limitando i danni se subissimo un incidente. Se questi due metodi non ci mantengono al sicuro, allora l'Isolamento sarebbe il modo migliore per procedere fino a quando il problema non viene risolto, per garantire che altri non siano influenzati dall'attacco o dalla violazione.

## **5.5 Forense Digitale**

### **Aspetti Principali**

Abbiamo parlato di Indagine sui dati e di raccolta di informazioni, ma conosciamo la procedura per investigare? La Digital Forensics offre un quadro entro cui possiamo investigare e riferire su eventuali problemi di sicurezza informatica subiti, o addirittura anticipare problemi individuandoli prima che un aggressore lo faccia. In questo modo, la Digital Forensics ci offre un metodo da seguire nelle indagini per assicurarci di coprire tutti i nostri punti critici.

### **Le 4 Fasi dell’Informatica Forense**

#### Collezione

Raccogliere e proteggere le prove digitali da dispositivi come computer e smartphone utilizzando tecniche adeguate per preservarne l'integrità.

#### Esaminazione

Esaminare le prove utilizzando strumenti forensi per recuperare file eliminati, analizzare i registri di sistema e ricostruire le attività dell'utente al fine di trovare informazioni rilevanti.

#### Analisi

Analizzare le informazioni acquisite attraverso la nostra raccolta e individuare una possibile soluzione per la problematica riscontrata, attraverso modifiche alle policy o revisioni tecniche.

#### Reporting

Redigere e sviluppare una documentazione dettagliata riguardo all'indagine, sia da presentare come soluzione che da conservare come documentazione della procedura e da integrare nelle procedure e politiche di sicurezza dell'organizzazione.

### **Conclusioni**

La digital forensics è una parte fondamentale di qualsiasi indagine e/o risposta a incidenti, in modo da consentire una soluzione a un problema e prevenire il ripetersi di attacchi o incidenti. Seguendo le 4 fasi, possiamo raccogliere informazioni che ci consentiranno di formulare un piano per l'incidente verificatosi, nonché aiutare a elaborare strategie per il futuro.

## **L’angolo del Geek**

Per coloro interessati, ecco un elenco di alcuni kit di strumenti per la risposta agli incidenti popolari e le loro caratteristiche:

* [Cynet](https://www.cynet.com/partners/cynet-for-incident-responders/) : An all-encompassing package that allows administrators to get a wide view of their system and understand and further resolve incidents or attacks. Cynet also provides a 24/7 team to assist in incident response.
* [Cyphon](https://www.cyphon.io): Un pacchetto completo che consente agli amministratori di ottenere una visione ampia del proprio sistema e comprendere e risolvere ulteriormente incidenti o attacchi. Cynet fornisce anche un team attivo 24 ore su 24 per assistere nella risposta agli incidenti.
* [GRR](https://grr-doc.readthedocs.io/en/v3.3.0/what-is-grr.html): È il framework di Google che consente agli analisti di condurre indagini forensi remote in tempo reale. Aiuta anche le squadre di risposta agli incidenti a intervenire in modo rapido ed efficiente per una valutazione più veloce e un'analisi remota. Comprende due parti: il client GRR, che viene distribuito sul sistema da investigare, e il server GRR, che aiuta gli analisti a eseguire azioni e elaborare i dati raccolti.
* [TheHive Project](https://thehive-project.org/): È una piattaforma IR open source gratuita che consente a diversi analisti di lavorare contemporaneamente sulle indagini sugli incidenti. Fornisce agli analisti la possibilità di impostare notifiche per i nuovi compiti assegnati e di visualizzare nuovi eventi e avvisi da diverse fonti, come riepiloghi via email e avvisi SIEM. I modelli integrati consentono agli analisti di ottenere informazioni chiave e individuare le misure corrette da prendere per una soluzione più rapida.

Strumenti e framework come questi rappresentano un ottimo punto di partenza per prepararsi a qualsiasi incidente o attacco che possa verificarsi. Esistono molte altre opzioni e strumenti, e questi sono solo alcuni. Ne conosci altri?

# **Conclusioni**

La chiave per affrontare qualsiasi incidente o attacco è la preparazione. Se abbiamo una procedura definita prima di un attacco, limitiamo il danno che un incidente può causare al nostro sistema. Definendo, comprendendo ed attuando una procedura di risposta agli incidenti, ci assicuriamo che il nostro team sappia cosa fare nel caso accada il peggio. Dopotutto, non importa quanto ci prepariamo, qualcosa può sempre andare storto inaspettatamente!

## **Quiz**

**È necessario un piano di risposta agli incidenti se abbiamo una sicurezza molto forte?**

a) No, non saremo attaccati con una buona sicurezza.

b) Non proprio, possiamo averne uno se vogliamo, ma non ne abbiamo bisogno.

c) Sì, ma solo per incidenti specifici.

**d) Sì, dovremmo sempre avere una politica di risposta agli incidenti, poiché questa fa parte di un solido sistema di sicurezza informatica.**

**Quali sono le 4 fasi della Digital Forensics?**

**a) Raccolta, Esame, Analisi e Reporting.**

b) Raccolta, Cancellazione, Analisi e Smaltimento.

c) Esame, Reporting, Riparazione e Ricerca della soluzione.

d) Cancellazione, Recupero, Riavvio e Reporting.

**Quale di questi non è una tecnica di mitigazione?**

**a) Disattivazione.**

b) Segmentazione.

c) Contenimento.

d) Isolamento.

**Una politica di risposta agli incidenti mira non solo a mitigare i danni, ma anche a prevenire ulteriori incidenti.**

**a) Vero.**

b) Falso.

**Qual è il termine per un tipo di attacco informatico in cui un aggressore intercetta la comunicazione tra due parti al fine di rubare informazioni sensibili?**

**a) Attacco Man-in-the-Middle (MitM).**

b) Attacco Cross-Site Scripting (XSS).

c) Attacco Cross-Site Request Forgery (CSRF).

d) Attacco Ransomware.

## **Fonti**

United States Securities and Exchange Commission. (2018). Equifax Inc. Form 8-K: Current report filing (Amended). Retrieved from: <https://www.sec.gov/Archives/edgar/data/33185/000119312518154706/d583804dex991.htm>