Università degli studi di Torino

SCUOLA DI SCIENZE DELLA NATURA

Corso di Laurea in Informatica

Tesi di Laurea Triennale

STRUMENTI E METODOLOGIE DI ANALISI PER LA SICUREZZA DELLE APPLICAZIONI WEB

Relatore:
Chiar.mo Prof.
Matteo Sereno

Controrelatore:
Prof.
Zio Paperone

Candidato:
Alessio Minoi

Anno Accademico 2021/2022

Ringrazio me e me stesso
per il sostegno avuto Author, *Title*

Prova nella prova

Facciamo una prova testuale per vedere se funzionano tutte le modifiche che voglio apportare

Italian abstract

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vestibulum nec augue tincidunt, sodales lorem fringilla, venenatis metus. Cras dictum nec urna vitae euismod. Nunc vulputate quam dolor, id convallis augue convallis sit amet. Aliquam nec felis sodales, condimentum massa ac, tincidunt nisi. Vestibulum posuere, lacus tempus facilisis cursus, velit libero mattis diam, vel aliquet magna turpis vitae ligula. Maecenas aliquet nulla at gravida mattis. Morbi vestibulum in ex sed ultricies. Morbi sodales mollis mauris, vitae tincidunt enim hendrerit et. Interdum et malesuada fames ac ante ipsum primis in faucibus. Suspendisse laoreet faucibus massa, quis elementum enim eleifend aliquet. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Etiam at tortor vestibulum, dictum augue ut, porta lorem. Sed venenatis feugiat diam. Integer eu diam nec dolor viverra hendrerit.

Vestibulum quis vehicula massa. Etiam dictum, enim vel luctus accumsan, dolor velit laoreet metus, nec pretium arcu dui nec nulla. Donec ac sollicitudin justo, ut ullamcorper nunc. Curabitur ornare, ipsum hendrerit dictum rutrum, nisl lectus cursus sapien, in condimentum ipsum magna vel lorem. Cras vulputate semper placerat. In nec quam condimentum, auctor nisl eu, viverra libero. Maecenas scelerisque, odio vel accumsan luctus, justo dui pharetra orci, sit amet feugiat lorem lacus ac enim. Donec ultrices nulla semper erat consectetur, vitae mattis nulla dictum. Fusce maximus tristique condimentum. Quisque et sodales lectus, vel posuere leo. In ac augue vel neque sagittis volutpat at nec justo. Proin bibendum lobortis neque, vitae vulputate lorem viverra in. Etiam neque risus, pretium sed tempor a, pharetra quis arcu. Morbi purus nibh, efficitur nec sollicitudin non, commodo vel massa.

Pellentesque eu neque lacus. Vivamus finibus consectetur tellus id imperdiet. In ut dolor ligula. Vivamus ac vehicula erat. Duis semper lacinia eros, sed ultrices orci tristique at. Proin in pellentesque massa. Nunc ultricies justo eget nibh condimentum sollicitudin. Mauris non ligula eget magna pulvinar pretium vel vitae ante. Aenean lacinia metus vel odio vehicula sollicitudin. Quisque nisi augue, faucibus a nulla faucibus, consequat vehicula elit. Donec dui mi, ornare quis sapien ac, finibus maximus mi. Etiam volutpat, arcu quis posuere sollicitudin, ligula elit tincidunt lectus, non dapibus augue nunc id est. Ut dictum et diam vel vulputate. Aliquam ut nibh eu nibh aliquet aliquam eget ut leo. Duis urna tellus, sodales non ornare ut, aliquet vitae mi. Nunc consequat est vitae elit consectetur, id iaculis libero congue.

Praesent sem neque, semper ac turpis eu, fringilla egestas erat. Fusce in leo velit. Sed faucibus viverra massa. Donec justo lorem, accumsan a nisi in, maximus placerat augue. Mauris posuere aliquet sapien sed viverra. In hac habitasse platea dictumst. Ut nec dictum purus, sit amet gravida risus.

Indice

Capitolo 1

Vulnerabilità e attacchi

1.1 Vulnerabilità

Una **vulnerabilità informatica** può essere intesa come una componente (esplicita o implicita) di un sistema informatico, in corrispondenza alla quale le misure di sicurezza sono assenti, ridotte o compromesse, il che rappresenta un punto debole del sistema e consente ad un eventuale aggressore di compromettere il livello di sicurezza dell'intero sistema.
Essa può indicare una debolezza che può consentire un possibile **attacco informatico** di compromettere un sistema, cioè di ridurre il livello di protezione fornito da tale sistema, fino al caso limite di inficiare il funzionamento.

1.1.1 Ciclo di vita

Le vulnerabilità attraversano un ciclo di vita che passa attraverso la scoperta e finisce con l'installazione del fix su sistemi affetti, passando per quattro fasi principali:

1. **Creazione**: la vulnerabilità nasce nel momento in cui viene scritto del codice contenente un errore e e tale codice viene rilasciato. In questa fase la vulnerabilità non rappresenta un problema, poiché nonostante esista non è nota, quindi non sfruttabile.

2. **Scoperta**: può avvenire in vari modi, anche per caso, e anche ad opera di soggetti malevoli. Da questo momento si parla di vulnerabilità e non più di errore nel codice.

3. **Diffusione**: viene condivisa la conoscenza delle vulnerabilità e il problema assume carattere globale. in questa fase vengono spesso creati automatismi e tool per sfruttare la vulnerabilità, permettendo ad utenti anche meno esperti di lanciare con successo un attacco. Proprio in questo momento gli attacchi aumentano esponenzialmente.

4. **Patch deploy**: il produttore del sistema elabora e pubblica un aggiornamento che risolve il bug nel codice.

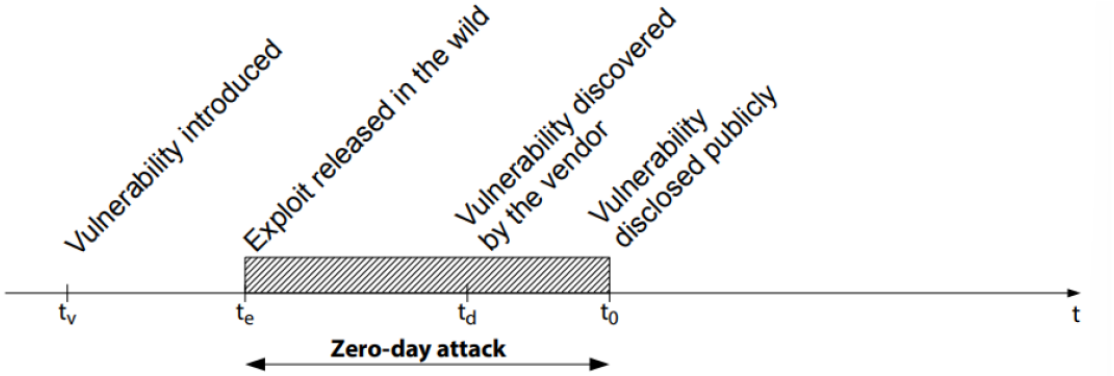

Figura 1.1

La scoperta di nuove vulnerabilità viene chiamata **vulnerabilità zero-day**, questo implica che tutti i sistemi sono soggetti ad una finestra di esposizione alla vulnerabilità. Il numero di **attacchi zero-day**, nel periodo $[t_e, t_0]$(figura1.1), aumenta rapidamente e ciò è dovuto alla rapida diffusione di conoscenza e alla creazione di **Exploit zero-day** [1] che permettono ad utenti meno esperti di sfruttare con successo tale vulnerabilità. Quando una vulnerabilità diventa nota, gli sviluppatori creano una patch per cercare di fermare l'attacco, ma spesso potrebbe passare del tempo prima che la patch venga rilasciata. Infatti capita spesso che le patch interferiscano con il corretto funzionamento dei sistemi o dei software installati, creando non pochi disagi; ciò comporta una preventiva fase di test su un numero limitato di macchine, e solo dopo accurati test un rilascio massivo a tutti i sistemi della società.

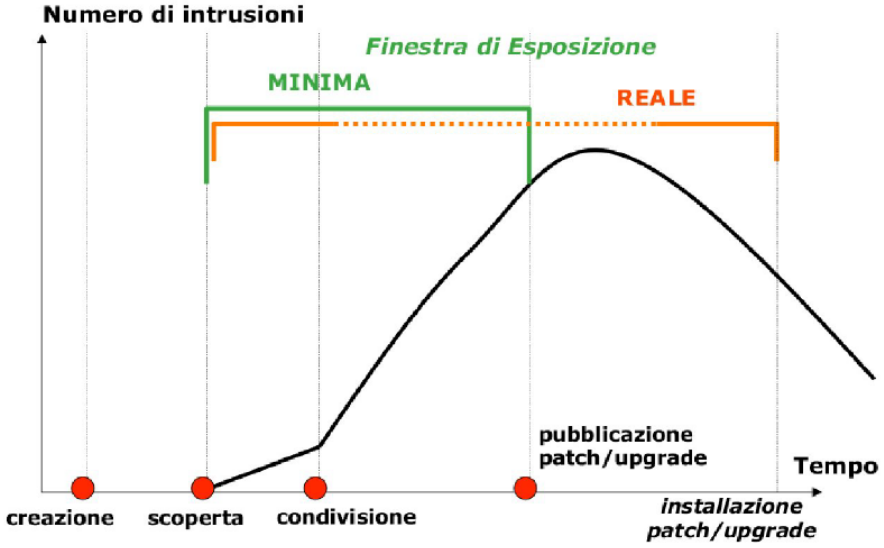

Figura 1.2: Ciclo di vita di una vulnerabilità

[1] è un qualunque programma che sfrutti una vulnerabilità zero-day per causare effetti indesiderati.

1.1.2 Obiettivi degli exploit zero-day (non so se tenerla o no)

Un attacco zero-day può sfruttare le vulnerabilità di svariati sistemi, tra cui:

- Sistemi Operativi
- Browser Web
- Applicazioni Office
- Componenti open-source
- Hardware e firmware
- Internet of Things

Esiste per tanto un'ampia gamma di potenziali vittime:

- Singoli utenti che utilizzano un sistema vulnerabile
- Singoli utenti che accedono a dati aziendali importanti
- Dispositivi hardware, firmware e Internet of Things
- Aziende e organizzazioni di grandi dimensioni
- Agenzie governative
- Obiettivi politici

È utile comprendere due tipologie di attacchi zero-day:

- Gli attacchi zero-day **mirati** hanno obiettivi potenzialmente di valore, ad esempio grandi organizzazioni, agenzie governative o persone di alto profilo.
- Gli attacchi zero-day **non mirati** sono invece rivolti contro utenti di sistemi vulnerabili, ad esempio un sistema operativo o un browser.

Anche quando gli autori degli attacchi non prendono di mira utenti specifici, moltissime persone possono tuttavia rimanere vittime di **attacchi zero-day**, solitamente come danno collaterale.

1.1.3 Identificare gli attacchi zero-day

Può essere difficile individuare le vulnerabilità zero-day, dal momento che possono assumere diverse forme. Data la natura di questi tipi di vulnerabilità, le informazioni dettagliate sugli exploit zero-day sono disponibili solo dopo che sono stati identificati. Le organizzazioni vittime di un exploit zero-day potrebbero notare traffico imprevisto o un'attività sospetta di scansione originata da un client o un servizio. Alcune delle tecniche di rilevamento zero-day includono:

1. Si utilizza come riferimento di database esistenti di malware che ne descrivono anche il comportamento. Anche se questi database vengono aggiornati molto velocemente e possono essere utili come riferimento, per definizione gli exploit zero-day sono nuovi e sconosciuti. Le informazioni reperibile in un database esistente sono quindi limitate.

2. In alternativa, alcune tecniche cercano le caratteristiche dei malware zero-day in base a come interagiscono con il sistema preso di mira. Invece di esaminare il codice dei file in ingresso, questa tecnica analizza le loro interazioni con il software esistente e cerca di determinare se sono il risultato di azioni dannose.

3. Il machine learning viene sempre utilizzato per rilevare i dati dagli exploit registrati in precedenza e poter stabilire un riferimento per il comportamento di un sistema sicuro in base ai dati delle interazioni passate e attuali con il sistema. Maggiore è la quantità di dati disponibili, più affidabile sarà il rilevamento.

Spesso si utilizza una combinazione di sistemi di rilevamento diversi.

1.1.4 Come proteggersi da attacchi zero-day

Per la protezione zero-day e la sicurezza del computer e dei dati, è essenziale sia per i singoli utenti che per le organizzazioni seguire delle **best-practice**, tra cui:

1. **Mantenere aggiornati tutti i software e i sistemi operativi.** I fornitori includono infatti nelle nuove versioni patch di sicurezza che coprono le vulnerabilità appena identificate. Mantenere i sistemi informatici aggiornati garantisce una sicurezza ancora maggiore.

2. **Usare solo le applicazioni essenziali.** Più software si utilizzano, maggiori saranno le potenziali vulnerabilità. Per ridurre i rischi nella propria rete, utilizzare solo applicazioni necessarie.

3. **Usare un firewall.** Un firewall [2] svolge un ruolo essenziale nella protezione del sistema dalle minacce zero-day.

4. **Educare gli utenti nelle organizzazioni.** Molti attacchi zero-day sfruttano l'errore umano. Insegnare ai dipendenti e utenti buone abitudini di sicurezza li proteggerà dalle minacce digitali.

1.1.5 CVE

Il **CVE** è un acronimo che sta per **Common Vulnerabilities and Exposures** e si tratta di un progetto finanziato dal Dipartimento di Sicurezza Nazionale Statunitense e dall'agenzia di Cybersecurity e Infrastructure Security. Si tratta di un database pubblico nel quale vengono aggiunte e aggiornate vulnerabilità in modo che chiunque possa accedervi e utilizzarlo. É un tool molto utile e viene utilizzato come standard per

[2] specificare il firewall cos'è

vari istituti di ricerca nel mondo. Ogni vulnerabilità inserita nel CVE, come vedremo successivamente, ha dei parametri di classificazione. Uno dei più importanti è il CVSS ovvero **Common Vulnerability Scoring System** cioè uno standard che indica la gravità di una vulnerabilità informatica da 0 a 10. I parametri col quale viene calcolato il CVSS sono:

- Vettore d'attacco (AV)
- Complessità dell'attacco (AC)
- Permessi richiesti (PR)
- Interazione da parte dell'utente (UI)
- Impatto in termini di confidenzialità delle informazioni, integrità dei sistemi e funzionalità dei sistemi.

Vengono utilizzati degli **identificatori CVE**,sono dei codici che identificano in modo univoco ogni vulnerabilità in sicurezza informatica. Gli identificatori possono avere lo status di voci, entry, o candidati, candidates a seconda che siano stati inseriti negli elenchi CVE o che siano sotto verifica per poi essere inclusi. Gli identificatori CVE vengono rilasciati a falle che soddisfano certi criteri:

- **Sono correggibili in modo indipendente**: cioè la vulnerabilità può essere corretta in modo indipendente da un qualsiasi altro bug.
- **Riconosciute dal produttore**: cioè il produttore o fornitore del software/hardware attesta che il bug esiste che ne conferma il potenziale impatto negativo sulla sicurezza;in alternativa chi segnala la vulnerabilità in maniera autonoma può produrre un report nel quale prova l'impatto negativo di quel bug, mostrando l'impatto negativo che ha avuto nella sicurezza del sistema.
- **Con impatto su un codebase**: alle falle che colpiscono più di un prodotto vengono assegnati CVE distinti. In presenza di librerie, protocolli o standard condivisi, alla falla viene assegnato un unico CVE soltanto nel caso in cui sia impossibile utilizzare il codice condiviso senza dare seguito a vulnerabilità. Al contrario, a ogni codice o prodotto interessato dalla falla viene assegnato un CVE unico.

Il **Common Vulnerability Scoring System** è, uno standard che certifica il livello di gravità di una particolare vulnerabilità inserita all'interno degli elenchi CVE. Il CVSS è costituito da tre gruppi metrici: Base, Temporale e Ambientale. Le metriche Base generano un punteggio compreso tra 0 e 10, che può quindi essere modificato assegnando un punteggio alle metriche Temporale e Ambientale. Un punteggio CVSS è anche **rappresentato come una stringa vettoriale** cioè una rappresentazione testuale compressa dei valori utilizzati per derivare il punteggio. Pertanto, CVSS è adatto come **sistema di misurazione standard** per industrie, organizzazioni e governi che necessitano di punteggi di gravità della vulnerabilità accurati e coerenti. Il **National Vulnerability Database** (NVD) fornisce punteggi CVSS per quasi tutte le vulnerabilità.

1.2 Attacchi informatici

L'**attacco informatico** viene definito come il tentativo di ottenere un accesso non autorizzato a servizi, risorse o informazioni di sistema e/o di compromettere l'integrità e, in generale, consiste nell'atto intenzionale di tentare di eludere uno o più servizi di sicurezza o i controlli di un sistema informativo digitale per alterare la riservatezza, l'integrità e la disponibilità dei dati.

1.2.1 I 10 attacchi più comuni

Denial-of-service DoS e Distributed denial-of-service DDoS

un attacco di DoS sovrasta le risorse di un sistema in modo che non possa rispondere alle richieste di servizio. Un attacco DDoS è anche un attacco alle risorse del sistema, ma è lanciato da un gran numero di macchine host che sono infettate da un software maligno controllato dall'attaccante. Il DoS non fornisce benefici diretti agli attaccanti, ma bensì punta a bloccare un servizio offerto da una compagnia o azienda.
Esistono diverse tipologie di attacchi DoS e DDoS, i più comuni sono:

- **Attacco TCP SYN flood**: un attaccante sfrutta l'uso dello spazio buffer durante un protocollo **handshake** di inizializzazione della sessione **TCP**. Il dispositivo attaccante inonda la coda in-process del sistema inviando tante richieste di connessione, ma non risponde quando il sistema di destinazione risponde a tali richieste. Questo fa sì che il sistema di destinazione vada in time-out mentre aspetta la risposta da parte dell'attaccante, in tal modo il sistema si blocca o diventa inutilizzabile quando la coda di connessione si riempie.
  Contromisure: utilizzare un firewall configurato per bloccare i pacchetti SYN in entrata, aumentare la dimensione della coda di connessione e diminuire il timeout sulle connessioni aperte.

- **Attacco Teardrop**: questo attacco fa sì che i campi di lunghezza e di offset di frammentazione dei pacchetti sequenziali **IP** si sovrappongono l'uno all'altro sull'host attaccato;il sistema attaccato tenta di ricostruire i pacchetti anche durante il processo, ma non ci riesce, finendo così per bloccarsi. **Contromisure**: se non ci sono patch a disposizione bloccare le porte 139 e 445.

- **Attacco Smurf**: questo attacco comporta l'utilizzo di **IP spoofing**[3] e **ICMP**[4] per saturare una rete bersaglio con il traffico. Questo attacco utilizza **echo request ICMP** mirate ad indirizzi **IP broadcast**. Tutti i dispositivi collegati al broadcast invieranno una **echo respond ICMP all'IP spoofato**, quindi a a riceverle non sarà il dispositivo attaccante, ma bensì sarà il dispositivo a cui hanno spoofato l'indirizzo IP.
  Contromisure: è necessario disabilitare i broadcast diretti agli IP ai router. Questo impedirà che la richiesta di broadcast ICMP echo arrivi ai dispositivi

[3] riuscire a sottrarre l'IP ad un altro dispositivo collegato alla rete, fingendosi tale dispositivo in modo tale da ingannare la vittima dell'attacco

[4] Aggiungere qualcosa su ICMP

di rete, altra opzione è quella di configurare gli endpoint per impedire loro di rispondere ai pacchetti ICMP da indirizzi broadcast.

- **Attacco Ping of Death**: questo tipo di attacco utilizza pacchetti IP per pingare un sistema bersaglio con una dimensione IP superiore al massimo di 65.535 byte. I pacchetti IP di questa dimensione non sono consentiti, quindi l'attaccante frammenta il pacchetto IP. Una volta che il sistema di destinazione riassembla il pacchetto, si possono verificare buffer overflow e altri crash.
  Contromisure: possono essere bloccati attraverso l'utilizzo di un firewall che controlli la dimensione massima dei paccheti IP frammentati.

- **Botnet**: le botnet sono i milioni di sistemi infettati con malware sotto il controllo degli hacker, utilizzate per effettuare attacchi DDoS. Questi bot vengono utilizzati per effettuare attacchi contro i sistemi di destinazione, spesso riempiendo la larghezza di banda e le capacità di elaborazione del sistema di destinazione. Questi attacchi sono difficili da tracciare perché le botnet si trovano in diverse località geografiche.
  Contromisure: possono essere mitigate da:
  - **Filtri RFC3704**: che negherà il traffico da indirizzi spoofed e aiuterà a garantire che il traffico sia tracciabile fino alla sua corretta rete di origine.
  - **Black hole filtering**: che blocca il traffico indesiderato prima che entri in una rete protetta. Quando viene rilevato un attacco DDoS, l'host BGP (Border Gateway Protocol) dovrebbe inviare aggiornamenti di routing ai router degli ISP in modo che indirizzino tutto il traffico diretto ai server vittime verso un'interfaccia null0 all'hop successivo.

Attacco Man-in-the-Middle MitM

si verifica quando un hacker si inserisce tra le comunicazioni di un un client e un server. Ecco alcuni tipi comuni di attacchi MitM:

- **Dirottamento della sessione**: in questo tipo di attacco MitM, un attaccante dirotta una sessione tra un client fidato e un server di rete. Il computer attaccante sostituisce il suo indirizzo IP con quello del client fidato, mentre il server continua la sessione, credendo di comunicare con il client.

- **IP spoofing**: l'IP spoofing è usato da un attaccante per convincere un sistema che sta comunicando con un'entità nota e fidata e fornisce quindi all'attaccante l'accesso al sistema. L'attaccante invia un pacchetto con l'indirizzo sorgente IP di un host noto e fidato invece del proprio indirizzo sorgente IP ad un host di destinazione. L'host potrebbe accettare il pacchetto e agire di conseguenza, concedendo l'accesso.

- **Replay**: un attacco di replay si verifica quando un attaccante intercetta e salva vecchi messaggi e poi cerca di inviarli in seguito, impersonando uno dei partecipanti.

Contromisure: attualmente non esiste una tecnologia o configurazione per prevenire tutti gli attacchi MitM. In generale, la crittografia e i certificati digitali forniscono un'efficace salvaguardia contro gli attacchi MitM, assicurando sia la riservatezza che l'integrità delle comunicazioni.

Attacchi di phishing e spear phishing

l'attacco di phishing è la pratica di inviare e-mail che sembrano provenire da fonti affidabili con l'obiettivo di ottenere informazioni personali o influenzare gli utenti a compiere delle azioni. Potrebbe essere una mail che carica un malware sul tuo computer, oppure un link a un sito web illegittimo che può indurti a scaricare malware o sottrarti le tue informazioni personali. Lo spear phishing è un tipo di attività di phishing molto mirata. Gli attaccanti si prendono del tempo per condurre delle ricerche sugli obiettivi e creare messaggi che siano personali e rilevanti. Per questo motivo, lo spear phishing può essere molto difficile da identificare ed è ancora più difficile proteggersi. **Contromisure**: Per ridurre il rischio di essere vittima di phishing, puoi usare queste tecniche:

- **Pensiero critico**: non valutare una mail in maniera affrettata, fermarsi un minuto e analizzare l'email.
- **Analizzare il link**: applicare anche in questo caso il pensiero critico per decifrare l'URL.
- **Analizzare le intestazioni delle email**: le intestazioni delle email definiscono come una mail sia arrivata al tuo indirizzo.
- **Sandboxing**: è possibile testare il contenuto delle e-mail in un ambiente sandbox, registrando l'attività di apertura dell'allegato o cliccando sui link all'interno dell'e-mail.

Attacco drive-by

gli attacchi drive-by download sono un metodo comune di diffusione di malware. Gli hacker cercano siti web insicuri e inseriscono uno script dannoso nel codice HTML o PHP di una delle pagine.Questo script potrebbe installare malware direttamente sul computer di qualcuno che visita il sito, o potrebbe reindirizzare la vittima a un sito controllato dagli hacker. A differenza di molti tipi di attacchi alla sicurezza informatica, un drive-by non si basa sul fatto che l'utente faccia qualcosa per attivare l'attacco, come nel caso del phishing, un download può sfruttare un'app, un sistema operativo o browser web che contiene falle nella sicurezza dovute ad aggiornamenti non riusciti o alla mancanza di aggiornamenti.
Contromisure: è necessario mantenere aggiornati i browser e i sistemi operativi ed evitare i siti web che potrebbero contenere codice dannoso. Non tenere troppi programmi e app inutili sul tuo dispositivo. Più plug-in hai, più vulnerabilità ci sono che possono essere sfruttate da attacchi drive-by.

Attacco SQL injection

si verifica quando un malfattore esegue una query SQL al database attraverso i dati di input dal client al server. I comandi SQL sono inseriti nell'input del piano dati per eseguire comandi SQL predefiniti. Un exploit SQL injection riuscito può leggere dati sensibili dal database, modificare i dati del database, eseguire operazioni di amministrazione sul database, recuperare i contenuti di un dato file e, in alcuni casi, emettere comandi sul sistema operativo.
Contromisure: per proteggervi da un attacco di SQL injection, applicare il modello least0privilege dei permessi nei vostri database. Attenersi alle stored procedure e alle istruzioni preparate precedentemente. Inoltre, convalidare i dati di input in funzione di una whishlist a livello di applicazione.

Attacco cross-site scripting (XSS)

gli attacchi XSS utilizzano risorse web di terze parti per eseguire script nel browser web o nell'applicazione web della vittima. In particolare, l'attaccante inietta un payload con JavaScript dannoso nel database di un sito web. Quando la vittima richiede una pagina dal sito web, il sito web trasmette la pagina, con il payload dell'attaccante come parte del corpo HTML, al browser della vittima, che esegue lo script dannoso. Queste vulnerabilità possono permettere ad un attaccante non solo di rubare cookie, ma anche di registrare le battute di tasti, catturare screenshot, scoprire e raccogliere informazioni di rete, e accedere e controllare in remoto la macchina.
Contromisure: per difendersi dagli attacchi XSS, gli sviluppatori possono sanitizzare i dati inseriti dagli utenti in una richiesta HTTP prima di restituirli. Convertire i caratteri speciali come ?, , /, <, > e gli spazi nei loro rispettivi equivalenti codificati in HTML. Dare agli utenti la disponibilità li script lato client.

Attacco con intercettazione

gli attacchi di **eavesdropping** si verificano attraverso l'**l'intercettazione del traffico di rete**. Con l'eavesdropping, un attaccante può ottenere password, numeri di carte di credito e altre informazioni riservate che un utente potrebbe inviare in rete. L'eavesdropping può essere passivo o attivo, con **passivo** si intende un hacker che rileva delle informazioni ascoltando la trasmissione dei messaggi nella rete, mentre con **attivo** si parla di un hacker che recupera attivamente le informazioni camuffandosi da endpoint[5] amico e inviando interrogazioni ai trasmettitori.

Attacco "Birthday" del compleanno

sono fatti contro gli algoritmi di **hash** che sono usati per verificare l'integrità di un messaggio, un software o una firma digitale. Un messaggio processato da una funzione di hash produce un messaggio digest (MD) di lunghezza fissa, indipendente dalla lunghezza del messaggio di input; questo MD caratterizza in modo univoco il messaggio. L'attacco di tipo birthday si riferisce alla probabilità di trovare due messaggi casuali

[5]aggiungere roba

che generano hash. Se un attaccante calcola per il messaggio lo stesso MD dell'utente, può tranquillamente sostituire il messaggio dell'utente con il suo, e il ricevitore non sarà in grado di rilevare la sostituzione anche se confronta gli MD.

Attacco malware

il malware può essere descritto come un software indesiderato che viene installato nel sistema senza il consenso dell'utente. Può attaccarsi al codice legittimo e propagarsi, può annidarsi in applicazioni utili o replicarsi attraverso internet. Alcune tipologie:

- **Virus macro**: si attaccano alla sequenza di inizializzazione di un applicazione. Quando l'applicazione viene aperta, il virus esegue le istruzioni prima di trasferire il controllo all'applicazione.
- **Infettatori di file**:di solito si attaccano al codice eseguibile, come i file .exe. Il virus viene installato quando il codice viene caricato. Un'altra versione di un file infector si associa a un file creando un file virus con lo stesso nome, ma con estensione .exe.
- **Infettatori di sistema o di boot-record**: si attacca al master boot record sui dischi rigidi. Quando il sistema viene avviato, guarda il settore di avvio e carica il virus in memoria, dove può propagarsi ad altri dischi e computer.
- **Virus polimorfici**: si nascondono attraverso vari cicli di crittografia e decrittografia. Il virus criptato e un motore di mutazione associato sono inizialmente decrittati da un programma di decriptazione. Il motore di mutazione sviluppa quindi una nuova routine di decriptazione e il virus cripta il motore di mutazione e una copia del virus con un algoritmo corrispondente alla nuova routine di decriptazione. Il pacchetto criptato del motore di mutazione e del virus è attaccato al nuovo codice, e il processo si ripete.
- **Trojan**
- **Bombe logiche**: è un tipo di software maligno che viene aggiunto a un'applicazione e viene attivato da un evento specifico, come una condizione logica o una data e un'ora specifica.
- **Virus furtivi**
- **Dropper**:è un programma usato per installare virus sui computer. In molti casi, il dropper non è infettato da codice dannoso e, quindi, potrebbe non essere rilevato dal software di scansione dei virus.
- **Ransomware**
- **Adware**
- **Spyware**

Contromisure generali per evitare questi possibili attacchi: Le misure per mitigare queste minacce variano, ma le basi della sicurezza rimangono le stesse: mantenere aggiornati i sistemi e utilizzare sistemi di protezione endpoint di nuova generazione, formare i dipendenti, configurare il firewall per mettere in whitelist solo le porte e gli host specifici di cui avete bisogno, mantenere forti le password, usate un modello di minimo privilegio nell'ambiente IT, fare backup regolari, prevedere un sistema di disaster recovery e controllare continuamente i sistemi IT alla ricerca di eventuali attività sospette.

Capitolo 2

Come le aziende si difendono: SOC e CERT

Un aspetto particolare della Cyber Security è quella che considera la possibilità di creare e promuovere le sinergie tra le attività dei **Security Operation Center SOC** e dei **Emergency Response/Readiness Team CERT** a beneficio di un'efficace presidio degli aspetti di sicurezza informatica di una specifica realtà aziendale.

2.1 SOC

Un **Security Operations Center** è un centro da cui vengono forniti servizi finalizzati alla sicurezza dei sistemi informativi dell'azienda stessa o clienti esterni.

Un SOC fornisce tre tipologie di servizi:

- **Servizi di gestione**: tutte le attività di gestione delle funzionalità di sicurezza legate all'infrastruttura (rete, sistemi e applicazioni) sono centralizzate dal SOC.
- **Servizi di monitoraggio**: l'infrastruttura IT e di Sicurezza vengono monitorate in tempo reale al fine d'individuare tempestivamente tentativi d'intrusione, di attacco o di uso improprio dei sistemi.
- Servizi proattivi: sono servizi finalizzati a migliorare il livello di protezione dell'organizzazione.

Sono offerti anche altre tipologie di servizi dal SOC:

- **Analisi proattiva e gestione dei sistemi e delle tecnologie di sicurezza informatica**: il servizio ha come obiettivo l'analisi proattiva h24 dei sistemi e delle tecnologie di sicurezza informatica, come ad esempio **IDS, IPS, FIREWALL**. I sistemi anti-intrusione permettono la gestione centralizzata delle pratiche di sicurezza informatica consentendo di identificare potenziali attacchi informatici provenienti da internet e dalla intranet. La scalabilità degli strumenti adoperati dal SOC è un altro fattore di fondamentale importanza, non deve comportare un grosso impatti operativo aggiungere un IDS a quelli già esistenti.

- **Security Device Management**: il servizio di Security Device Management si sviluppa attorno a due principali processi:
  - **Gestione del guasto**: obiettivo principale è garantire il funzionamento continuo ed ottimale dell'infrastruttura di sicurezza del Cliente sia dal punto di vista sistemistico che dei presidi di sicurezza.
  - **Gestione della configurazione**: obiettivo principale è garantire il costante allineamento delle regole di firewalling alle esigenze del cliente e riguarda tutti gli apparati gestiti dal SOC. La gestione della configurazione comprende le attività di configurazione e modifica delle policy di filtraggio o autorizzazione al passaggio del traffico dati tra una sorgente esterna ed una fonte interna (o viceversa)
- **Reportistica**: i log provenienti dalle console o dagli strumenti utilizzati vengono solitamente analizzati e rielaborati in modo da renderli facilmente comprensibili ai clienti. Questa reportistica è particolarmente importante perché, oltre a fornire il dettaglio di eventuali tentativi di intrusione da parte dei soggetti non autorizzati o di incidenti che si sono verificati per il periodo di tempo a cui il report si riferisce, può permettere al cliente di intraprendere azione preventive.
- **Avviso di sicurezza**:il servizio è volto a notificare ai clienti, quanto prima possibile, la scoperta di nuove vulnerabilità in modo tale che possano essere prese per tempo le dovuto contromisure atte a mitigare o annullare gli impatti delle nuove vulnerabilità.
- **Mitigazione DDoS**:il servizio ha come obiettivo il mitigare le conseguenze di un attacco di tipo DDos indirizzato verso un servizio critico facente parte dell'infrastruttura di rete di un cliente. Il compito del servizio è quindi garantire, a fronte di una segnalazione ricevuta da un cliente, la corretta attivazione delle procedure necessarie per risolvere l'incidente di sicurezza. Vengono valutate le contromisure da adottate ed attivato il processo di "pulitura" e di reinstradamento del traffico.
- **Valutazione della sicurezza**: alcuni elementi di servizio fanno parte delle attività:
  - **Vulnerability assessment**: è volto ad individuare vulnerabilità note dei sistemi e dei servizi installati sugli stessi. Tale attività è svolta tramite tecnologie specifiche e che vengono configurate, perfezionate e personalizzate per ogni assessment.
  - **Penetration Test**: è svolto ad individuare e sfruttare vulnerabilità note o ancora sconosciute dei sistemi, dei servizi e degli applicativi web installati sugli stessi. Il processo di penetration test, sfruttando le vulnerabilità, è in grado di evidenziare in maniera più efficace il livello di minaccia rappresentato da ognuna di esse e la relativa stima degli impatti. Tale attività è svolta sia tramite numerose tecnologie che vengono configurate, perfezionate e personalizzate per ogni assessment, sia tramite attività manuali specifiche per ogni servizio, sistema ed applicativo analizzato.

– **Assistenza tecnica**: in genere il SOC può fornire ai clienti anche l'assistenza tecnica specialistica per tutte le problematiche legate a problemi di funzionalità, violazione di sistema, aggiornamento e configurazione di software e hardware per la sicurezza. L'assistenza tecnica per la risoluzione di queste problematiche può essere fornita da remoto o on-site a seconda delle problematiche e del contratto stipulato tra le parti.

2.1.1 Le tre aree di attività prevalenti del SOC

Le tre attività di aree di attività prevalenti sono:

- threat prevention;
- attacks detection and containment;
- security systems (or features) tuning

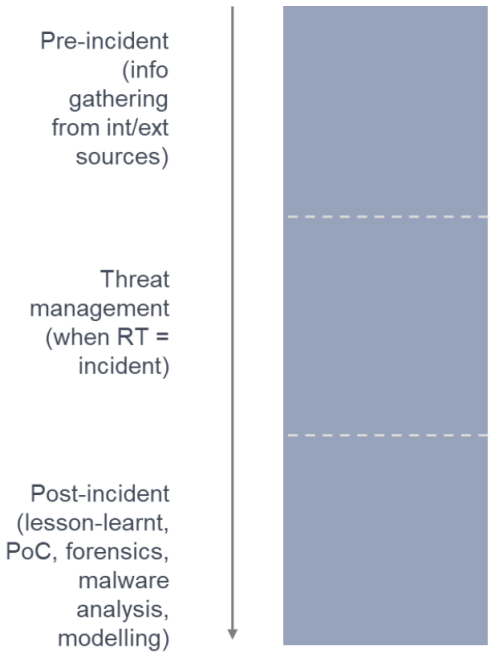

Figura 2.1

In figura 2.1, si evidenzia come l'operatività di un SOC si estenda lungo tutta la "filera" che va dalla raccolta dei dati atomici e "grezzi" sui sistemi monitorati fino alla memorizzazione/archiviazione degli stessi, e alla successiva analisi e correlazione. Tale analisi abilita un monitoraggio proattivo a vari livelli, nonché la rilevazione (detenction) di eventi di sicurezza informatica complessi, che possono o meno concretizzarsi in incidenti e per i quali è necessario innescare un'opportuna reazione.

2.1.2 Il Security Information and Event Management System

Come nota si segnala che la fase centrale, della figura 2.1, di archiviazione e aggregazione tradizionalmente avviene nel cosidetto **SIEM Security Information and Event Management**

2.2 CERT

I **CERT** sono organizzazioni, gestite e finanziate generalmente da Università o Enti Governativi, incaricate di raccogliere e gestire le segnalazioni d'incidenti informatici e potenziali **vulnerabilità** nei software che provengono dalla comunità degli utenti. I CERT si pongono come un punto di riferimento per gli utenti di riferimento per gli utenti della rete, in grado di aiutarli a risolvere qualunque problema legato alla sicurezza informatica. Di norma un CERT è composto da persone specializzate in diversi ambiti, per esempio amministratore di rete, amministratori di sistema ed esperti in sicurezza informatica. I compiti fondamentali di un CERT consistono nel rispondere alle segnalazioni degli utenti vittime d'incidenti informatici e nell'analizzare i sistemi hardware e software per individuare eventuali vulnerabilità. Ciò che ha contributo ad accrescere le funzioni dei CERT, le cui competenze sono già suddivise in vari settori:

- **Assistenza tecnica**: da parte di un CERT può avvenire in due modi: da un lato come assistenza diretta, attuando piani immediati d'incidenti response in caso di segnalazione da parte di uno o più utenti. Dall'altro lato la massiccia diffusione d'informazioni contenenti, le contromisure adeguate per i tipi più comuni d'incidenti, allo scopo di far acquisire agli utenti la consapevolezza del problema della sicurezza e stimolarli ad auto-proteggersi.

- **Ricerca e sviluppo**: consiste in un monitoraggio costante dei sintomi informatici, dei programmi applicativi e della rete, allo scopo di analizzare il loro stato di sicurezza e il loro livello di sensibilità a potenziali attacchi. Sulla base delle informazioni ottenute il CERT attua piani di realizzazione e implementazione di tecnologie utili a correggere le vulnerabilità, a resistere agli attacchi e a prevenire minacce future.

- **Formazione**:molti CERT organizzano dei corsi di formazione destinati ad amministratori di rete e di sistema personale tecnico in generale, allo scopo d'istruire nella creazione e gestione di un proprio team.

- **Informazione**: le attività di assistenza consentono loro di raccogliere informazioni sugli incidenti cui rispondono, per esempio quale vulnerabilità è stata sfruttata, quale tipo di attacco è stato portato a termine, quali danni ha provocato nel sistema e in che modo si è riusciti a risolvere il problema.

2.2.1 I vantaggi dei CERT (INDECISO SU QUESTA PARTE)

Più in particolare questo tipo di entità permette:

- un **coordinamento centralizzato** delle problematiche di sicurezza IT all'interno di un'organizzazione, agendo da Point of Contact.
- La capacità di fornire a tali problematiche, qualora si trasformassero in incidenti, una **risposta centralizzata e spcializzata**;
- le **conoscenze** per gestire gli aspetti legali legati alla raccolta e conservazione della digital evidence [1], anche in caso di procedimenti legali.
- il **monitoraggio continuo** degli sviluppi nel settore della sicurezza informatica.
- lo **stimolo continuo e la costruzione di awaraness** [2]

Nel caso in cui poi ruolo si estenda oltre i confini che la definizione presuppone, si arriva alla disponibilità in locale della necessaria esperienza per supportare e assistere gli utenti nelle procedure di recovery dagli incidenti.

2.2.2 Il ruolo chiave di un CERT

Nella figura 2.2 si può notare il ruolo chiave di un CERT.
Come si evince dalle tipologie di attività definite accanto all'asse verticale, è un ruolo

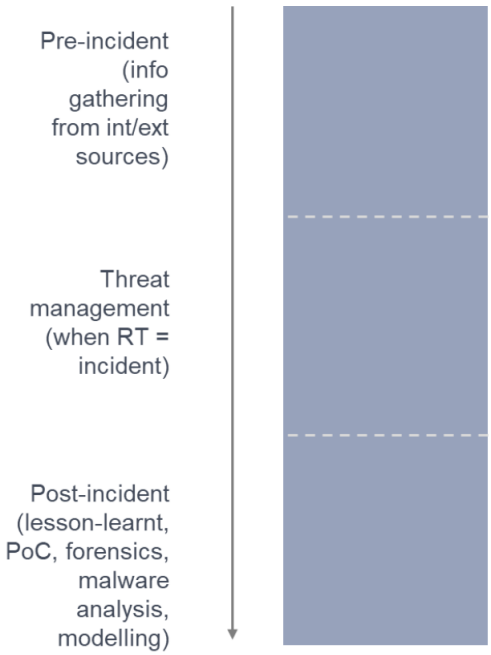

Figura 2.2

maggiormente rivolto alla alla creazione e implementazione di "readiness" rispetto alla gestione degli incidenti, durante tutto il ciclo di vita degli stessi.
Quindi in sintesi si parte dallo studio e dall'arricchimento di conoscenza preliminare

[1] aggiungere nota
[2] spiegare cos'è

riguardo alle fenomenologie in in campo, sia rispetto all'analisi tecnologica delle singole tipologie di minacce, sia per quanto riguarda l'analisi e la modellazione dei fenomeni più generali e delle motivazioni, mediante fonti esterne e collaborazioni con enti analoghi, fino ad arrivare alla alla vera core competence: la capacità di dare supporto specialistico nel corso di un incidente.
E da un CERT ci si può attendere **un supporto a 360°: non solo tecnico, ma anche comunicativo**.

2.2.3 Il valore aggiunto del CERT

Il valore aggiunto del CERT è la possibilità, in seguito ad un "incidente tipo", di studiarlo, modellarlo e renderne disponibili internamente e/o esternamente le caratteristiche distintive ed identificative. Ciò, se formalizzato in modalità condivisibili e standardizzate, costituisce un utilissimo riferimento in futuro , in ottica di una più efficace reazione al medesimo evento.
Il tutto scarica a terra il massimo del potenziale valore nel momento in cui il threat management viene efficacemente attutato in real-time, ossia quando, grazie alle informazioni pregresse e alla capacità disponibili nella struttura, il CERT può efficacemente supportare le realtà che vi si affidano nella gestione degli incidenti legati alla sicurezza informatica.

2.3 I punti di contatto tra il SOC e il CERT

Quanto puntualizzato sinora rispetto ai ruoli prinicipali delle due entità SOC e CERT è finalizzato a mettere in luce un evidente punto di contatto: entrambe le realtà vengono coinvolte in quella che è la fase più critica del presidio della sicurezza informatica in ambito aziendale (ma non solo): **la gestione dell'incidente**.
La figura 2.3 è ottenuta incrociando i diagrammi relativi alle principali attività di SOC e CERT e si vede bene come la gestione dell'incidente rappresenti una fase comune.

Qui, la conoscenza pregressa che arriva dal CERT e la padronanza tecnica (contestualizzata alla realtà operativa) che caratterizza il SOC possono realmente fare la differenza, se opportunamente combinate. Come si evince dalla figura 2.3, in questa fase operano assieme professionalità differenti provenienti delle due, e l'evento può essere trattato molto più efficacemente in quanto si uniscono le competenze di:

- persone che hanno esatta percezione dello stato dei sistemi, in tempo reale;
- persone che sanno interpretare con chiarezza il significato dei segnali, in prospettiva più ampia, e condividerne il senso e le implicazioni;

In particolare, primario elemento di valore che emerge da una gestione congiunta è che in questo modo la remediation sarà "actionable", in quanto legata tecnicamente ai sistemi su cui si è rilevata la problematica, ma sarà allo stesso tempo di portata generale, in quanto derivata da una conoscenza condivisa a livello di settore. Si esce pertanto dalla logica della pura risoluzione dell'emergenza, affrontando invece le problematiche

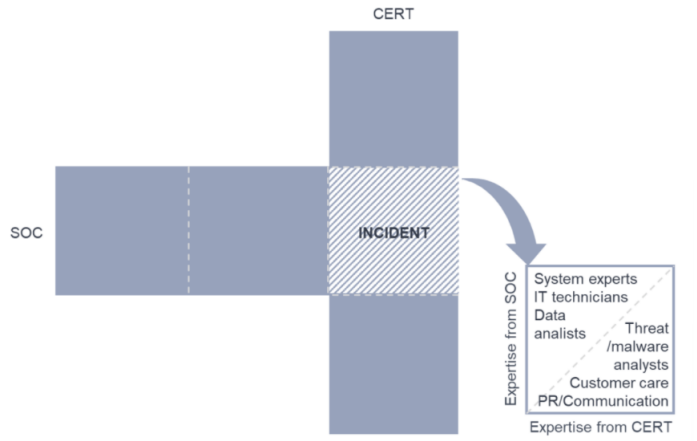

Figura 2.3

in modo strutturato.
Riassumendo, la collaborazione di SOC e CERT (come strutture formalizzate, interne o esterne a una realtà aziendale, o anche semplicemente come ambiti di competenza) se correttamente realizzata a livello tecnico/organizzato permette di ipotizzare il beneficio potenziale di una gestione degli eventi/incidenti di sicurezza informatica che:

- permette l'adozione di misure concrete e immediate applicabili, in quanto elaborate per essere attuate sui medesimi sistemi gestiti dalla componente SOC;
- pervenga a soluzioni che risolvano il problema alla radice, o che quantomeno siano quanto di meglio si possa fare con le conoscenze del momento per adottare una soluzione definitiva, in quanto dalla conoscenza generalista detenuta dalla componente CERT.

Capitolo 3

Caso d'uso

Elenco delle figure

Elenco delle tabelle

Bibliografia

[1] A. Einstein, "Zur Elektrodynamik bewegter Körper. (German) [On the electrodynamics of moving bodies]," *Annalen der Physik*, vol. 322, no. 10, pp. 891–921, 1905.

[2] M. Goossens, F. Mittelbach, and A. Samarin, *The LaTeX Companion*. Reading, Massachusetts: Addison-Wesley, 1993.

[3] D. Knuth, "Knuth: Computers and typesetting."