Sicurezza

Il bisogno di cybersecurity

In questo capitolo vengono spiegati il significato del termine cybersecurity e i motivi per la crescente domanda di professionisti della cybersecurity. Vengono inoltre spiegati cosa sono identità e dati online, dove si trovano e perché interessano ai criminali informatici.

In questo capitolo vengono inoltre trattati i dati aziendali e i motivi per cui devono essere protetti. Vengono descritti gli autori di attacchi informatici e cosa vogliono. I professionisti della cybersecurity devono avere le stesse competenze degli autori di attacchi informatici, ma devono rispettare le leggi locali, nazionali e internazionali. I professionisti della cybersecurity devono anche utilizzare le loro capacità in modo etico.

In questo capitolo sono inclusi anche contenuti che spiegano brevemente la guerra informatica e i motivi per cui nazioni e governi necessitano di professionisti della cybersecurity per aiutare a proteggere cittadini e infrastrutture.

Cos'è la cybersecurity?

La rete di informazioni in formato elettronico connessa è diventata parte integrante della nostra vita quotidiana. Tutti i tipi di aziende, mediche, finanziarie e istituti scolastici usano tale rete per lavorare efficacemente. Utilizzano la rete per acquisire, elaborare, archiviare e condividere grandi quantità di informazioni digitali. Dato che viene raccolta e condivisa una quantità sempre crescente di informazioni, la protezione di tali informazioni sta diventando sempre più essenziale per la sicurezza nazionale e la stabilità economica.

La cybersecurity rappresenta l’impegno costante per proteggere i sistemi interconnessi e tutti i dati associati ai sistemi da utilizzi non autorizzati e danni. A livello personale, è necessario salvaguardare identità, dati e dispositivi di elaborazione. A livello aziendale, è responsabilità di tutti proteggere la reputazione, i dati e i clienti dell’azienda. A livello statale, sono in gioco la sicurezza nazionale, la protezione e il benessere dei cittadini.

La tua identità online e offline

Data la crescente quantità di tempo passato online, la tua identità, sia online sia offline può influenzare la tua vita. La tua identità offline rappresenta la persona con cui amici e parenti interagiscono quotidianamente a casa, a scuola, sul lavoro. Loro conoscono i tuoi dati personali quali nome, età e indirizzo. La tua identità online rappresenta chi sei nel cyberspazio. La tua identità online è come ti presenti agli altri online. Tale identità online deve rivelare una quantità limitata di dati riguardo a te.

Devi porre la massima attenzione scegliendo un nome utente o un alias per l’identità online. Il nome utente non deve includere alcuna informazione personale. Deve essere un nome appropriato e rispettoso. Tale nome utente non deve indurre gli estranei a pensare che tu possa essere un facile bersaglio per i crimini informatici o le attenzioni indesiderate.

I tuoi dati

Qualsiasi informazione su di te può essere considerata dato personale. I dati personali possono identificarti in modo univoco come individuo. Tali dati includono foto e messaggi scambiati online con la tua famiglia e con gli amici. Altre informazioni quali nome, numero di previdenza sociale, data e luogo di nascita o nome da ragazza della madre sono noti a te e sono usati per identificarti.

Anche informazioni quali i dati medici, finanziari, lavorativi e i titoli di studio possono essere usati per identificarti online.

Cartelle mediche

Ogni volta che ti rechi nell'ambulatorio del medico, ulteriori informazioni vengono aggiunte alla tua cartella medica elettronica (EHR, electronic health records). Le prescrizioni del tuo medico sono inserite in tale cartella medica. La cartella include salute fisica, mentale e altri dati personali che possono non essere prettamente medici. Ad esempio, se da bambino hai ricevuto consulenze in occasione di grandi cambiamenti familiari, questo dato sarà inserito nella tua cartella medica. Oltre alla cronologia medica e ai dati personali, la cartella può contenere anche informazioni sulla tua famiglia.

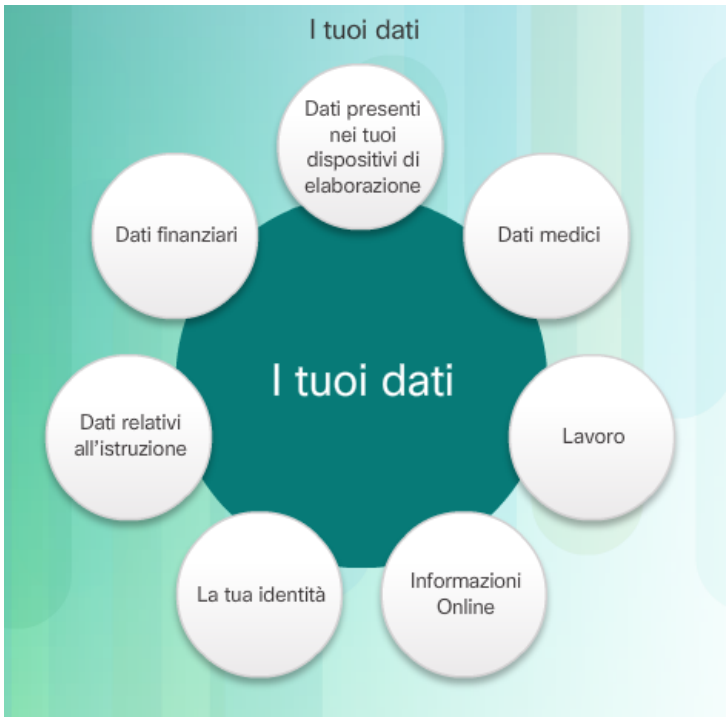
I dispositivi medici come le fitness band usano la piattaforma cloud per consentire i trasferimenti, l'archiviazione e la visualizzazione wireless di dati clinici come la frequenza cardiaca, la pressione del sangue e la glicemia. Tali dispositivi possono generare enormi quantità di dati clinici che possono essere aggiunti alla tua cartella medica.

Curriculum scolastico

Progredendo nella formazione, le informazioni sui risultati e i voti, le presenze, i corsi frequentati, i titoli e i riconoscimenti ottenuti ed eventuali note disciplinari saranno registrati nel curriculum scolastico. Tale curriculum può contenere anche le informazioni sui contatti, lo stato di salute e le vaccinazioni e informazioni sui corsi di formazione speciali inclusi i programmi educativi personalizzati (IEP, individualized education programs).

Dati lavorativi e finanziari

I tuoi dati finanziari possono includere informazioni sulle entrate e le spese. I dati fiscali possono includere buste paga, estratti conto delle carte di credito, il rating del credito e altre informazioni bancarie. Le informazioni lavorative possono includere gli incarichi precedenti e le relative prestazioni.



Dove sono i tuoi dati?

Tutte queste informazioni ti riguardano. Esistono varie leggi che proteggono la privacy e i tuoi dati nel tuo paese. Ma sai dove si trovano i tuoi dati?

Quando sei nell'ambulatorio del medico, la conversazione con il tuo medico viene registrata nella cartella medica. A fini di fatturazione, tali informazioni possono essere condivise con la compagnia di assicurazioni per garantire una corretta fatturazione e la qualità del lavoro. Nella cartella medica, insieme ai dati della visita è indicata anche la compagnia di assicurazioni.

Le carte fedeltà dei negozi possono essere un modo conveniente per risparmiare denaro sugli acquisti. Tuttavia, il negozio compila un profilo degli acquisti e utilizza tali informazioni per scopi interni. Il profilo mostra che un acquirente compra regolarmente prodotti di una determinata marca e un certo gusto di dentifricio. Il negozio usa tali informazioni per inviare all’acquirente determinate offerte speciali dei partner commerciali. Utilizzando la carta fedeltà, il negozio e i partner commerciali hanno un profilo indicante il comportamento relativo agli acquisti di un cliente.

Quando condividi le foto online con gli amici, sai chi può averne una copia? Le copie delle foto sono sui tuoi dispositivi. I tuoi amici possono avere copie di tali foto scaricate nei loro dispositivi. Se le foto sono condivise pubblicamente, anche degli estranei possono averne copie. Possono scaricarle o acquisirne schermate. Poiché le foto erano pubblicate online, sono inoltre salvate su server ubicati in varie parti del mondo. A questo punto le foto non si trovano più solo sui tuoi dispositivi di elaborazione.

I tuoi dispositivi di elaborazione

I tuoi dispositivi di elaborazione non si limitano a memorizzare i tuoi dati. Ora questi dispositivi sono diventati il portale per i tuoi dati e generano informazioni da essi.

Se non hai scelto di ricevere estratti conto cartacei di tutti i tuoi conti, utilizzi i dispositivi di elaborazione per accedere a tali dati. Se desideri una copia digitale dell’estratto conto più recente della carta di credito, utilizzi i dispositivi di elaborazione per accedere al sito Web dell’emittente della carta. Se desideri saldare gli addebiti della carta di credito online, accedi al sito Web della banca per trasferire fondi con i dispositivi di elaborazione. Oltre a consentirti l’accesso alle informazioni, i dispositivi di elaborazione possono anche generare informazioni su di te.

Con tali informazioni disponibili online, i tuoi dati personali diventano sfruttabili dagli hacker.

Vogliono il tuo denaro

Se possiedi qualcosa di valore, i criminali lo vogliono.

Le tue credenziali online hanno molto valore. Tali credenziali offrono ai ladri l’accesso ai tuoi account. Potresti pensare che le miglia guadagnate con i voli frequenti non siano importanti per i criminali informatici. Non più. Dopo aver violato circa 10.000 account American Airlines e United, i criminali informatici hanno prenotato e modificato gratuitamente voli utilizzando le credenziali rubate. Anche se le miglia guadagnate con i voli frequenti sono state restituite ai clienti dalle compagnie aeree, ciò dimostra il valore delle credenziali di accesso. Un criminale potrebbe sfruttare anche le tue relazioni. Potrebbe accedere ai tuoi account online e alla tua reputazione per raggirarti spingendoti a inviare denaro a parenti e amici. Il criminale può inviare messaggi affermando che parenti o amici hanno bisogno di un tuo bonifico per tornare a casa dopo aver perso il portafoglio.

I criminali usano molta immaginazione nel cercare di raggirarti per farsi consegnare il tuo denaro. Non solo rubano il tuo denaro, possono anche rubare la tua identità e rovinarti la vita.

Vogliono la tua identità

Oltre a rubare denaro per un guadagno monetario a breve termine, i criminali desiderano profitti a lungo termine rubandoti l'identità.

Dato che i costi medici aumentano, anche i ladri di identità in questo settore sono in aumento. I ladri di identità possono rubare l'assicurazione sanitaria e usare i tuoi vantaggi per loro stessi; tali procedure mediche adesso sono registrate nella tua cartella.

Le procedure fiscali annuali possono variare da paese a paese, tuttavia i criminali informatici vedono questo periodo come un'opportunità. Ad esempio, negli Stati Uniti i contribuenti devono inviare le dichiarazioni entro il 15 aprile di ogni anno. L'Internal Revenue Service (IRS) non controlla la dichiarazione rispetto alle informazioni del datore di lavoro fino a luglio. Un ladro di identità può inviare una dichiarazione falsa e ottenere il rimborso. I mittenti legittimi se ne accorgeranno quando i loro rimborsi saranno rifiutati dall'IRS. Con l'identità rubata possono inoltre aprire conti con carta di credito e addebitare spese a tuo nome. Ciò causerà danni al tuo rating del credito rendendoti più difficile l'accesso ai prestiti.

Le credenziali personali possono inoltre fornire l'accesso ai dati aziendali e governativi.

Tipi di dati aziendali

Dati tradizionali

I dati aziendali comprendono informazioni personali, proprietà intellettuali e dati finanziari. Le informazioni personali includono candidature, buste paga, lettere di offerta, contratti con il datore di lavoro e qualsiasi informazione utilizzata per le decisioni sulle assunzioni. La proprietà intellettuale, come brevetti, marchi registrati e piani per nuovi prodotti, consente all'azienda di ottenere un vantaggio economico sulla concorrenza. Tale proprietà intellettuale può essere considerata un segreto commerciale; la perdita di tali informazioni può essere disastrosa per il futuro dell'azienda. I dati finanziari, quali dichiarazione dei redditi, bilancio e rendiconto del flusso di cassa di un'azienda offrono una panoramica sullo stato di salute dell'azienda stessa.

Internet of Things e Big Data

Con la comparsa di Internet of Things (IoT), la quantità di dati da gestire e proteggere è molto aumentata. IoT è un'ampia rete di oggetti fisici, quali sensori e apparecchiature che si estende oltre la tradizionale rete di computer. Tutte queste connessioni, oltre al fatto che abbiamo espanso la capacità di archiviazione e i servizi di archiviazione tramite il Cloud e la virtualizzazione, portano a una crescita esponenziale dei dati. Questi dati hanno creato una nuova area di interesse nella tecnologia e nelle aziende denominata "Big Data". Con la velocità, il volume e la varietà di dati generati da IoT e dalle attività aziendali quotidiane, la riservatezza, l'integrità e la disponibilità di tali dati è vitale per la sopravvivenza dell'azienda.

Riservatezza, integrità e disponibilità

Riservatezza, integrità e disponibilità note come la triade CIA (Figura 1) sono una linea guida per la sicurezza informatica di un'azienda. La riservatezza garantisce la privacy dei dati restringendo l'accesso tramite la crittografia di autenticazione. L'integrità garantisce l'accuratezza e l'affidabilità

delle informazioni. La disponibilità garantisce che solo gli utenti autorizzati possano accedere alle informazioni.

Riservatezza

Un sinonimo di riservatezza può essere privacy. Le policy aziendali devono limitare l'accesso alle informazioni al personale autorizzato e garantire che solo le persone autorizzate possano visualizzare tali dati. I dati possono essere suddivisi in scomparti in base alla sicurezza o ai livelli di sensibilità delle informazioni. Ad esempio, uno sviluppatore di programmi Java non deve avere accesso ai dati personali di tutti i dipendenti. Inoltre, i dipendenti devono partecipare a corsi di formazione per comprendere le best-practice nel salvaguardare le informazioni sensibili per proteggere loro stessi e l'azienda dagli attacchi. I metodi per garantire la riservatezza comprendono: crittografia dei dati, ID nome utente e password, autenticazione a due fattori e minima esposizione delle informazioni sensibili.

Integrità

L'integrità è accuratezza, coerenza e affidabilità dei dati nell'intero ciclo di vita. I dati devono rimanere inalterati durante la loro trasmissione e preservati da entità non autorizzate. Le autorizzazioni per i file e il controllo degli accessi degli utenti possono prevenire accessi non autorizzati. Il controllo delle versioni può essere usato per prevenire modifiche accidentali da parte di utenti autorizzati. I backup devono essere disponibili per il ripristino dei dati corrotti e l'hashing delle checksum può essere usato per verificare l'integrità dei dati durante il trasferimento.

La checksum viene usata per verificare l'integrità dei file o delle stringhe di caratteri dopo il trasferimento da un dispositivo a un altro sulla rete locale o via Internet. Le checksum sono calcolate con le funzioni hash. Alcune della checksum comuni sono MD5, SHA-1, SHA-256 e SHA-512. Una funzione hash utilizza un algoritmo matematico per trasformare i dati in un valore a lunghezza fissa che rappresenta i dati, come mostrato in figura 2. Il valore di hashing serve esclusivamente per un confronto. Dal valore di hashing, non è possibile recuperare direttamente i dati. Ad esempio, se si dimentica la password, non è possibile recuperarla dal valore di hashing. È necessario reimpostare la password.

Quando un file viene scaricato, è possibile verificarne l'integrità controllando il valore di hashing della sorgente con quello generato dal calcolatore di hashing. Confrontando i valori di hashing, è possibile garantire che il file non sia stato manomesso o corrotto durante il trasferimento.

Disponibilità

La manutenzione delle apparecchiature, le riparazioni hardware, l'aggiornamento di sistemi operativi e software e la creazione di backup garantisce la disponibilità di rete e dati agli utenti autorizzati. È necessario avere in atto dei piani per il rapido ripristino da disastri naturali o provocati dall'uomo. I dispositivi o il software di sicurezza come i firewall proteggono contro le interruzioni dell'operatività dovute agli attacchi come il Denial-of-Service. Quest'ultimo si verifica quando un attacco cerca di sovraccaricare le risorse per rendere i servizi non disponibili per gli utenti.

Le conseguenze di una violazione della sicurezza

Proteggere l’azienda da tutti i possibili attacchi informatici non è fattibile per alcuni motivi. Le competenze necessarie per configurare e mantenere una rete sicura possono essere costose. Gli autori degli attacchi continueranno sempre a trovare nuovi modi per violare le reti. Alla fine, un attacco informatico avanzato e mirato avrà successo. In tal caso la priorità sarà la velocità di risposta all’attacco da parte del team addetto alla sicurezza per minimizzare la perdita di dati, l’interruzione dell'operatività e i redditi.

Adesso sai che qualsiasi informazione pubblicata online può rimanere online per sempre, anche se tu fossi in grado di cancellare tutte le copie in tuo possesso. Se i server hanno subito un attacco, le informazioni personali riservate possono essere rese pubbliche. Un hacker (o un gruppo di hacker) può danneggiare il sito web dell’azienda pubblicando informazioni non vere e rovinando la reputazione dell’azienda ottenuta in anni di lavoro. Inoltre, gli hacker possono oscurare il sito web dell’azienda causando una perdita di reddito. Se il sito Web rimane inaccessibile per lunghi periodi, l’azienda può apparire inaffidabile e perdere credibilità. Se il sito Web o la rete dell’azienda ha subito una violazione, ciò può causare la perdita di documenti riservati, la diffusione di segreti commerciali e il furto di proprietà intellettuale. La perdita di tutte queste informazioni può impedire la crescita e l’espansione dell’azienda.

Il costo monetario di una violazione è molto superiore alla semplice spesa per la sostituzione di dispositivi smarriti o rubati, all’investimento per la sicurezza esistente e per il rafforzamento della sicurezza fisica degli edifici. L’azienda può avere la responsabilità di contattare tutti i clienti interessati dalla violazione e dover affrontare azioni legali. Con tutto questo scompiglio, i dipendenti possono decidere di lasciare l'azienda. L’azienda può doversi concentrare meno sulla crescita e più sul recupero della reputazione.

Violazione della sicurezza: Esempio 1

Il gestore di password online, LastPass, ha rilevato un'attività insolita sulla rete a luglio 2015. È stato scoperto che alcuni hacker avevano rubato indirizzi e-mail, promemoria di password e hash di autenticazione degli utenti. Fortunatamente per gli utenti, gli hacker non sono stati in grado di ottenere gli archivi crittografati di password.

Nonostante la violazione della sicurezza, LastPass è riuscita a proteggere le informazioni degli account degli utenti. LastPass richiede una verifica delle e-mail o un'autenticazione a più fattori ogni volta che viene eseguito un nuovo accesso da un dispositivo o indirizzo IP sconosciuto. Gli hacker avranno inoltre bisogno della password principale per accedere all'account.

Gli utenti di LastPass sono responsabili di proteggere i propri account. Gli utenti dovranno sempre usare password principali complesse e cambiarle periodicamente. Gli utenti dovranno sempre porre la massima attenzione agli attacchi di phishing. Un esempio di un attacco phishing è l'invio di e-mail fasulle da parte di un autore degli attacchi dichiarando di essere LastPass. Le e-mail chiedono agli utenti di fare clic su un collegamento integrato e modificare la password. Il collegamento della e-mail punta ad una versione fraudolenta del sito Web per rubare la password principale. Gli utenti non dovranno mai fare clic su collegamenti integrati nelle e-mail. Inoltre, gli utenti dovranno sempre porre la massima attenzione ai promemoria delle password. Il promemoria della password non deve rivelare le password. Ancora più importante, gli utenti devono attivare l'autenticazione a più fattori, laddove disponibile, per qualsiasi sito Web che la offre.

Se gli utenti e i provider di servizi utilizzano entrambi gli strumenti e le procedure corretti per salvaguardare le informazioni degli utenti, i dati degli utenti possono essere protetti anche in caso di violazione della sicurezza.

Violazione della sicurezza: Esempio 2

Il produttore di giocattoli high tech per bambini, Vtech ha subito una violazione della sicurezza nel suo database a novembre 2015. Tale violazione potrebbe riguardare milioni di clienti in tutto il mondo inclusi i bambini. La violazione dei dati ha esposto informazioni sensibili fra cui i nomi, gli indirizzi e-mail, le password, le foto e i registri delle chat dei clienti.

Un tablet giocattolo è diventato un nuovo bersaglio per gli hacker. I clienti avevano condiviso foto e usato le funzioni di chat tramite i tablet giocattolo. Le informazioni non erano correttamente protette e il sito Web dell'azienda non supportava le comunicazioni protette su protocollo SSL. Sebbene la violazione non abbia esposto le informazioni sulle carte di credito e i dati di identificazione personali, l'azienda è stata sospesa nelle contrattazioni in borsa a causa delle elevate preoccupazioni per l'attacco degli hacker.

Vtech non ha protetto correttamente le informazioni dei propri clienti che sono state esposte durante la violazione. Nonostante l'azienda abbia informato i clienti che le password erano state sottoposte a hashing, gli hacker avevano comunque la possibilità di decifrarle. Le password del database erano state crittografate usando una funzione hash MD5 ma le domande di sicurezza e le risposte erano memorizzate come testo in chiaro. Sfortunatamente, la funzione hash MD5 ha delle vulnerabilità note. Gli hacker possono determinare le password originali confrontando milioni di valori di hashing precalcolati.

Con le informazioni esposte da questa violazione dei dati, i criminali informatici possono usarle per creare account e-mail, richiedere crediti e commettere crimini prima che i bambini raggiungano l'età scolare. Per i genitori di questi bambini, i criminali informatici possono impadronirsi degli account online perché molte persone riutilizzano le password su vari siti Web e account.

La violazione della sicurezza non solo ha avuto un impatto sulla privacy dei clienti, ma ha rovinato la reputazione dell'azienda, come indicato dall'azienda quando è stata sospesa dalle trattative in borsa.

Per i genitori, si tratta di una richiamo a porre maggiore attenzione alla privacy online dei loro figli e a richiedere maggiore protezione per i prodotti destinati ai bambini. I fabbricanti di prodotti connessi in rete devono essere più aggressivi nella protezione dei dati sui clienti e della privacy, ora e in futuro, poiché il panorama degli attacchi informatici è in costante evoluzione.

Tipi di autori degli attacchi

Gli autori degli attacchi sono individui o gruppi che tentano di sfruttare le vulnerabilità a scopo di guadagno personale o finanziario. Gli autori degli attacchi sono interessati a tutto, dalle carte di credito al design dei prodotti, a qualsiasi cosa di valore.

Dilettanti: queste persone sono talvolta definite Script Kiddies. Sono generalmente hacker con competenze scarse o nulle che spesso usano strumenti esistenti o istruzioni trovate su Internet per lanciare attacchi. Alcuni di loro sono solo curiosi, mentre altri cercano di dimostrare le loro competenze e causare problemi. Possono usare strumenti di base ma il risultato può essere ugualmente devastante.

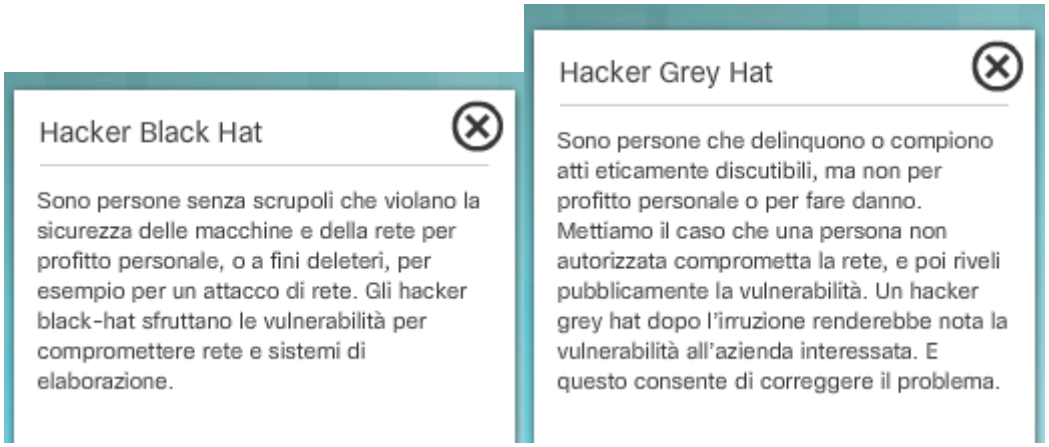
Hacker: questo gruppo di autori degli attacchi viola computer e reti per ottenere l'accesso. A seconda delle intenzioni della violazione, questi autori degli attacchi sono classificati come white, gray o black hat. Gli hacker white hat violano reti o sistemi informatici per scoprirne le debolezze e poter migliorare la sicurezza di tali sistemi. Queste violazioni sono effettuate con autorizzazione e

tutti i risultati sono consegnati al proprietario. D'altro canto gli autori degli attacchi black hat sfruttano qualsiasi vulnerabilità per ottenere un guadagno personale, finanziario o politico illegale. Gli autori degli attacchi gray hat si posizionano a metà fra i white hat e i black hat. I gray hat possono identificare una vulnerabilità in un sistema. Possono segnalare la vulnerabilità ai proprietari del sistema se tale azione coincide con i loro programmi. Alcuni hacker gray hat pubblicano le informazioni sulla vulnerabilità in Internet in modo che altri autori degli attacchi possano sfruttarle.

Nella figura sono riportati dettagli sulle espressioni hacker white hat, hacker black hat, e hacker gray hat.

Hacker organizzati: questi hacker includono organizzazioni di criminali informatici, hacktivist, terroristi e hacker sponsorizzati dagli stati. I criminali informatici sono generalmente gruppi di criminali professionisti focalizzati su controllo, potenza e ricchezza. I criminali sono altamente focalizzati e organizzati e possono persino fornire il crimine informatico come servizio ad altri criminali. Gli hacktivist effettuano dichiarazioni politiche per creare consapevolezza su problemi importanti per loro. Gli autori degli attacchi sponsorizzati dallo stato acquisiscono intelligence o commettono sabotaggi per conto del proprio governo. Sono in genere altamente specializzati e ben finanziati e i loro attacchi sono mirati a obiettivi specifici a vantaggio dei loro governi.

Fare clic qui per visualizzare una rappresentazione grafica dei profili degli hacker.



Minacce interne ed esterne

Minacce alla sicurezza interna

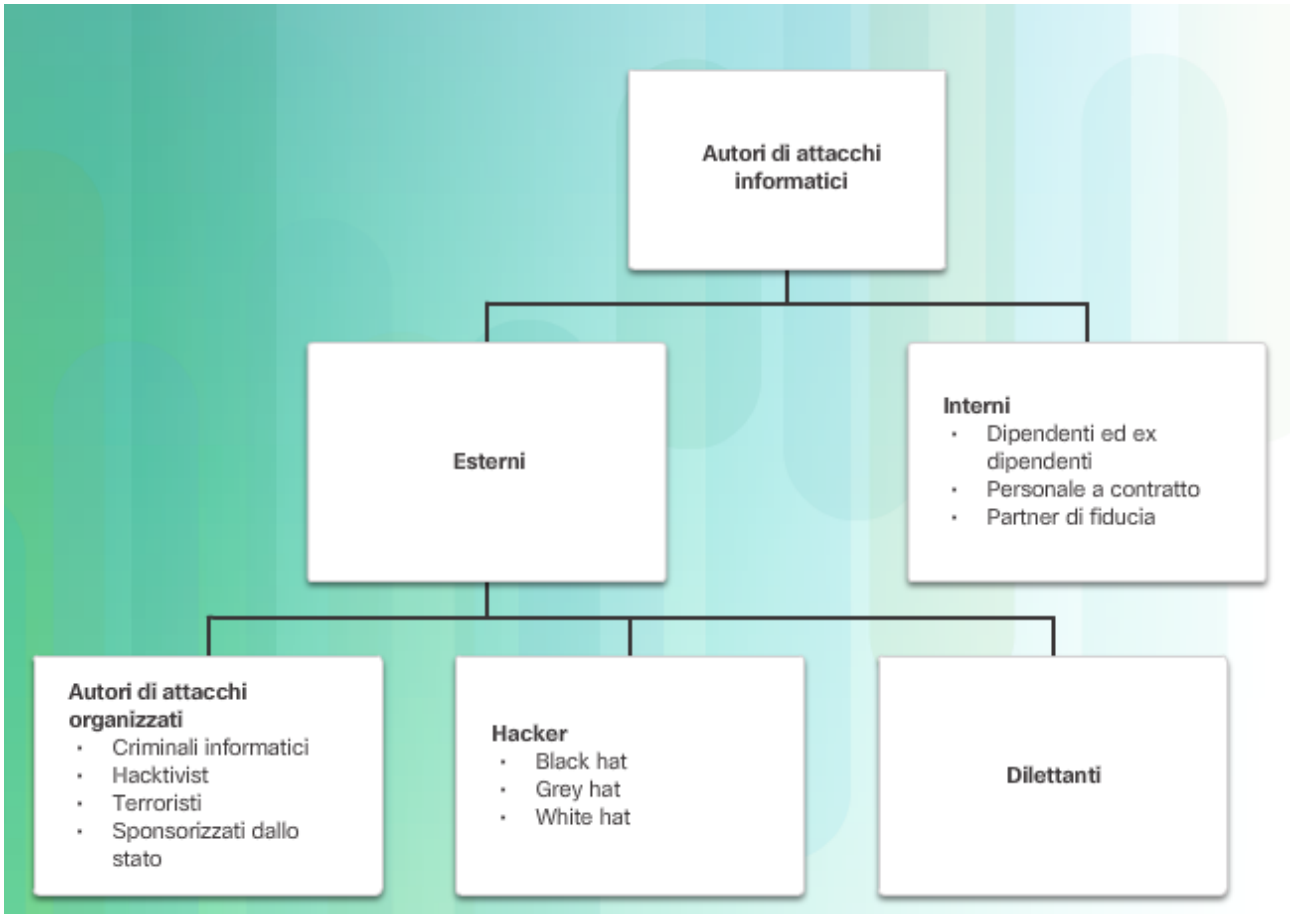
Gli attacchi possono essere originati dall'interno dell'azienda o dall'esterno come mostrato in figura. Un utente interno come un dipendente o un partner a contratto, può accidentalmente o intenzionalmente:

- Gestire male i dati riservati
- Minacciare l'attività dei server interni o dei dispositivi dell'infrastruttura di rete
- Facilitare gli attacchi esterni collegando supporti USB infetti al sistema informatico aziendale
- Inserire accidentalmente il malware nella rete tramite e-mail o siti web dannosi

Le minacce interne hanno inoltre il potenziale di causare maggiori danni rispetto alle minacce esterne, poiché gli utenti interni hanno accesso diretto agli edifici e ai relativi dispositivi delle infrastrutture. Inoltre i dipendenti conoscono la rete aziendale, le sue risorse e i dati riservati oltre ai vari livelli di utenti o privilegi amministrativi.

Minacce alla sicurezza esterne

Le minacce esterne da parte di dilettanti o autori di attacchi esperti possono sfruttare le vulnerabilità della rete o dei dispositivi di elaborazione, oppure usare il social engineering per ottenere l'accesso.



Problemi legali nella cybersecurity

I professionisti della cybersecurity devono avere le stesse competenze degli hacker, in particolare dei black hat per proteggere dagli attacchi. Una differenza fra un hacker e un professionista della cybersecurity sta nel fatto che il professionista della cybersecurity deve lavorare entro i limiti della legalità.

Problemi legali personali

Non è necessario essere un dipendente per essere soggetto alle leggi sulla cybersecurity. Nella vita privata potresti avere le opportunità e le competenze per violare il computer o la rete di un'altra persona. Un vecchio detto recita: "Solo perché puoi non è detto che devi". Ricordalo. La maggior parte degli hacker lascia una traccia, consapevolmente o meno, e tramite queste tracce è possibile risalire all'hacker.

I professionisti della cybersecurity acquisiscono molte competenze che possono essere usate per scopi positivi o negativi. Coloro che utilizzano le proprie competenze nell'ambito del sistema legale per proteggere l'infrastruttura, le reti e la privacy sono sempre molto richiesti.

Problemi legali aziendali

In molti Paesi sono in vigore leggi sulla cybersecurity. Possono riguardare l'infrastruttura critica, le reti e la privacy sia personale sia aziendale. Le aziende sono tenute a rispettare tali leggi.

In alcuni casi, se violi le leggi sulla cybersecurity nell'ambito lavorativo, l'azienda ne subirà le conseguenze legali e tu potresti perdere il lavoro. In altri casi, potresti essere perseguito, multato e condannato.

In generale, se hai dubbi sulla legalità di un'azione o di un comportamento, presupponi che sia illegale non procedere. L'azienda può avere un ufficio legale o una persona nel reparto risorse umane in grado di rispondere alle tue domande prima di commettere qualcosa di illegale.

Legge internazionale e cybersecurity

L'ambito della legge sulla cybersecurity è molto più recente della cybersecurity stessa. Come citato in precedenza, in molti Paesi sono in vigore delle leggi in merito e ne saranno approvate altre.

La legge internazionale sulla cybersecurity è ancora relativamente nuova. L'International Multilateral Partnership Against Cyber Threats (IMPACT) è la prima partnership pubblica-privata focalizzata sulle minacce informatiche. IMPACT è una partnership globale di governi, industrie e ambienti universitari dedicati a migliorare le funzionalità globali nell'affrontare le minacce informatiche. Nella figura viene mostrato il sito Web di IMPACT.

Problemi etici nella cybersecurity

Oltre a lavorare nell'ambito della legalità, i professionisti della cybersecurity devono dimostrare un comportamento etico.

Problemi etici personali

Una persona può agire in maniera non etica e non essere soggetta a procedimenti penali, multe o reclusione. Ciò perché l'azione potrebbe non essere stata tecnicamente illegale. Ma non significa che il comportamento sia accettabile. Il comportamento etico è abbastanza facile da accertare. È impossibile elencare tutti i vari comportamenti non etici che possono essere tenuti da una persona con competenze di cybersecurity. Ne seguono due. Ci si deve chiedere:

- Vorrei forse scoprire che qualcuno ha violato il mio computer e alterato le immagini nei miei siti dei social network?
- Vorrei forse scoprire che un tecnico informatico di cui mi fidavo per risolvere un problema di rete, ha divulgato dati personali su di me ai colleghi ottenuti lavorando sulla rete?

Se la risposta a una di queste domande è "no", non comportatevi in questo modo con gli altri.

Cos'è la guerra cibernetica (cyberwarfare)?

Il cyberspazio è diventato un’altra importante dimensione della guerra, dove le nazioni possono combattere senza i tradizionali scontri di truppe e macchine. Ciò consente ai Paesi con una presenza militare minima di avere la stessa forza delle altre nazioni nel cyberspazio. La guerra cibernetica è un conflitto basato su Internet che comporta la penetrazione nelle reti e nei sistemi informatici di altri Paesi. Questi autori di attacchi hanno le risorse e le competenze per lanciare massicci attacchi basati su Internet contro altre nazioni per causare danni o interrompere i servizi, ad esempio disattivare la rete elettrica.

Un esempio di un attacco sponsorizzato dallo stato ha coinvolto il malware Stuxnet, progettato per danneggiare l’impianto di arricchimento dell’uranio iraniano. Il malware Stuxnet non ha violato i computer per rubare informazioni. È stato progettato per danneggiare fisicamente le apparecchiature controllate dai computer. Ha utilizzato un codice modulare programmato per eseguire specifiche attività nel malware. Ha utilizzato certificati digitali rubati per far apparire legittimo l’attacco al sistema.

Lo scopo della guerra cibernetica

L'obiettivo principale della guerra cibernetica è acquisire un vantaggio sugli avversari, indipendentemente dal fatto che essi siano nazioni o concorrenti.

Una nazione può costantemente invadere l’infrastruttura di un’altra nazione, rubare segreti della difesa e raccogliere informazioni sulla tecnologia per colmare il divario nel proprio settore industriale e militare. Oltre allo spionaggio industriale e militare la guerra cibernetica può sabotare l’infrastruttura di altre nazioni e costare vite nelle nazioni prese di mira. Ad esempio, un attacco può disattivare la rete elettrica di una grande città. Il traffico andrebbe in tilt. Lo scambio di merci e servizi sarebbe interrotto. In situazioni di emergenza, i pazienti non possono ricevere le cure necessarie. Anche l’accesso a Internet può essere interrotto. Colpendo la rete elettrica, l’attacco può influenzare la vita quotidiana dei cittadini normali.

Inoltre, i dati sensibili che hanno subito violazioni possono consentire agli autori degli attacchi di ricattare i funzionari pubblici. Tali informazioni possono consentire a un autore di attacchi di spacciarsi per un utente autorizzato e accedere alle informazioni o ai dispositivi sensibili.

Se il governo non è in grado di difenderli dagli attacchi informatici, i cittadini possono perdere la fiducia nelle capacità del governo di proteggerli. La guerra cibernetica può destabilizzare una nazione, bloccare il commercio e influenzare la fiducia dei cittadini verso il proprio governo senza nemmeno invadere fisicamente la nazione presa di mira.

Gli attacchi: concetti e tecniche

In questo capitolo vengono spiegate le modalità con cui i professionisti della cybersecurity analizzano gli effetti di un attacco informatico. Illustra le vulnerabilità di protezione di natura hardware e software suddivise per categorie.

Vengono analizzate le varie tipologie di software dannoso (noto come malware) e i sintomi generati dal malware. Vengono trattati i vari metodi utilizzati dagli autori degli attacchi per penetrare in un sistema nonché gli attacchi di tipo denial of service.

Gli attacchi informatici più recenti sono considerati perlopiù attacchi misti. Gli attacchi misti impiegano varie tecniche per penetrare nei sistemi e attaccarli. Quando è impossibile evitare un attacco, è compito dei professionisti della cybersecurity ridurne l'impatto.

Individuazione delle vulnerabilità di protezione

Per vulnerabilità di protezione si intende qualsiasi tipo di difetto software o hardware. Dopo avere individuato una vulnerabilità, gli utenti malintenzionati tentano di sfruttarla. Exploit *è il* termine utilizzato per descrivere un programma scritto allo scopo di sfruttare una vulnerabilità nota. L'atto di utilizzare un exploit contro una vulnerabilità è definito “attacco”. L'obiettivo di un attacco è ottenere l'accesso a un sistema, ai dati al suo interno o a una risorsa specifica.

Vulnerabilità software

Le vulnerabilità software sono solitamente introdotte da errori nel sistema operativo o nel codice delle applicazioni e malgrado tutto l'impegno posto dalle aziende nell'individuazione e nel patching di tali vulnerabilità, spesso ne emergono di nuove. Microsoft, Apple e altri produttori di sistemi operativi rilasciano patch e aggiornamenti quasi ogni giorno. È frequente anche l'utilizzo di aggiornamenti delle applicazioni. Applicazioni quali browser Web, app per dispositivi mobili e server Web vengono spesso aggiornate dalle aziende o dalle organizzazioni che ne sono responsabili.

Nel 2015 una vulnerabilità importante, denominata SYNful Knock, è stata individuata in Cisco IOS. Questa vulnerabilità ha consentito agli autori degli attacchi di ottenere il controllo di router di livello enterprise, quali Cisco 1841, 2811 e 3825. In questo modo gli autori degli attacchi potevano monitorare tutta la comunicazione di rete e infettare altri dispositivi. Questa vulnerabilità è stata introdotta nel sistema a seguito dell'installazione di una versione IOS alterata nei router. Per evitare una simile situazione, è importante verificare sempre l'integrità dell'immagine IOS scaricata e limitare l'accesso fisico all'attrezzatura solo al personale autorizzato.

L'obiettivo degli aggiornamenti software è restare aggiornati ed evitare che le vulnerabilità possano essere sfruttate. Sebbene alcune aziende abbiano team dedicati ai test di penetrazione per la ricerca, l'individuazione e il patching delle vulnerabilità software prima che subiscano attacchi, sono specializzati nell'individuazione delle vulnerabilità nel software anche ricercatori per la sicurezza di terze parti.

Project Zero di Google è un esempio eccellente di tale prassi. Dopo avere individuato numerose vulnerabilità in vari software utilizzati dagli utenti finali, Google ha istituito un team permanente dedicato appunto all'individuazione delle vulnerabilità nel software.

Vulnerabilità hardware

Le vulnerabilità hardware vengono spesso introdotte da difetti di progettazione dell'hardware. La memoria RAM ad esempio, è essenzialmente costituita da condensatori molto vicini fra di loro. È stato scoperto che, a causa della prossimità, cambiamenti costanti applicati a uno di questi condensatori potrebbero influenzare i condensatori adiacenti. Sulla base di questo difetto di progettazione, è stato creato un exploit denominato Rowhammer. Riscrivendo ripetutamente la memoria negli stessi indirizzi, l'exploit Rowhammer consente di recuperare i dati dalle celle di memoria dell'indirizzo attiguo, anche se tali celle sono protette.

Le vulnerabilità hardware sono specifiche dei modelli di dispositivi e generalmente non ne viene eseguito l'exploit tramite tentativi di compromissione casuali. Benché gli exploit hardware siano più

comuni negli attacchi estremamente mirati, la protezione da malware tradizionale e un sistema di sicurezza fisica sono una protezione sufficiente per gli utenti abituali.

Suddivisione in categorie delle vulnerabilità di protezione

La maggior parte delle vulnerabilità di protezione software rientra in una delle seguenti categorie:

Overflow del buffer: questa vulnerabilità è dovuta alla scrittura di dati oltre i limiti del buffer. I buffer sono aree di memoria allocate a un'applicazione. Modificando i dati oltre i limiti di un buffer, l'applicazione accede alla memoria allocata ad altri processi. Questa condizione può portare a un arresto anomalo del sistema, alla compromissione dei dati o all'esecuzione dell'escalation dei privilegi.

Input non validato: i programmi spesso operano con input di dati. Tali dati immessi nel programma possono avere contenuto dannoso, progettato per forzare un comportamento non intenzionale del programma. Si pensi a un programma che riceve un'immagine per l'elaborazione. Un utente malintenzionato può creare un file di immagine con dimensioni dell'immagine non valide. Le dimensioni create per fini dannosi potrebbero forzare il programma ad allocare buffer di dimensioni non corrette e impreviste.

Race condition: questa vulnerabilità si ha quando l'output di un evento dipende da output ordinati o temporizzati. Un condition rate diventa fonte di vulnerabilità quando gli eventi ordinati o temporizzati richiesti non si verificano nell'ordine o nei tempi corretti.

Punti deboli nelle procedure di sicurezza: sistemi e dati sensibili possono essere protetti con tecniche quali autenticazione, autorizzazione e crittografia. Gli sviluppatori non devono tentare di creare i propri algoritmi di protezione, perché potrebbero introdurre vulnerabilità. È di gran lunga preferibile che gli sviluppatori utilizzino librerie di protezione già create, collaudate e verificate.

Problemi di controllo degli accessi: il processo di controllo degli accessi consente di verificare l'autore di un'operazione e spazia dalla gestione dell'accesso fisico alle apparecchiature all'assegnazione delle autorizzazioni e dei diritti di accesso a una risorsa, ad esempio di lettura o modifica del file. Molte vulnerabilità di protezione vengono create dall'utilizzo non corretto del controllo degli accessi.

Quasi tutti i sistemi di controllo degli accessi e le procedure di sicurezza possono essere elusi quando l'autore degli attacchi ha accesso fisico all'apparecchiatura obiettivo. Ad esempio, a prescindere dalle autorizzazioni impostate per un file, il sistema operativo non può impedire a un utente di aggirarlo e leggere i dati direttamente dal disco. Per proteggere il computer e i dati in esso contenuti, occorre limitare l'accesso fisico e utilizzare tecniche di crittografia per proteggere i dati da tentativi di furto o danneggiamento.

Tipologie di malware

Il malware, abbreviazione di software dannoso (Malicious Software), è qualsiasi codice utilizzabile per il furto dei dati, il bypass del controllo degli accessi oppure il danneggiamento o la compromissione di un sistema. Di seguito sono riportate alcune tipologie comuni di malware:

Spyware: questo malware è progettato per tracciare e spiare l'utente. Lo spyware spesso comprende activity tracker, sequenze di tasti e acquisizione di dati. In un tentativo di eludere le misure di sicurezza, lo spyware spesso modifica le impostazioni di protezione. Lo spyware è di frequente associato a software legittimo o Trojan horse.

Adware: l'Advertising supported software è progettato per recapitare automaticamente pubblicità. L'adware è spesso installato con alcune versioni software. Alcuni adware sono progettati per recapitare solo pubblicità ma è frequente che contengano spyware.

Bot: derivante dalla parola robot, un bot è un malware progettato per eseguire automaticamente azioni, solitamente online. Sebbene la maggior parte dei bot sia innocua, un utilizzo crescente di bot dannosi è rappresentato dai botnet. Molti computer sono infetti da bot programmati per restare in attesa dei comandi dell'autore degli attacchi.

Ransomware: questo malware è progettato per tenere bloccato un sistema informatico o i dati in esso contenuti fino al pagamento di una somma. Il ransomware solitamente agisce crittografando i dati nel computer con una chiave sconosciuta all'utente. Altre versioni del ransomware possono sfruttare vulnerabilità specifiche del sistema per bloccare il sistema. ll ransomware viene diffuso nel sistema da un file scaricato o mediante una determinata vulnerabilità software.

Scareware: è un tipo di malware progettato per indurre l'utente a eseguire un'azione specifica facendo leva sulla paura. Lo scareware crea finestre pop-up simili alle finestre di dialogo del sistema operativo. Queste finestre visualizzano messaggi creati per informare l'utente che il sistema è a rischio o che necessita dell'esecuzione di un programma specifico per tornare allo stato normale di funzionamento. In realtà, non è stato accertato o rilevato alcun problema e se l'utente accetta e approva l'esecuzione del programma indicato, il sistema viene infettato da malware.

Rootkit: questo malware è progettato per modificare il sistema operativo al fine di creare una backdoor. Gli autori degli attacchi utilizzano poi la backdoor per accedere al computer in remoto. La maggior parte dei rootkit sfrutta le vulnerabilità software per eseguire l'escalation dei privilegi e modificare i file di sistema. È inoltre frequente che i rootkit modifichino gli strumenti di monitoraggio e le analisi forensi del sistema, rendendone estremamente difficile il rilevamento. Spesso, per un computer infetto da rootkit occorre procedere alla cancellazione e reinstallazione dei dati del sistema.

Virus: un virus è un codice eseguibile dannoso collegato ad altri file eseguibili, spesso programmi legittimi. La maggior parte dei virus richiede attivazione da parte dell'utente finale e può attivarsi a un'ora o una data specifica. I virus possono essere innocui e visualizzare semplicemente un'immagine o distruttivi, ad esempio quelli progettati per modificare o eliminare i dati. Possono inoltre essere programmati per mutare ed evitare il rilevamento. La diffusione della maggior parte dei virus ora avviene per mezzo di unità USB, dischi ottici, condivisioni di rete o e-mail.

Trojan horse: un Trojan horse è un tipo di malware che esegue operazioni dannose sotto forma di un'operazione desiderata. Questo codice dannoso procede all'exploit dei privilegi dell'utente che lo esegue. I trojan sono spesso presenti in file di immagini, file audio o giochi. Un Trojan horse differisce da un virus perché si associa a file non eseguibili.

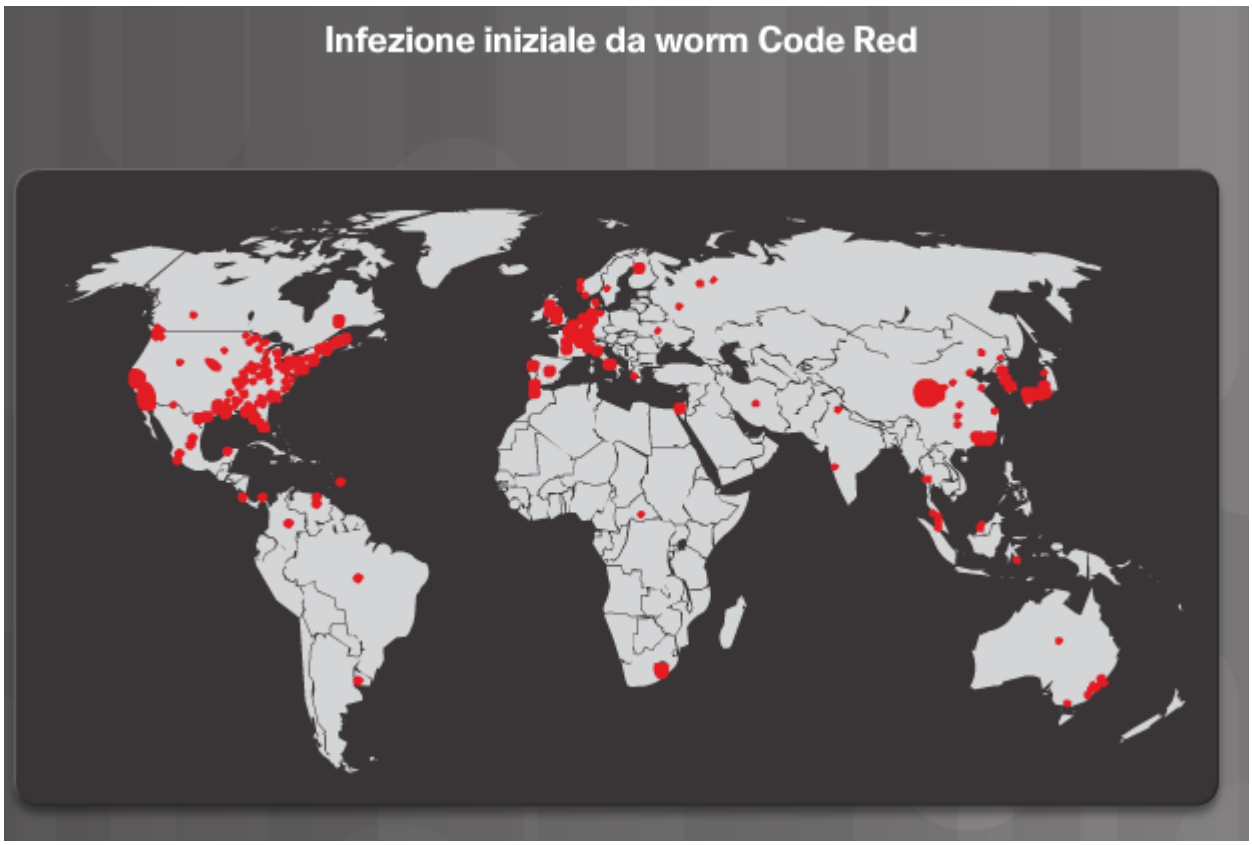
Worm: i worm sono costituiti da codice dannoso che si replica in modo autonomo sfruttando le vulnerabilità nelle reti. Solitamente i worm rallentano le reti. Mentre per l'esecuzione di un virus occorre un programma host, i worm possono attivarsi autonomamente. Dopo l'infezione iniziale, non necessitano più di alcuna interazione da parte dell'utente. Quando l'host è infettato, il worm è in grado di diffondersi molto rapidamente in rete. I worm condividono pattern analoghi. Tutti hanno una vulnerabilità abilitante, un modo per propagarsi e contengono un payload.

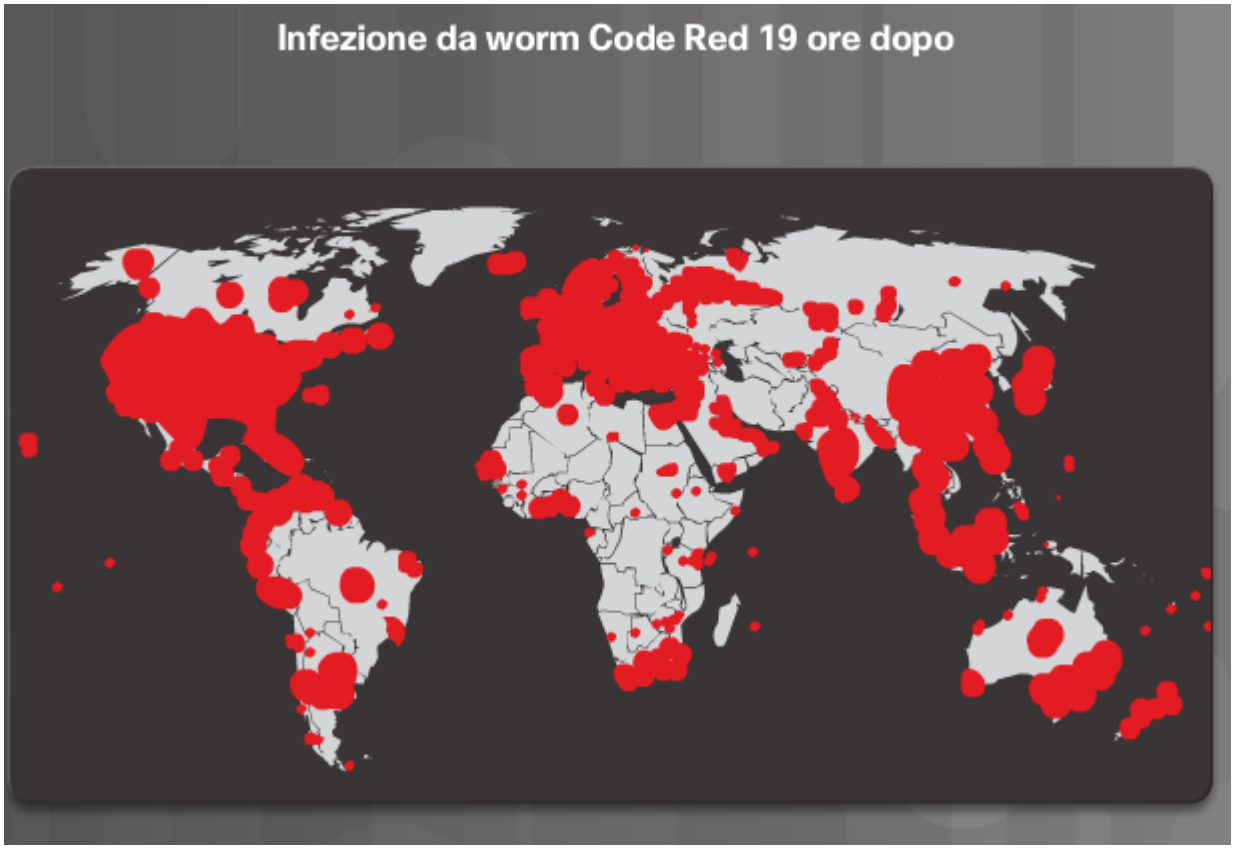
I worm sono responsabili di alcuni degli attacchi più devastanti di Internet. Nel 2001 il worm Code Red aveva infettato 658 server. Dopo 19 ore, il worm aveva infettato 300.000 server .

Man-In-The-Middle (MitM): il MitM consente all'autore dell'attacco di prendere il controllo su un dispositivo senza che l'utente ne sia a conoscenza. Con questo livello di accesso, l'autore dell'attacco

può intercettare e acquisire informazioni dell'utente prima del loro trasferimento nella destinazione prevista. Gli attacchi di tipo MitM sono ampiamente utilizzati per il furto di informazioni di natura finanziaria. Esistono molte tecniche e tipologie di malware che forniscono agli autori degli attacchi funzionalità MitM.

Man-In-The-Mobile (MitMo): variazione di man-in-middle, il MitMo è un tipo di attacco impiegato per acquisire il controllo su un dispositivo mobile. Una volta infettato, al dispositivo mobile può essere richiesto di esfiltrare informazioni sensibili dell'utente e inviarle agli autori degli attacchi. ZeuS, un esempio di exploit con funzionalità MitMo, consente agli autori degli attacchi di acquisire silenziosamente i messaggi SMS di verifica in 2 fasi inviati agli utenti.





Sintomi del malware

Di seguito sono riportati sintomi di infezione da malware comuni a prescindere dal tipo di malware con cui è stato infettato un sistema:

- Aumento nell'utilizzo di CPU.
- Riduzione nella velocità del computer.
- Il computer spesso si blocca o si arresta in modo anomalo.
- Riduzione nella velocità di navigazione nel Web.
- Problemi inspiegabili con le connessioni di rete.
- File modificati.
- File eliminati.
- Presenza di file, programmi o icone desktop sconosciuti.
- Processi sconosciuti in esecuzione.
- I programmi si disattivano o riconfigurano autonomamente.
- Invio di e-mail senza che l'utente ne sia a conoscenza o abbia acconsentito.

Social engineering

Il social engineering è un attacco di accesso in cui si tenta di manipolare gli utenti nell'esecuzione di azioni o nella divulgazione di informazioni riservate. I social engineer spesso contano sulla disponibilità delle persone a rendersi utili oltre ad approfittare delle loro debolezze. L'autore degli attacchi, ad esempio, potrebbe contattare un dipendente autorizzato con un problema urgente che richiede accesso immediato alla rete. Potrebbe far leva sulla vanità del dipendente, evocare autorità con tecniche di name-dropping o fare ricorso alla cupidigia del dipendente.

Di seguito sono riportati alcuni tipi di attacchi di social engineering:

- **Pretexting**: si ha quando l'autore degli attacchi si rivolge a un individuo mentendogli nel tentativo di ottenere l'accesso a dati con privilegi. Ne è un esempio un autore di attacchi che finge di avere necessità di dati di natura personale o finanziaria per poter verificare l'identità del destinatario.
- **Tailgating**: si ha quando l'autore degli attacchi segue rapidamente una persona autorizzata in un luogo sicuro.
- **Something for Something (Quid pro quo)**: si ha quando l'autore degli attacchi chiede dati personali a un interlocutore in cambio di qualcosa, ad esempio un regalo.

Violazione delle password Wi-Fi

Per violazione delle password Wi-Fi si intende il processo di individuazione delle password utilizzate per proteggere una rete wireless. Di seguito sono riportate alcune tecniche utilizzate nella violazione delle password:

Social engineering: l'autore degli attacchi manipola una persona per farsi comunicare la password di cui è a conoscenza.

Attacchi "brute-force": l'autore degli attacchi prova varie password nel tentativo di indovinare quella giusta. Se la password è un numero di 4 cifre, ad esempio, l'autore degli attacchi dovrebbe provare tutte e 10.000 le combinazioni. Gli attacchi "brute-force" si avvalgono solitamente di un file elenco di parole. Si tratta di un file di testo contenente un elenco di parole estratte da un dizionario. Un programma prova ogni parola e le combinazioni più comuni. Dato che gli attacchi "brute-force" richiedono tempo, per indovinare password complesse ne occorre molto di più. Alcuni degli strumenti di attacco "brute-force" per le password sono Ophcrack, L0phtCrack, THC Hydra, RainbowCrack e Medusa.

Network sniffing: restando in ascolto dei pacchetti inviati sulla rete e acquisendoli, l'autore degli attacchi potrebbe riuscire a scoprire la password se questa è stata inviata in forma non crittografata. Quando la password è crittografata, l'autore degli attacchi può riuscire comunque a identificarla utilizzando uno strumento di violazione delle password.

Phishing

Il phishing consiste nell'invio da parte di un utente malintenzionato, di un’e-mail fraudolenta dissimulata come proveniente da una fonte legittima e attendibile. L'intento del messaggio è convincere con l'inganno il destinatario a installare il malware sul dispositivo o a condividere dati di natura personale o finanziaria. Un esempio di phishing è un'e-mail creata per sembrare inviata da un negozio al dettaglio, in cui si chiede all'utente di selezionare un collegamento per ottenere un

premio. Il collegamento potrebbe accedere a un finto sito in cui si richiedono dati personali oppure installare un virus.

Lo spear phishing è un attacco di tipo phishing altamente mirato. Sebbene sia il phishing che lo spear phishing utilizzino e-mail per raggiungere le vittime, le e-mail inviate da quest'ultimo sono personalizzate per un individuo specifico. L'autore degli attacchi prima di inviare l'e-mail esegue una ricerca sugli interessi dell'obiettivo. Ad esempio, l'autore degli attacchi scopre che l'obiettivo è interessato alle auto e sta valutando di acquistare un modello specifico. L'autore degli attacchi si collega allo stesso forum di discussione sulle auto di cui è membro l'obiettivo, crea un'offerta di vendita di auto e invia l'e-mail all'obiettivo. L'e-mail contiene un collegamento per accedere alle immagini dell'auto. Quando l'obiettivo seleziona il collegamento, il malware viene installato sul computer dell'obiettivo.

Exploit delle vulnerabilità

L'exploit delle vulnerabilità è un altro metodo diffuso di infiltrazione. Gli autori degli attacchi analizzano i computer per ottenerne le informazioni. Di seguito è riportato un metodo diffuso di exploit delle vulnerabilità:

Fase 1. Raccolta di informazioni sul sistema obiettivo. Questa operazione è eseguibile in molti modi differenti, ad esempio mediante scanner di porte o social engineering. L'intento è apprendere quanto più possibile sul computer obiettivo.

Fase 2. Una parte delle informazioni pertinenti ottenute nella fase 1, potrebbe riguardare il sistema operativo, la relativa versione e un elenco dei servizi in esecuzione su di esso.

Fase 3. Una volta conosciuti sistema operativo e versione dell'obiettivo, l'autore degli attacchi cerca vulnerabilità note specifiche di tale versione di sistema operativo o di altri servizi del sistema operativo.

Fase 4. Individuata una vulnerabilità, l'autore degli attacchi cerca un exploit scritto in precedenza da utilizzare. Se non è stato scritto alcun exploit, l'autore degli attacchi può considerare di scriverne uno.

Minacce persistenti avanzate

Uno dei metodi utilizzati per penetrare in un sistema sono le minacce avanzate persistenti (APT). Si tratta di un'operazione multi fase avanzata e dissimulata a lungo termine posta in essere contro un obiettivo specifico. Data la sua complessità e il livello di competenza richiesto, un APT è ben finanziato. Un APT è mirato a organizzazioni o nazioni per motivi commerciali o politici.

Generalmente collegato allo spionaggio basato sulla rete, lo scopo dell'APT è implementare malware personalizzato su uno o più dei sistemi obiettivo senza essere rilevato. Essendo caratterizzato da un'operazione multi fase e da vari tipi personalizzati di malware che interessano dispositivi differenti ed eseguono funzioni diverse, un singolo autore di attacchi manca spesso della serie di competenze, delle risorse o della perseveranza necessarie per un attacco di tipo APT.

DoS

Gli attacchi Denial-of-Service (DoS) sono un tipo di attacchi alla rete. Un attacco DoS genera una sorta di interruzione del servizio di rete a utenti, dispositivi o applicazioni. Esistono due tipi principali di attacchi DoS:

Overwhelming Quantity of Traffic: in questo tipo di attacco un enorme volume di dati viene inviato a una rete, un host o un'applicazione a una velocità ingestibile. Ciò causa un rallentamento nella trasmissione o nella risposta oppure l'arresto anomalo di un dispositivo o di un servizio.

Maliciously Formatted Packets: in questo tipo di attacco un pacchetto formattato con intento dannoso viene inviato a un host o a un'applicazione e il ricevente non è in grado di gestirlo. Ad esempio, l'autore degli attacchi invia pacchetti contenenti errori non identificabili dall'applicazione oppure inoltra pacchetti non correttamente formattati. In tal modo, il dispositivo ricevente risulta estremamente lento oppure si arresta in modo anomalo.

Gli attacchi DoS sono considerati un grave rischio in quanto possono facilmente interrompere la comunicazione e causare significative perdite di tempo e denaro. Questi attacchi sono relativamente semplici da attuare, anche da un autore di attacchi inesperto.

DDoS

Un attacco Distributed DoS (DDoS) è simile al DoS ma originato da più sorgenti coordinate. Ad esempio, un attacco DDoS potrebbe procedere nel seguente modo:

> L'autore degli attacchi crea una rete di host infetti denominata botnet. Gli host infetti sono detti zombie. Gli zombie sono controllati da sistemi gestori.
>
> I computer zombie analizzano e infettano costantemente altri host, creando nuovi zombie. Una volta pronto, l'hacker ordina ai sistemi gestori di far eseguire ai botnet di zombie un attacco DDoS.

Alterazione SEO

I motori di ricerca come Google operano classificando le pagine e presentando risultati pertinenti basati sulle query di ricerca degli utenti. A seconda della pertinenza del contenuto del sito Web, possono comparire ai livelli più alti o più bassi dell'elenco dei risultati di ricerca. Con l'acronimo SEO, Search Engine Optimization ovvero ottimizzazione dei motori di ricerca, sono identificate una serie di tecniche utilizzate per migliorare la classificazione di un sito Web da parte del motore di ricerca. Anche se molte aziende legittime sono specializzate nell'ottimizzazione dei siti Web per migliorarne la posizione di visualizzazione, un utente malintenzionato potrebbe utilizzare tecniche SEO per fare in modo che un sito Web dannoso compaia nelle prime posizioni dei risultati di ricerca. Questa tecnica è detta SEO poisoning.

L'obiettivo più comune del SEO poisoning è aumentare il traffico verso siti dannosi che potrebbero contenere malware o eseguire il social engineering. Per forzare il posizionamento di un sito dannoso ai livelli più alti dei risultati di ricerca, gli autori degli attacchi si avvalgono dei termini di ricerca più diffusi.

Che cos'è un attacco misto?

Gli attacchi misti utilizzano varie tecniche per compromettere un obiettivo. Impiegando contemporaneamente più tecniche di tipo diverso, gli autori degli attacchi ottengono malware che sono un ibrido degli schemi di worm, Trojan horse, spyware, keylogger, spam e phishing. Il trend degli attacchi misti è rivelatore di malware più complessi ed espone i dati degli utenti a un grande rischio.

La tipologia più comune di attacco misto si avvale di messaggi e-mail spam, messaggistica istantanea o siti Web legittimi per distribuire collegamenti da cui vengono scaricati segretamente malware o spyware sul computer. Un altro attacco misto molto diffuso impiega il DDoS in combinazione con e-mail di phishing. Inizialmente, il DDoS viene utilizzato per disattivare il sito Web di una Banca conosciuta e inviare e-mail ai clienti della banca per scusarsi dell'inconveniente. L'e-mail indirizza inoltre gli utenti su un falso sito di emergenza che consente il furto dei loro dati di accesso reali.

Molti dei worm più dannosi per i computer come Nimbda, CodeRed, BugBear, Klez e Slammer sono classificati più specificatamente come attacchi misti, come indicato di seguito:

- Alcune varianti di Nimbda utilizzavano allegati e-mail, download di file da un server Web violato e il file sharing (condivisione di file) Microsoft (ad es. condivisioni anonime) come metodi di propagazione.

- Altre varianti di Nimbda erano in grado di modificare gli account guest del sistema per fornire privilegi amministrativi all'autore degli attacchi o al codice dannoso.

Anche i recenti worm Conficker e ZeuS/LICAT sono stati classificati come attacchi misti. Conficker faceva ricorso a tutti i metodi di propagazione tradizionali.

Cosa si intende per riduzione dell'impatto?

Sebbene la maggior parte delle odierne aziende di successo sia a conoscenza dei problemi di sicurezza più comuni e dedichi notevole impegno alla loro prevenzione, nessuna procedura di sicurezza è efficiente al 100%. Poiché una violazione è probabile che si verifichi quando la ricompensa è alta, le aziende e le organizzazioni devono essere preparate anche a contenere i danni.

È importante capire che l'impatto di una violazione non è connesso esclusivamente all'aspetto tecnico di essa, ad esempio furto di dati, danneggiamento di database o danni alla proprietà intellettuale, ma i danni si estendono anche alla reputazione dell'azienda. Rispondere a una violazione dei dati è un processo estremamente dinamico.

Di seguito sono riportate alcune importanti misure che un'azienda dovrebbe adottare, secondo molti esperti di sicurezza, quando viene identificata una violazione della sicurezza:

- Comunicare il problema. Internamente i dipendenti devono essere informati del problema e invitati a intraprendere azioni adeguate. Esternamente, i clienti devono essere informati tramite comunicazione diretta e annunci ufficiali. La comunicazione crea trasparenza, fattore essenziale in questo tipo di situazione.
- È importante essere sinceri e responsabili in caso di colpa dell'azienda.
- Fornire dettagli. Spiegare a cosa è dovuta la situazione e cosa è stato compromesso. Si presume inoltre che l'azienda si faccia carico dei costi relativi ai servizi di protezione dal furto di identità per i clienti interessati.
- Capire cosa ha causato e facilitato la violazione. Se necessario rivolgersi a esperti in analisi forense per cercare e scoprire i dettagli.
- Utilizzare quanto scoperto dall'indagine forense per fare in modo che simili violazioni non si ripetano in futuro.
- Verificare che tutti i sistemi siano puliti, non sia stata installata alcuna backdoor e nient'altro sia stato compromesso. Gli autori degli attacchi spesso tentano di lasciare una backdoor per agevolare future violazioni. Verificare che questa situazione non si verifichi.
- Istruire dipendenti, partner e clienti su come evitare future violazioni.

Proteggere dati e privacy

Questo capitolo è incentrato sui dispositivi e i dati personali. Contiene suggerimenti per la protezione dei dispositivi, la creazione di password complesse e l'utilizzo sicuro delle reti wireless. Nel capitolo si analizza inoltre l'aspetto della sicurezza costante dei dati.

I dati online sono preziosi per i criminali informatici. In questo capitolo vengono illustrate brevemente le tecniche di autenticazione che consentono di mantenere al sicuro i propri dati. Vengono spiegati inoltre metodi utili per migliorare la sicurezza dei dati online con suggerimenti riguardo alle operazioni eseguibili o meno online.

Proteggere i dispositivi di elaborazione

I dispositivi di elaborazione memorizzano i dati e sono il portale per la vita online dell'utente. Di seguito è riportato un breve elenco dei possibili passi da intraprendere per proteggere i dispositivi di elaborazione dalle intrusioni:

- **Mantenere il firewall attivo:** che sia di tipo software o di tipo hardware installato su un router, il firewall deve essere attivato e aggiornato per impedire agli hacker di accedere ai dati personali o aziendali. Fare clic su Windows 7, Windows 8o Windows 10 per attivare il firewall nella rispettiva versione di Windows. Fare clic qui per attivare il firewall sui dispositivi Mac OS X.

- **Utilizzare antivirus e antispyware**: il software dannoso, ad esempio virus, Trojan horse, worm, ransomware e spyware, viene installato sui dispositivi di elaborazione senza autorizzazione dell'utente per ottenere l'accesso al computer e ai dati in esso contenuti. I virus possono distruggere i dati, rallentare il computer o assumerne il controllo. Un modo con cui i virus possono assumere il controllo del computer è permettendo agli spammer di trasmettere e-mail tramite l'account dell'utente. Uno spyware è in grado di monitorare le attività online dell'utente, raccogliere dati personali o produrre pubblicità popup indesiderata sul browser Web mentre l'utente è online. Un'ottima regola è scaricare software esclusivamente da siti Web attendibili, innanzitutto per evitare l'installazione di spyware. Il software antivirus è progettato per analizzare il computer e le e-mail in entrata allo scopo di individuare eventuali virus ed eliminarli. Talvolta il software antivirus contiene anche un antispyware. È importante mantenere aggiornato il software per proteggere il computer dal software dannoso più recente.

- **Gestire sistema operativo e browser**: gli hacker tentano sempre di sfruttare le vulnerabilità dei sistemi operativi e dei browser Web. Per proteggere computer e dati, configurare le impostazioni di sicurezza di computer e browser su un livello di protezione medio o alta. Aggiornare il sistema operativo del computer compresi i browser Web e scaricare e installare regolarmente le patch software e gli aggiornamenti di sicurezza più recenti messi a disposizione dai fornitori.

- **Proteggere tutti i dispositivi:** i dispositivi di elaborazione, che siano PC, laptop, tablet o smartphone, devono essere protetti da password per prevenire l'accesso non autorizzato. Le informazioni memorizzate devono essere crittografate, in particolare per quanto riguarda i dati sensibili o riservati. Per i dispositivi mobili, memorizzare esclusivamente le informazioni necessarie, nell'eventualità che questi dispositivi vengano rubati o smarriti quando non si è in casa. Se uno qualsiasi dei dispositivi subisce violazioni, i criminali informatici possono avere accesso a tutti i dati tramite il provider di servizi di cloud storage, ad esempio iCloud o Google Drive.

I dispositivi IoT espongono l'utente ad un rischio persino maggiore dei dispositivi di elaborazione. Sebbene desktop, laptop e piattaforme mobili ricevano aggiornamenti software frequenti, la maggior parte dei dispositivi IoT continua a mantenere il firmware originale. Se nel firmware vengono individuate vulnerabilità, è probabile che il dispositivo IoT rimanga vulnerabile. A peggiorare il problema, i dispositivi IoT sono spesso progettati per chiamare casa e richiedono accesso a Internet. Per raggiungere Internet, la maggior parte dei produttori di dispositivi IoT utilizza la rete locale del cliente. Ne consegue che i dispositivi IoT sono più soggetti a violazioni e quando accade consentono l'accesso alla rete locale e ai dati del cliente. Il miglior modo per proteggersi da questo scenario è avere dispositivi IoT in una rete isolata condivisa solo con altri dispositivi IoT.

Fare clic qui per visitare Shodan, uno strumento di analisi di dispositivi IoT basato su Web.

Utilizzare le reti wireless in sicurezza

Le reti wireless consentono ai dispositivi compatibili Wi-Fi, ad esempio laptop e tablet, di collegarsi alla rete mediante l'identificatore di rete, noto come SSID (Service Set Identifier). Per evitare intrusioni nella rete wireless domestica, occorre modificare lo SSID preimpostato e la password predefinita per l'interfaccia di amministrazione basata su browser. Gli hacker conoscono questo genere di informazioni di accesso predefinite. È inoltre necessario crittografare la comunicazione wireless abilitando le funzioni di sicurezza wireless e crittografia WPA2 sul router wireless. Facoltativamente, il router wireless può essere configurato per non trasmettere lo SSID, aggiungendo un'ulteriore protezione dal rilevamento della rete, anche se questa misura non deve essere considerata una protezione adeguata per una rete wireless.

Fare clic qui per ulteriori informazioni sulla protezione dei dati in caso di utilizzo delle reti wireless.

Quando si è fuori casa, un hot spot Wi-Fi pubblico consente di accedere ai dati online e navigare in Internet. È tuttavia consigliabile non accedere ad alcun dato personale sensibile o inviarlo tramite una rete wireless pubblica. Verificare se il computer è configurato con condivisione di file e supporti e controllare che richieda l'autenticazione dell'utente con crittografia. Per evitare che altri possano intercettare i dati (operazione nota come "eavesdropping") durante l'utilizzo di una rete wireless pubblica è opportuno utilizzare tunnel e servizi VPN crittografati. Il servizio VPN fornisce accesso sicuro a Internet, con una connessione crittografata tra il computer e il server VPN del provider di servizi VPN. Con un tunnel VPN crittografato, anche se la trasmissione dati viene intercettata non è decifrabile.

Molti dispositivi, come smartphone e tablet, sono forniti con il protocollo wireless Bluetooth. Questa funzionalità consente ai dispositivi abilitati Bluetooth di collegarsi fra loro e condividere informazioni. Sfortunatamente, gli hacker possono eseguire l'exploit della funzionalità Bluetooth per intercettare le trasmissioni su alcuni dispositivi, stabilire controlli degli accessi in remoto, distribuire malware e scaricare le batterie. Per evitare questi problemi, disattivare la funzionalità Bluetooth quando non è in uso.

Utilizzare password univoche per ogni account online

È probabile che si possegga più di un account online e ogni account deve avere una password univoca. Le password da ricordare sono molte. Tuttavia, il mancato utilizzo di password complesse e univoche rende l'utente e i suoi dati vulnerabili agli attacchi dei criminali. Utilizzare la stessa password per tutti gli account online è come utilizzare la stessa chiave per tutte le porte, se l'autore degli attacchi riuscisse a scoprire la password avrebbe la possibilità di accedere a tutto ciò che l'utente possiede. Qualora i criminali informatici ottenessero la password ad esempio tramite un attacco di phishing, tenterebbero di accedere agli altri account online. Se l'utente utilizza una sola password valida per tutti gli account, i criminali possono accedere a qualsiasi account, rubare o cancellare i dati oppure decidere di agire fingendo di essere l'utente.

Utilizziamo talmente tanti account che necessitano di password: sono troppi dati da ricordare. Una soluzione per evitare di riutilizzare le password oppure di utilizzare password vulnerabili è avvalersi di uno strumento per la gestione di password. Tale strumento memorizza e cripta tutte le varie password complesse dell'utente. Lo strumento può quindi aiutare l'utente ad accedere

automaticamente agli account online. La sola password da ricordare è quella master per accedere allo strumento per la gestione delle password e gestire tutti gli account e le password.

Suggerimenti per la scelta di una buona password:

- Non utilizzare parole o nomi tratti da un dizionario in qualsiasi lingua sia
- Non utilizzare errori ortografici comuni di parole del dizionario
- Non utilizzare nomi di computer o di account
- Se possibile, usa caratteri speciali come ! @ # $ % ^ & * ( )
- Utilizzare una password composta da almeno dieci caratteri

Utilizzare passphrase anziché password

Per evitare l'accesso fisico non autorizzato ai dispositivi di elaborazione, è possibile utilizzare passphrase al posto delle password. È più facile creare una passphrase lunga che una password in quanto generalmente è in forma di frase anziché di parola. La maggiore lunghezza rende la passphrase meno vulnerabile agli attacchi con dizionario o brute force. Inoltre, una passphrase è forse più semplice da ricordare in particolare quando occorre cambiare password di frequente. Di seguito sono riportati alcuni suggerimenti per la scelta di buone password o passphrase:

Suggerimenti per la scelta di una buona passphrase:

- Scegliere un'affermazione significativa
- Aggiungere caratteri speciali come ! @ # $ % ^ & * ( )
- Maggiore è la lunghezza e migliore è la passphrase
- Evitare frasi comuni o famose, ad esempio testi di una canzone famosa

Anche se l'accesso ai computer e ai dispositivi di rete è protetto, è importante proteggere e preservare i dati.

Crittografare i dati

I dati devono sempre essere crittografati. Potresti pensare di non avere segreti né niente da nascondere, quindi per quale motivo ricorrere alla crittografia? Potresti inoltre pensare che a nessuno interessino i tuoi dati. Probabilmente non è così.

Sei pronto a mostrare foto e documenti agli estranei? Sei pronto a condividere con gli amici le informazioni finanziarie memorizzate sul computer? Intendi rendere note al pubblico e-mail e password di account?

Può essere un problema persino maggiore se un'applicazione dannosa infetta il computer o il dispositivo mobile sottraendo informazioni potenzialmente preziose, numeri di conto e password e altri documenti ufficiali. Questo tipo di informazioni può portare a furti di identità, frodi o richieste di riscatto. I criminali informatici potrebbero decidere semplicemente di crittografare i dati e renderli inutilizzabili fino al pagamento di un riscatto.

Cos'è la crittografia? La crittografia è il processo di conversione delle informazioni in formato non leggibile da terzi non autorizzati. Solo una persona autorizzata e attendibile in possesso della chiave o della password segreta è in grado di decriptare i dati e accedervi nel formato originale. La

crittografia in sé non evita l'intercettazione dei dati. Può soltanto impedire che persone non autorizzate visualizzino il contenuto o vi accedano.

Per crittografare file, cartelle e persino intere unità vengono utilizzati programmi software.

Encrypting File System (EFS) è una funzionalità Windows per la crittografia dei dati. L'EFS è direttamente collegata a un account utente specifico. Solo l'utente che ha crittografato i dati potrà accedervi una volta crittografati con EFS. Per crittografare i dati utilizzando la funzionalità EFS in tutte le versioni Windows, procedere come descritto di seguito:

Fase 1. Selezionare uno o più file o cartelle.

Fase 2. Fare clic con il pulsante destro del mouse sui dati selezionati **>Proprietà**.

Fase 3. Fare clic su **Avanzate…**

Fase 4. Selezionare la casella di controllo **Crittografa contenuto per la protezione dei dati**.

Fase 5. I file e le cartelle crittografati con EFS vengono visualizzati in verde come illustrato nella figura.

Eseguire il backup dei dati

Malfunzionamento dell'Hard Drive. Smarrimento del laptop. Furto dello smartphone. Cancellazione della versione originale di un documento importante. L'uso del backup potrebbe evitare la perdita di dati insostituibili, ad esempio le foto di famiglia. Per eseguire correttamente il backup, è necessario una posizione di archiviazione aggiuntiva per copiarvi automaticamente e con regolarità i dati.

La posizione aggiuntiva per i file di backup può essere sulla rete locale, un percorso secondario oppure nel cloud. Archiviando il backup dei dati localmente, l'utente ha il controllo totale dei dati. Si può decidere di copiare tutti i dati su un dispositivo Network Attached Storage (NAS), un semplice hard drive esterno o anche di selezionare poche cartelle importanti per il backup su pen drive, CD/DVD oppure nastri. In tale scenario, l'utente è il proprietario ed è totalmente responsabile per il costo e la manutenzione della periferica di memorizzazione. Abbonandosi a un servizio di cloud storage il costo dipende dallo spazio di archiviazione necessario. Con un servizio di cloud storage come Amazon Web Services (AWS), l'utente ha accesso ai dati di backup fino a quando ha accesso all'account. Un abbonamento a servizi di archiviazione online, potrebbe richiedere maggiore selettività riguardo ai dati di cui eseguire il backup per il costo dell'archiviazione e i costanti trasferimenti di dati online. Uno dei vantaggi dell'archiviazione di un backup in una posizione alternativa è la sicurezza in caso di incendio, furto o altre catastrofi diverse dal guasto della periferica di memorizzazione.

Eliminazione permanente dei dati

Quando si sposta un file nel cestino o si elimina in modo permanente, il file viene semplicemente reso inaccessibile dal sistema operativo. Chiunque con gli strumenti forensi adatti può ancora recuperarlo grazie a una traccia magnetica lasciata sull'hard drive.

Per cancellare i dati in modo che non siano più recuperabili, devono essere sovrascritti più volte con valori uno e zero. Per evitare il recupero di file eliminati, possono servire strumenti appositamente progettati per tale operazione. Il programma SDelete di Microsoft (per Vista e versione superiore), è proposto come in grado di rimuovere completamente i file sensibili. Shred per Linux e Secure Empty Trash per Mac OSX sono strumenti che forniscono un servizio analogo.

Il solo modo per avere la certezza che i dati o i file non siano recuperabili, è distruggere fisicamente l'hard drive o la periferica di memorizzazione. Molti criminali hanno pensato follemente che i propri file fossero impenetrabili o non recuperabili.

Oltre ad archiviarli sugli hard drive locali, i dati possono essere memorizzati online nel cloud. Anche queste copie devono essere eliminate. Occorre chiedersi "dove sono salvati i miei dati?" Esiste un backup da qualche parte? Sono crittografati? Quando è necessario eliminare i dati o disfarsi di un hard drive o di un computer, la domanda da farsi è "Ho protetto i dati per impedire che cadessero in mani sbagliate?"

Autenticazione a due fattori

Servizi online molto diffusi come Google, Facebook, Twitter, LinkedIn, Apple e Microsoft, utilizzano l'autenticazione a due fattori per aumentare il livello di sicurezza dell'accesso all'account. Oltre a nome utente e password o al PIN (Personal Identification Number) o percorso, l'autenticazione a due fattori richiede un secondo token, ad esempio:

- **Un oggetto fisico**: carta di credito, carta Bancomat, telefono o fob
- **Una scansione biometrica**: impronte digitali, impronta palmare e riconoscimento facciale o vocale

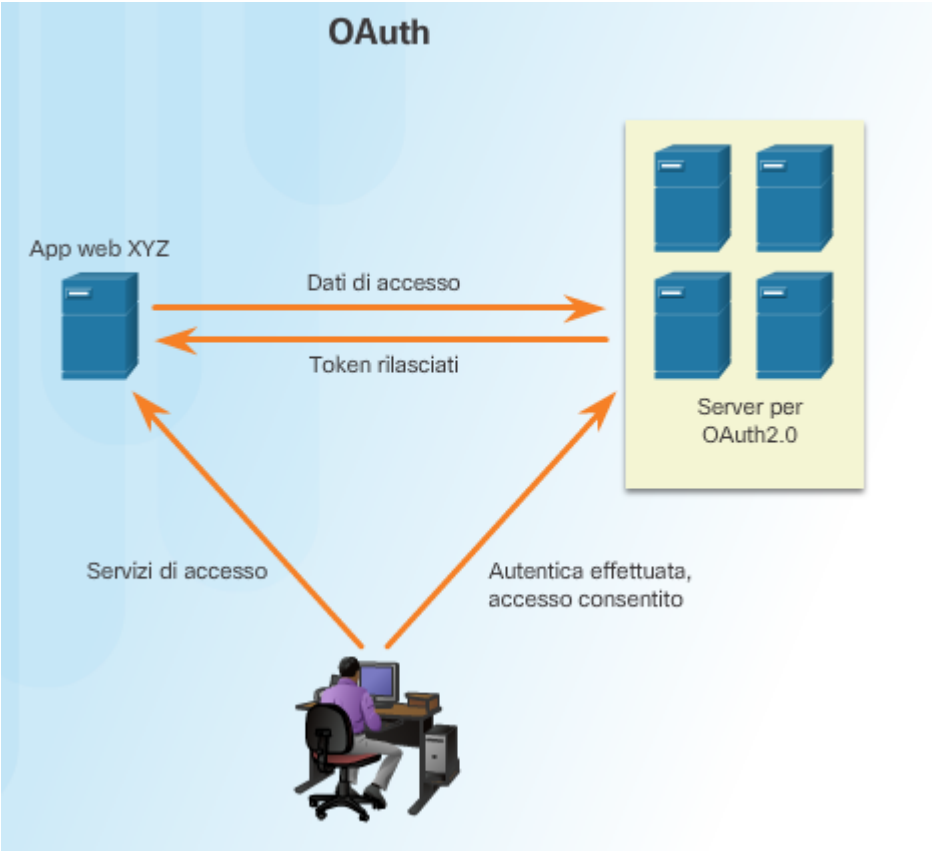
Anche con l'autenticazione a due fattori, gli hacker possono ancora accedere agli account online tramite attacchi quali phishing, malware e social engineering.

Vai qui per scoprire se i siti Web visitati utilizzano l'autenticazione a due fattori.

OAuth 2.0

Open Authorization (OAuth) è un protocollo standard aperto che permette alle credenziali degli utenti finali di accedere alle applicazioni di terze parti senza esporre la password. OAuth agisce da intermediario nella decisione se consentire o meno agli utenti finali di accedere ad applicazioni di terze parti. Ad esempio, si desidera accedere all'applicazione Web XYZ e non si dispone di un account utente per l'accesso a questa applicazione Web. Tuttavia, XYZ ha la possibilità di consentire l'accesso utilizzando le credenziali del sito Web social media ABC. Quindi si accede al sito Web con le credenziali di accesso del social media.

Per questa operazione, l'applicazione "XYZ" viene registrata con "ABC" ed è un'applicazione approvata. Quando si accede a XYZ si utilizzano le credenziali per ABC. Quindi XYZ richiede un token di accesso ad ABC per proprio conto. A questo punto si ha l'accesso a XYZ. XYZ non possiede informazioni sull'utente e le credenziali utente e questa interazione è totalmente trasparente per l'utente. L'utilizzo di token segreti evita che applicazioni dannose acquisiscano informazioni e dati dell'utente.



Non condividere troppe informazioni sui social media

Per poter salvaguardare la propria privacy sui social media, è necessario condividere il minor numero possibile di informazioni. Non è consigliabile condividere informazioni come data di nascita, indirizzo e-mail o numero di telefono sul proprio profilo. Chi ha bisogno di conoscere tali dati personali probabilmente li conosce già. Non compilare completamente il profilo sui social media, ma fornisci solo le informazioni minime obbligatorie. Inoltre, è importante controllare le impostazioni del social media per consentire soltanto alle persone conosciute di visualizzare le attività o avviare conversazioni.

Più dati personali si condividono online e più facile è per qualcuno creare un profilo basato su tali dati e trarne vantaggio offline.

Hai dimenticato nome utente e password per un account online? Si suppone che domande di sicurezza come "qual è il nome da nubile di tua madre?" o "in quale città sei nato?" aiutino a proteggere gli account dagli intrusi. Tuttavia, chi desidera accedere agli account può cercare le risposte su Internet. Puoi rispondere a queste domande fornendo informazioni false, purché tu riesca a ricordare le risposte. In caso di problemi a ricordarle, puoi avvalerti di uno strumento per la gestione delle password per gestirle.

Privacy di e-mail e browser Web

Ogni giorno si utilizzano milioni di messaggi e-mail per comunicare con gli amici e dirigere l'attività. L’e-mail è un mezzo comodo per comunicare velocemente. L'invio di un'e-mail è paragonabile all'invio di un messaggio su cartolina postale. Il messaggio su cartolina viene trasmesso in maniera visibile a chiunque sia in grado di guardarlo, il messaggio e-mail viene trasmesso in chiaro ed è leggibile a chi ne ha accesso. Queste comunicazioni passano inoltre da un

server all'altro durante il percorso verso la destinazione. Anche se i messaggi e-mail vengono cancellati, possono rimanere archiviati sui server di posta per un certo periodo.

Chi ha accesso fisico al computer o al router, può vedere quali siti Web sono stati visitati tramite la cronologia del browser Web, la cache e anche i file di log. Per ridurre al minimo questo problema è possibile abilitare la modalità di esplorazione in privato sul browser Web. La maggior parte dei browser Web più diffusi ha la propria modalità di esplorazione in privato:

- **Microsoft Internet Explorer**: InPrivate
- **Google Chrome**: Incognito
- **Mozilla Firefox**: scheda Private / finestra Private
- **Safari**: Private: Private browsing

Abilitando la modalità privata, i cookie vengono disabilitati e i file Internet temporanei insieme alla cronologia di esplorazione vengono rimossi alla chiusura della finestra o del programma.

Mantenere privata la cronologia di esplorazione può impedire ad altri utenti di ottenere informazioni sulle tue attività online e di indurti a effettuare acquisti con pubblicità mirate. Anche con la funzione di esplorazione privata abilitata e i cookie disabilitati, le aziende stanno sviluppando metodi diversi di fingerprinting degli utenti al fine di raccogliere informazioni e tracciarne il comportamento. Ad esempio, i dispositivi intermediari come i router, possono contenere informazioni sulla cronologia di esplorazione Web dell'utente.

In definitiva, è responsabilità dell'utente salvaguardare identità, dati e dispositivi di elaborazione. Quando si invia un'e-mail, occorre includere informazioni mediche? Alla successiva esplorazione di Internet, la trasmissione è sicura? Alcune semplici precauzioni possono eliminare i problemi in seguito.

Proteggere l'azienda

Questo capitolo verte su alcune delle tecnologie e alcuni processi utilizzati dai professionisti della cybersecurity per proteggere reti, apparecchiature e dati aziendali. Innanzi tutto, verranno illustrati i numerosi tipi di firewall, appliance di sicurezza e software attualmente utilizzati, insieme alle best-practice in vigore.

Successivamente, verranno analizzati i botnet, le tattiche kill chain, la sicurezza basata sui comportamenti e l'uso di NetFlow per il monitoraggio delle reti.

La terza sezione esamina l'approccio di Cisco alla cybersecurity, basato sui team CSIRT e sul manuale della sicurezza e mostra gli strumenti impiegati dai professionisti della cybersecurity per rilevare e prevenire gli attacchi alle reti.

Tipi di firewall

Il firewall è un muro o una partizione progettata per impedire la diffusione degli incendi da un punto all'altro degli edifici. Nelle reti di computer, il firewall è progettato per controllare o filtrare le comunicazioni autorizzate in ingresso e in uscita dai dispositivi o dalle reti, come mostrato nella figura. I firewall possono essere installati su singoli computer, allo scopo di proteggere ciascuno di essi (firewall basati su host) oppure possono essere costituiti da dispositivi di rete autonomi che

proteggono intere reti di computer nonché tutti i dispositivi host collegati a esse (firewall basati sulle reti).

Nel tempo, a mano a mano che gli attacchi ai computer e alle reti sono diventati sempre più sofisticati, sono stati sviluppati nuovi tipi di firewall che svolgono varie funzioni destinate alla protezione delle reti. Di seguito viene riportato l'elenco dei tipi di firewall più diffusi:

- **Firewall a livello di rete** – il filtro opera in base agli indirizzi IP d'origine e di destinazione
- **Firewall a livello di trasporto** – il filtro opera in base alle porte dati d'origine e di destinazione nonché sugli stati delle connessioni
- **Firewall a livello applicativo** – il filtro opera in base ad applicazioni, programmi e servizi
- **Firewall per il controllo di applicazioni basato sul contesto** – il filtro opera in base a utente, dispositivo, ruolo, applicazione e profilo della minaccia
- **Server proxy** – esegue il filtraggio delle richieste di contenuti Web quali URL, dominio, mezzi di comunicazione ecc
- **Server proxy reverse** – posizionati davanti ai server Web, i server proxy reverse proteggono, nascondono, eseguono l'offload e distribuiscono gli accessi ai server Web
- **Firewall NAT (Network Address Translation)** – nasconde o maschera gli indirizzi privati degli host di rete
- **Firewall basato su host** – esegue il filtraggio delle chiamate a porte e servizi di sistema nell'ambito del sistema operativo di un determinato computer

Scansione delle porte

La scansione delle porte è un processo di verifica di computer, server o altri host di rete volto all'individuazione di eventuali porte aperte. Nell'ambito di una rete, a ciascuna applicazione eseguita in un dispositivo viene assegnato un identificativo chiamato numero di porta. Il numero di porta è utilizzato a entrambe le estremità della trasmissione, affinché ciascun dato venga trasmesso correttamente all'applicazione che lo richiede. La scansione delle porte può essere utilizzata impropriamente come strumento di ricognizione per identificare il sistema operativo e i servizi eseguiti in un computer o host oppure, in modo legittimo, dagli amministratori di rete per verificare le policy di sicurezza all'interno di una rete.

Per valutare la sicurezza del firewall che protegge una rete di computer nonché quella delle porte, si può usare uno strumento per la scansione delle porte come Nmap per individuare tutte le porte aperte eventualmente presenti. La scansione delle porte può essere considerata come il segnale di un attacco alla rete imminente e, pertanto, non deve essere eseguita nei confronti di server pubblici collegati a Internet, né di reti aziendali, senza autorizzazione.

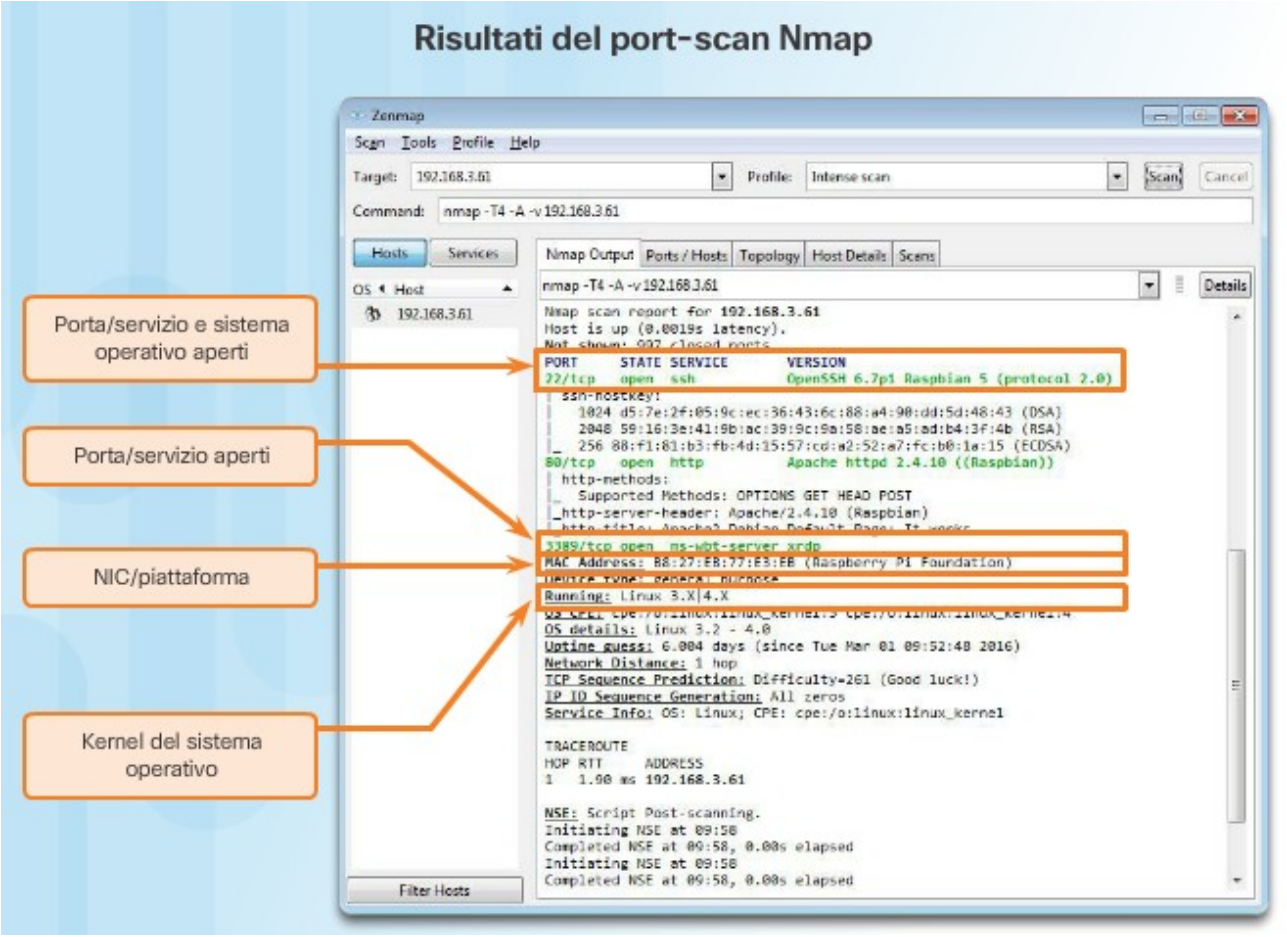
Per effettuare una scansione delle porte Nmap su un computer collegato a una rete domestica locale, scarica e avvia un programma come Zenmap, indica l'indirizzo IP di destinazione del computer che si intende esaminare, scegliere un profilo di scansione predefinito e, quindi, avviare il procedimento. La scansione Nmap indicherà tutti i servizi in esecuzione (ad esempio i servizi Web, i servizi e-mail ecc.) e i numeri delle porte. In generale, la scansione di una porta restituisce uno dei tre risultati seguenti:

- **Aperta o Accettata** – L'host ha risposto indicando che un servizio è in ascolto sulla porta.

- **Chiusa, Rifiutata o Non in ascolto** – L'host ha risposto indicando che i tentativi di connessione alla porta verranno rifiutati.
- **Filtrata, Interrotta o Bloccata** – Non è stata ricevuta alcuna risposta dall'host.

Per eseguire una scansione delle porte di una rete da una posizione esterna, devi avviare il procedimento dall'esterno. Questo significa condurre una scansione delle porte Nmap nei confronti del tuo firewall o dell'indirizzo IP pubblico del tuo router. Per determinare il tuo indirizzo IP pubblico, usa un motore di ricerca come Google e digitare la frase "qual è il mio indirizzo IP". Il motore di ricerca restituisce l'indirizzo IP pubblico.

Per eseguire la scansione di sei porte normalmente utilizzate del tuo router o firewall, accedi allo strumento Nmap Online Port Scanner all'indirizzo https://hackertarget.com/nmap-online-port-scanner/, Inserisci l'indirizzo IP pubblico nella casella*IP address to scan… (indirizzo IP da analizzare)*, quindi fai clic su *Quick Nmap Scan (scansione rapida Nmap)*. Se la risposta è *aperto* per uno o più delle porte 21, 22, 25, 80, 443 o 3389, molto probabilmente nel router o nel firewall è stato attivato il port forwarding e, nella rete privata, sono in esecuzione server, come mostrato nella figura.



Appliance di sicurezza

Attualmente, nessuna appliance di sicurezza o apparato tecnologico è in grado di soddisfare, da solo, tutte le necessità in fatto di sicurezza della rete. Poiché è necessario implementare un'ampia gamma di appliance e strumenti per la sicurezza, è fondamentale che essi funzionino insieme. Le appliance di sicurezza si dimostrano maggiormente efficaci quando fanno parte di un sistema.

Le appliance di sicurezza possono essere costituite da dispositivi autonomi, come i router e i firewall, schede installate all'interno di dispositivi di rete oppure da moduli dotati di processore e

memoria cache propri. Le appliance di sicurezza possono anche essere costituite da strumenti software eseguiti all'interno di dispositivi di rete. Le appliance di sicurezza si suddividono nelle seguenti categorie generali:

Rilevamento degli attacchi in tempo reale

Il software non è perfetto. Quando un hacker sfrutta un errore contenuto in un software prima che il creatore di quest'ultimo possa porvi rimedio, si è in presenza di un attacco zero-day. Considerato il livello di sofisticatezza e la portata degli attacchi zero-day attualmente rilevati, accade spesso che gli attacchi alle reti abbiano successo e che, adesso, la bontà delle misure di difesa sia misurata in base alla velocità con cui una rete riesce a reagire a un attacco. La capacità di rilevare gli attacchi non appena essi vengono sferrati, ossia in tempo reale, unita a quella di fermarli immediatamente, o almeno entro pochi minuti rappresenta l'obiettivo ideale. Purtroppo, attualmente molte aziende non sono in grado di rilevare gli attacchi, se non giorni o addirittura mesi dopo che essi si sono verificati.

- **Scansione in tempo reale dalla periferia all'endpoint** - il rilevamento degli attacchi in tempo reale richiede l'esecuzione di scansioni per mezzo di firewall e di dispositivi di rete IDS/IPS. Inoltre, è necessario avvalersi anche di strumenti di rilevamento di malware client/server di nuova generazione dotati di collegamenti con centri globali per lo studio delle minacce. Attualmente, i dispositivi e il software per la scansione attiva individuano le anomalie di rete utilizzando l'analisi basata sui contesti e il rilevamento dei comportamenti.
- **Attacchi DDoS e risposta in tempo reale** - il DDoS è una delle principali minacce che richiedono un rilevamento e una risposta in tempo reale. È molto difficile difendersi dagli attacchi DDoS, poiché questi ultimi hanno origine da centinaia, se non migliaia, di host zombie e assumono l'apparenza di traffico legittimo, come mostrato nella figura. Per molte aziende, gli attacchi DDoS periodici compromettono i server Internet e la disponibilità della rete. La capacità di rilevare gli attacchi DDoS e reagire in tempo reale è fondamentale.

Proteggersi dal malware

In che modo ti difendi dalla presenza costante di attacco zero-day nonché dalle minacce avanzate persistenti (APT, Advanced Persistent Threat) che rubano dati per lunghi periodi di tempo? Una soluzione consiste nell'utilizzo, a livello aziendale, di una soluzione per il rilevamento del malware avanzato in grado di agire in tempo reale.

Gli amministratori di rete devono monitorare costantemente la rete alla ricerca di indizi di malware o di comportamenti che rivelino la presenza di un'APT. Cisco ha messo a punto AMP Threat Grid che analizza milioni di file e li associa a centinaia di milioni di altri artefatti malware analizzati, fornendo una visione globale degli attacchi, delle campagne e della distribuzione del malware. AMP è un software client/server implementato negli endpoint host, come i server standalone o in altri dispositivi di sicurezza di rete. La figura mostra i vantaggi dell'AMP Threat Grid.

Best-practice per la sicurezza

Molte associazioni nazionali e professionali hanno pubblicato elenchi di best-practice per la sicurezza. Di seguito viene riportato l'elenco di alcune di esse:

- **Eseguire la valutazione dei rischi** – conoscere il valore di ciò che si sta proteggendo aiuta a giustificare le spese in materia di sicurezza.

- **Creare una policy di sicurezza** – creare una policy che definisca chiaramente regole aziendali, mansioni e aspettative.
- **Misure per la sicurezza fisica** – limitare l'accesso agli armadi di rete, ai luoghi dove si trovano i server nonché ai dispositivi antincendio.
- **Misure di sicurezza nei confronti delle risorse umane** – è necessario condurre ricerche adeguate sul dipendenti e prevedere un controllo del background di ciascuno..
- **Eseguire e testare i backup** – eseguire backup periodici e verificare che essi consentano il recupero dei dati.
- **Mantenere patch e aggiornamenti per la sicurezza** – aggiornare periodicamente sistemi operativi e programmi a bordo di server, client e dispositivo di rete.
- **Attuare il controllo degli accessi** – configurare ruoli e livelli di privilegi diversificati in base agli utenti e utilizzare sistemi di autenticazione forte.
- **Verificare periodicamente la capacità di reazione agli incidenti** – costituire un team per la reazione agli incidenti ed eseguire test sulla risposta in caso di emergenza nel caso di diversi scenari.
- **Implementare uno strumento per il monitoraggio, l'analisi e la gestione della rete** - scegliere una soluzione per il monitoraggio di sicurezza che si integri con altre tecnologie.
- **Implementare dispositivi per la sicurezza di rete** – usare router, firewall e altre appliance di sicurezza di nuova generazione.
- **Implementare una soluzione completa per la sicurezza degli endpoint** – usare software antimalware e antivirus a livello aziendale.
- **Educare gli utenti** – educare utenti e dipendenti ad adottare procedure di sicurezza.
- **Crittografare i dati** – crittografare tutti i dati aziendali sensibili, comprese le e-mail.

Alcune delle linee guida più utili si trovano in repository organizzativi quali il NIST (National Institute of Standards and Technology) e il CSRC (Computer Security Resource Center), come mostrato nella figura.

Una delle organizzazioni più conosciute e rispettate nell'ambito della formazione in materia di cybersecurity è l'istituto SANS. Vai qui per ulteriori informazioni sul SANS e sulle opportunità di formazione e certificazione che offre.

Botnet

I botnet sono gruppi di bot, collegati attraverso Internet, controllati da persone o gruppi malintenzionati. In genere, i computer bot vengono infettati quando gli utenti visitano siti Web, aprono allegati alle e-mail o, anche, file multimediali infetti.

I botnet possono essere costituiti da decine, o anche centinaia, di migliaia di bot. Questi bot possono essere attivati per distribuire malware, lanciare attacchi DDoS, diffondere e-mail di spam o eseguire attacchi brute-force per la violazione delle password. I botnet sono generalmente controllati per mezzo di un server di comando e controllo.

I criminali informatici spesso affittano i botnet a terzi per scopi illegittimi, ricevendo in cambio un canone.

La figura mostra in che modo sia possibile usare i filtri del traffico botnet per comunicare alle community di tutto il mondo che si occupano di sicurezza l'ubicazione dei botnet stessi.

La kill chain nella cyberdifesa

Nell'ambito della cybersecurity, la kill chain descrive le fasi di un attacco ai sistemi informatici. Sviluppata da Lockheed Martin come infrastruttura di sicurezza per il rilevamento e la reazione agli incidenti, la kill chain informatica è costituita dalle fasi seguenti:

Fase 1. Ricognizione - gli hacker raccolgono informazioni sull'obiettivo.

Fase 2. Adescamento - gli hacker creano un payload dannoso di tipo exploit da inviare all'obiettivo.

Fase 3. Dirottamento - gli hacker inviano il payload dannoso di tipo exploit all'obiettivo per mezzo di e-mail o altri metodi.

Fase 4. Exploit - l'exploit viene eseguito.

Fase 5. Installazione - il malware e le backdoor vengono installate all'interno dell'obiettivo.

Fase 6. Comando e controllo - il controllo remoto dell'obiettivo viene assunto per mezzo di un canale o di un server di comando e controllo.

Fase 7. Azione - gli hacker eseguono azioni dannose quali il furto di informazioni oppure sferrano, dall'interno della rete, ulteriori attacchi nei confronti di altri dispositivi attuando nuovamente le fasi della kill chain.

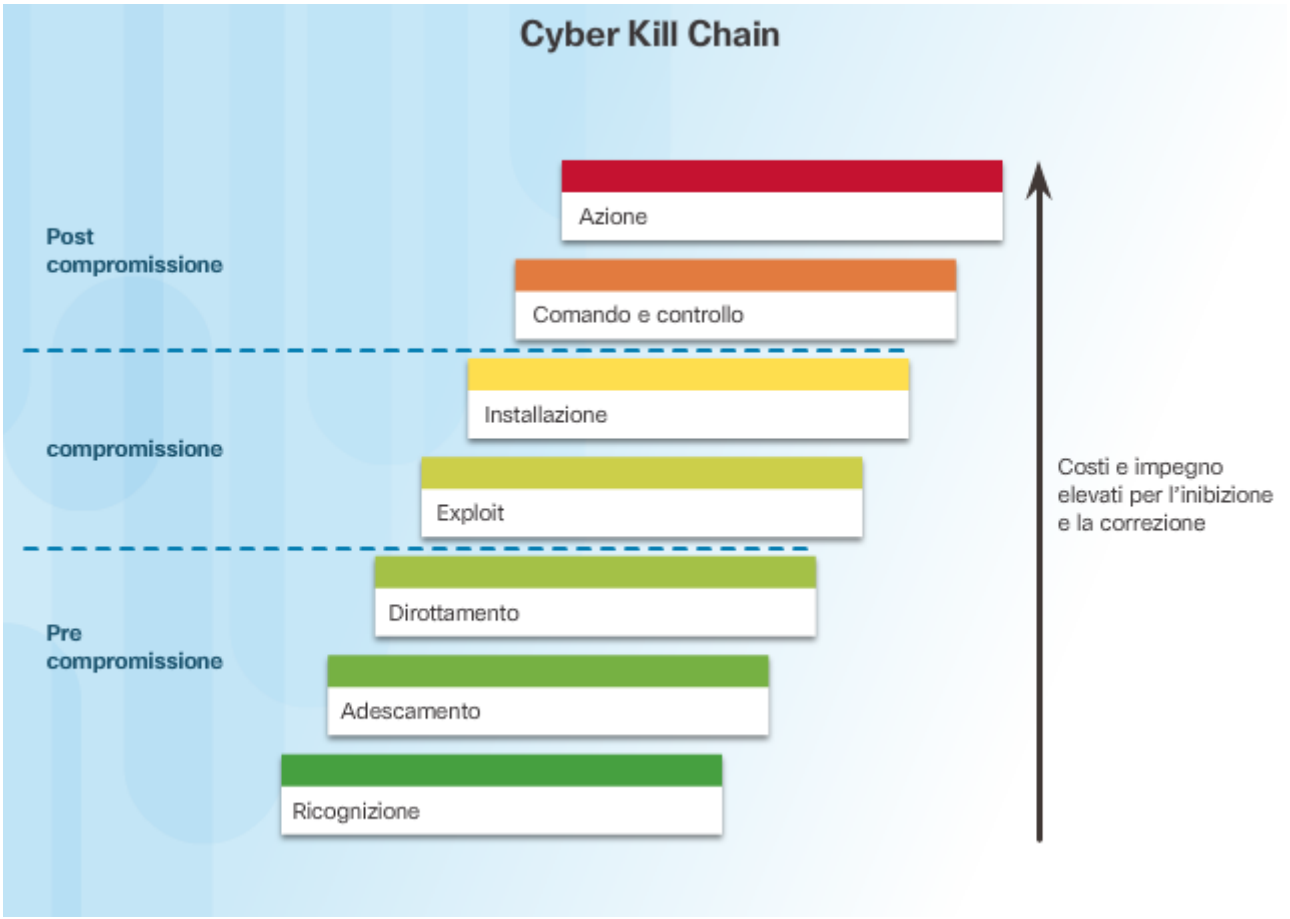
Per proteggersi dalle kill chain, le difese deputate alla sicurezza delle reti sono progettate in base alle fasi che le costituiscono. Di seguito vengono riportate domande relative alle difese aziendali che traggono spunto dalla modalità di funzionamento delle kill chain informatiche:

• Quali sono i segnali di un attacco in corso in ciascuna fase della kill chain?

• Quali strumenti di sicurezza sono necessari per rilevare i segnali di attacco in ciascuna delle fasi?

• Vi sono lacune nella capacità dell'azienda di rilevare un attacco?

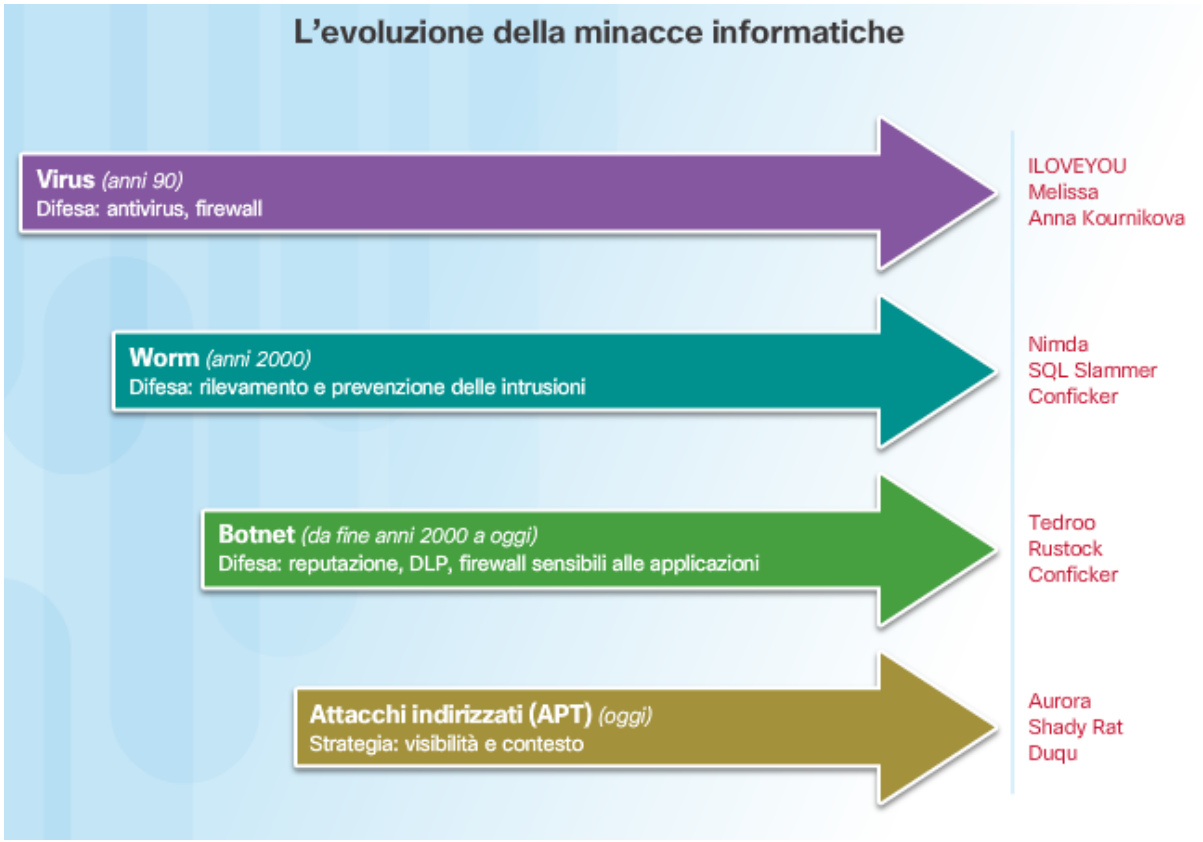
Secondo Lockheed Martin, comprendere le fasi della kill chain ha consentito all'azienda di predisporre ostacoli a difesa della struttura, rallentare gli attacchi e, in ultima analisi, impedire la perdita dei dati. La figura mostra in che modo ciascuna fase della kill chain comporti un aumento dello sforzo e dei costi necessari per impedire e rimediare agli attacchi.



Sicurezza basata sui comportamenti

La sicurezza basata sui comportamenti è una forma di rilevamento delle minacce che non si affida a firme note, ma sfrutta il contesto informativo per rilevare eventuali anomalie di rete. Il rilevamento basato sui comportamenti comporta l'acquisizione e l'analisi del flusso di comunicazioni tra un utente di una rete locale e una destinazione, locale o remota. Queste comunicazioni, una volta acquisite e analizzate, rivelano contesti e modelli di comportamento che possono essere utilizzati per rilevare eventuali anomalie. Il rilevamento basato sui comportamenti può portare alla scoperta di un attacco, grazie allo scostamento da un comportamento normale.

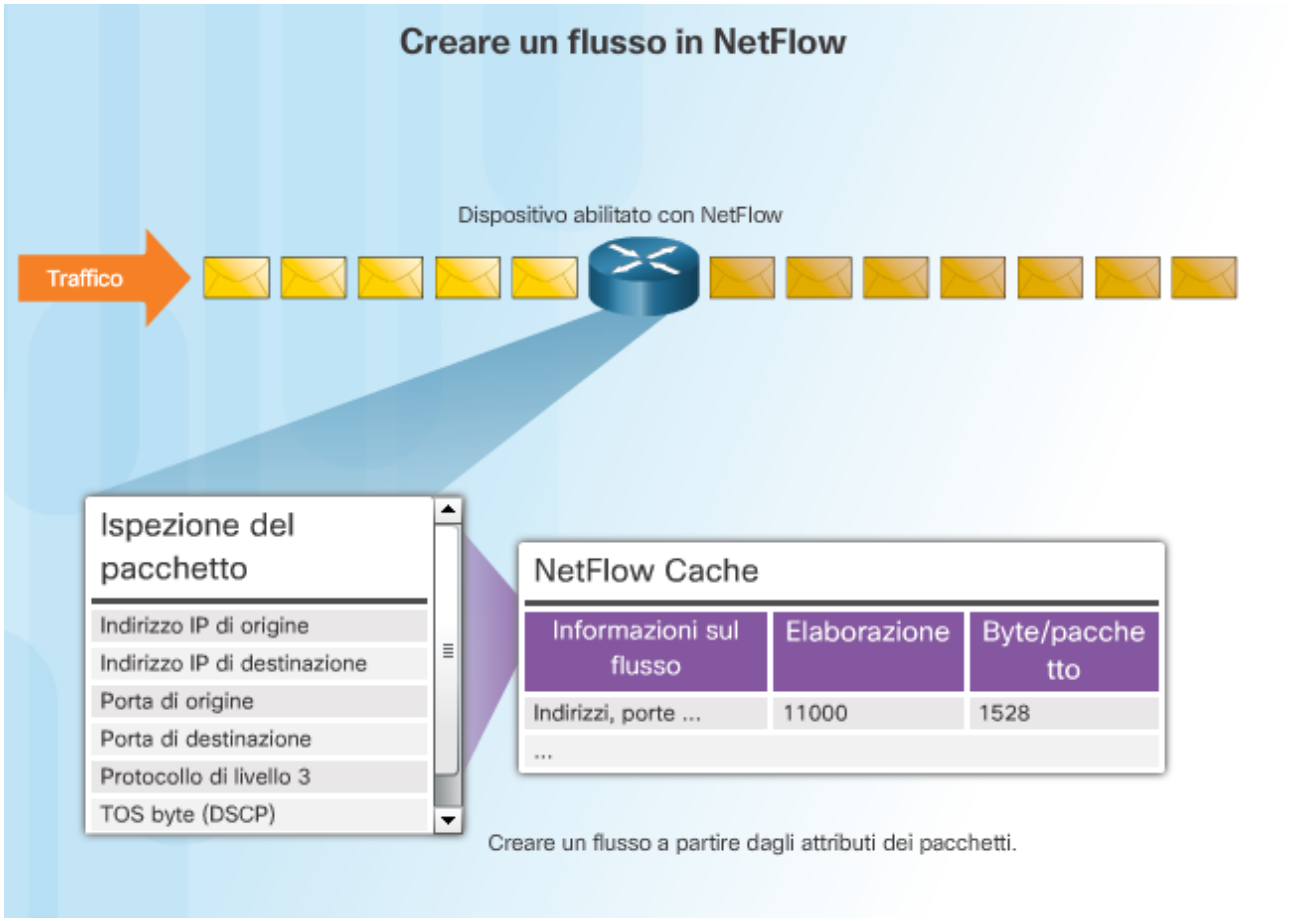
- **Honeypot** - gli honeypot sono strumenti di rilevamento basati sui comportamenti che attirano gli hacker facendo leva sui loro schemi di comportamento dannoso. Quando gli hacker sono all'interno dell'honeypot, gli amministratori di rete possono acquisire, registrare e analizzare il loro comportamento. Questo consente agli amministratori di ampliare le proprie conoscenze e, quindi, mettere a punto meccanismi di difesa migliori.
- **Cisco Cyber Threat Defense Solution Architecture (architettura delle soluzioni Cisco Cyber Threat Defense)** - si tratta di un'architettura di sicurezza che impiega il rilevamento basato sui comportamenti e gli indicatori per fornire maggiore visibilità, contesto e controllo. In caso di attacco, l'obiettivo è conoscere "chi", "cosa", "dove", "quando" e "in che modo". Per realizzare tale obiettivo, questa architettura impiega numerose tecnologie per la sicurezza.



NetFlow

La tecnologia Cisco NetFlow viene impiegata per raccogliere informazioni sul flusso dei dati all'interno delle reti. Le informazioni fornite da NetFlow possono essere paragonate alla bolletta telefonica per il traffico di rete. Esse mostrano chi e quali dispositivi si trovano nella rete nonché quando e in che modo utenti e dispositivi hanno avuto accesso alla rete. NetFlow è un componente importante nel rilevamento e nell'analisi basati sui comportamenti. Gli switch, i router e i firewall di Cisco dotati di NetFlow possono fornire informazioni sui dati in ingresso, in uscita e in transito nella rete. Le informazioni vengono trasmesse ai collettori NetFlow che raccolgono, archiviano e analizzano i record.

NetFlow è in grado di ricavare informazioni sull'uso a partire da numerose caratteristiche diverse relative al modo in cui i dati transitano nelle reti, come mostrato in figura. Grazie alla raccolta di informazioni sui flussi dei dati di rete, NetFlow è in grado di determinare comportamenti di riferimento basati su oltre 90 attributi diversi.



CSIRT

Molte grandi aziende dispongono di un gruppo CSIRT (Computer Security Incident Response Team) preposto alla ricezione, analisi e reazione agli incidenti in materia di sicurezza informatica, come mostrato nella Figura 1. L'obiettivo principale del CSIRT è garantire la conservazione dell’azienda, dei sistemi e dei dati tramite indagini esaustive delle violazioni di sicurezza. Per prevenire gli incidenti di sicurezza, il CSIRT Cisco effettua una valutazione proattiva delle minacce, pianifica la riduzione del rischio, analizza le tendenze mostrate dalle violazioni ed esamina l'architettura di sicurezza, come mostrato nella Figura 2.

Il CSIRT Cisco collabora con il FIRST (Forum of Incident Response and Security Teams), il NSIE (National Safety Information Exchange), il DSIE (Defense Security Information Exchange) e il DNS-OARC (Operations Analysis and Research Center).

Esistono entità CSIRT nazionali e pubbliche, come la divisione CERT del Software Engineering Institute della Carnegie Mellon University disponibili a collaborare con aziende e CSIRT nazionali a sviluppare, utilizzare e migliorare le rispettive capacità di gestione degli incidenti.

Manuale della sicurezza

La tecnologia cambia costantemente. Questo significa che anche gli attacchi informatici si evolvono. Nuove vulnerabilità e metodi di attacco vengono scoperti continuamente. La sicurezza sta diventando una preoccupazione aziendale significativa, a causa dell'impatto in termini finanziari e di reputazione delle violazioni della sicurezza. Gli attacchi hanno per obiettivo reti di importanza critica e dati sensibili. È necessario che le aziende mettano a punto piani per prepararsi, gestire e rimediare alle violazioni.

Uno dei modi migliori per prepararsi a una violazione della sicurezza è impedirla. È necessario disporre di linee guida per l'identificazione dei rischi di cybersecurity relativi a sistemi, risorse, dati e funzionalità, la protezione dei sistemi tramite l'implementazione di dispositivi di sicurezza e la formazione del personale e il rilevamento tempestivo degli eventi di cybersecurity. Quando viene rilevata una violazione della sicurezza, è indispensabile intraprendere azioni adeguate per minimizzarne l'impatto e i danni. Il piano di reazione deve essere flessibile e deve prevedere varie possibili azioni da porre in essere durante la violazione. Una volta contenuta la violazione e ripristinati i sistemi e i servizi violati, è necessario aggiornare le misure e i processi di sicurezza in modo da tenere conto delle lezioni apprese durante l'incidente.

Tutte queste informazioni devono essere registrate nel manuale per la sicurezza. Il manuale per la sicurezza contiene una raccolta di interrogazioni (report) ripetibili relative a origini dati relativi a eventi di sicurezza che conducono al rilevamento degli incidenti e alla reazione a questi ultimi. Idealmente, il manuale per la sicurezza deve adempiere ai seguenti compiti:

- Rilevare i computer infettati da malware.
- Rilevare attività di rete sospette.
- Rilevare tentativi di autenticazione irregolari.
- Descrivere e illustrare il traffico in ingresso e in uscita.
- Fornire informazioni di riepilogo su tendenze, statistiche e conteggi.
- Garantire modalità di accesso rapide e fruibili a statistiche e metriche.
- Correlare gli eventi per tutte le origini dati interessate.

Strumenti per la prevenzione e il rilevamento degli incidenti

Ecco alcuni degli strumenti utilizzati per rilevare e prevenire gli incidenti di sicurezza.

- **SIEM** – i sistemi SIEM (Security Information and Event Management, gestione di eventi e informazioni sulla sicurezza) sono costituiti da software che raccoglie e analizza gli allarmi relativi alla sicurezza, i log e altri dati cronologici e in tempo reale provenienti dai dispositivi di sicurezza presenti nella rete.
- **DLP** – i sistemi DLP (Data Loss Prevention) sono elementi software o hardware progettati per impedire il furto o la fuoriuscita di dati sensibili dalle reti. I sistemi DLP possono concentrarsi sull'autorizzazione all'accesso ai file, lo scambio o la copia di dati, il monitoraggio delle attività degli utenti e molto altro. I sistemi DLP sono progettati per monitorare e proteggere dati che presentino tre stati diversi: dati in uso, dati in movimento e dati a riposo. I dati in uso sono principalmente riferiti ai client; i dati in movimento sono quelli che si muovono attraverso la rete e i dati a riposo sono riferiti all'archiviazione dei dati.
- **Cisco ISE e TrustSec** – gli strumenti Cisco ISE (Identity Services Engine) e Cisco TrustSec intervengono sull'accesso alle risorse di rete creando policy che segmentano l'accesso stesso in categorie (ospiti, utenti mobili, dipendenti) senza aggiungere complessità. La classificazione del traffico si basa sull'identità degli utenti o dei dispositivi. Per ulteriori informazioni su ISE, fai clic su Play nella figura.
- Fare clic su qui per leggere la trascrizione di questo video.

IDS e IPS

Il sistema di rilevazione delle intrusioni (IDS, Intrusion Detection System), mostrato nella figura, può essere realizzato attraverso un dispositivo di rete dedicato oppure impiegando uno dei molti strumenti disponibili all'interno di server e firewall che analizzano i dati confrontandoli con un database di regole o di firme di attacchi alla ricerca di traffico dannoso. Se viene rilevata una corrispondenza, l'IDS registra il rilevamento e crea un avviso destinato all'amministratore di rete. Quando viene rilevata una corrispondenza, il Sistema di rilevazione delle intrusioni non esegue alcuna azione e, pertanto, non impedisce il verificarsi degli attacchi. Il compito dell'IDS consiste unicamente nel rilevare, registrare e riferire.

La scansione effettuata dall'IDS rallenta la rete (dando origine a un fenomeno noto come latenza). Per impedire ritardi nel funzionamento della rete, gli IDS normalmente vengono posizionati offline, separati dal normale traffico di rete. Viene eseguita la copia o il mirroring dei dati da parte di uno switch che, in seguito, li inoltra all'IDS per il rilevamento offline. Vi sono anche strumenti IDS che possono essere installati nell'ambito del sistema operativo di un computer host come Linux o Windows.

I sistemi di prevenzione delle intrusioni (IPS, Intrusion Prevention System) sono in grado di bloccare o rifiutare traffico in base a regole positive o in caso di corrispondenza della firma. Uno dei sistemi IPS/IDS più conosciuti è Snort, la cui versione commerciale è Cisco Sourcefire. Sourcefire è in grado di eseguire l'analisi in tempo reale di traffico e porte, registrazioni, ricerca e analisi della corrispondenza dei contenuti; inoltre, può rilevare tentativi di verifica, attacchi e operazioni di scansione delle porte. Inoltre, esso si integra all'interno di strumenti di terze parti per la creazione di report e analisi di prestazioni e log.