CyberSecurity

- Apprendere i fondamenti di un comportamento online sicuro.
- Conoscere i vari tipi di malware e di attacchi e in che modo le aziende si stanno proteggendo.
- Prendere in esame varie opportunità di carriera nella cybersecurity.

Dopo la lettura sarai più consapevole dell'importanza di un comportamento sicuro online, delle potenziali conseguenze degli attacchi informatici e delle possibili opzioni di carriera nella cybersecurity.

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

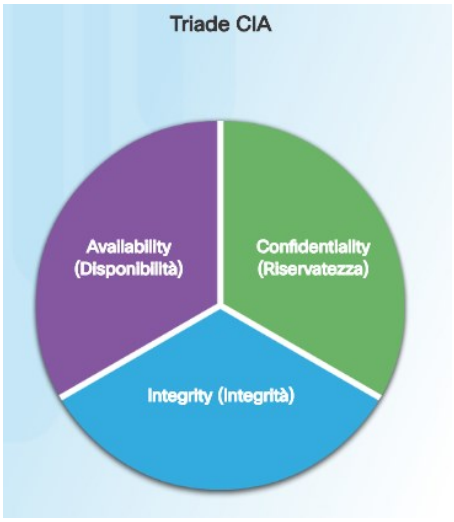
Dati tradizionali

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.

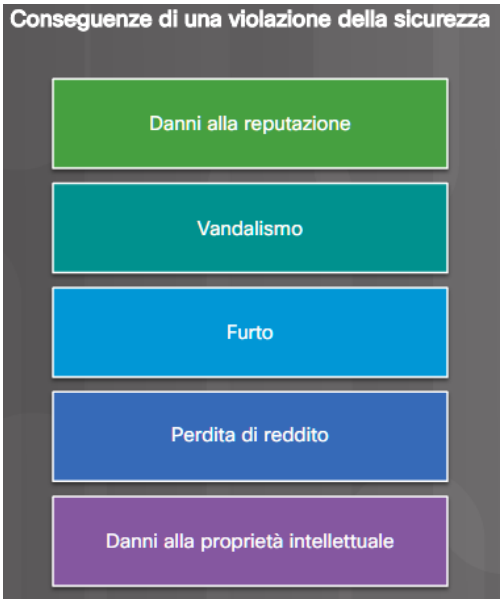
La checksum viene usata per verificare l'integrità dei file o delle stringhe di caratteri dopo il trasferimento da un dispositivo a un altro sulla rete locale o via Internet. Le checksum sono calcolate con le funzioni hash. Alcune della checksum comuni sono MD5, SHA-1, SHA-256 e SHA-512. Una funzione 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.

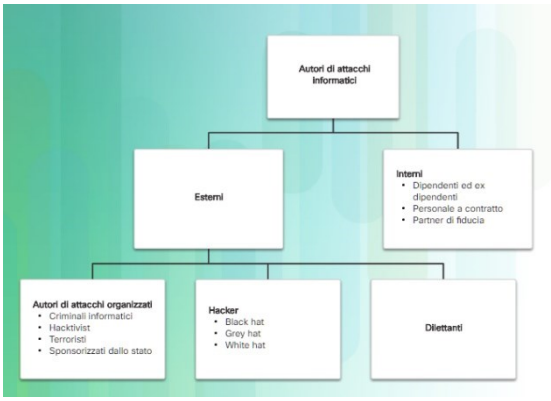
Hacker: questo gruppo di autori degli attacchi viola computer e reti per ottenere l'accesso. A seconda delle intenzioni della violazione, questi autori degli attacchi sono classificati come white, gray o black hat. Gli hacker white hat violano reti o sistemi informatici per scoprirne le debolezze e poter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

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 e 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.

Problemi etici aziendali

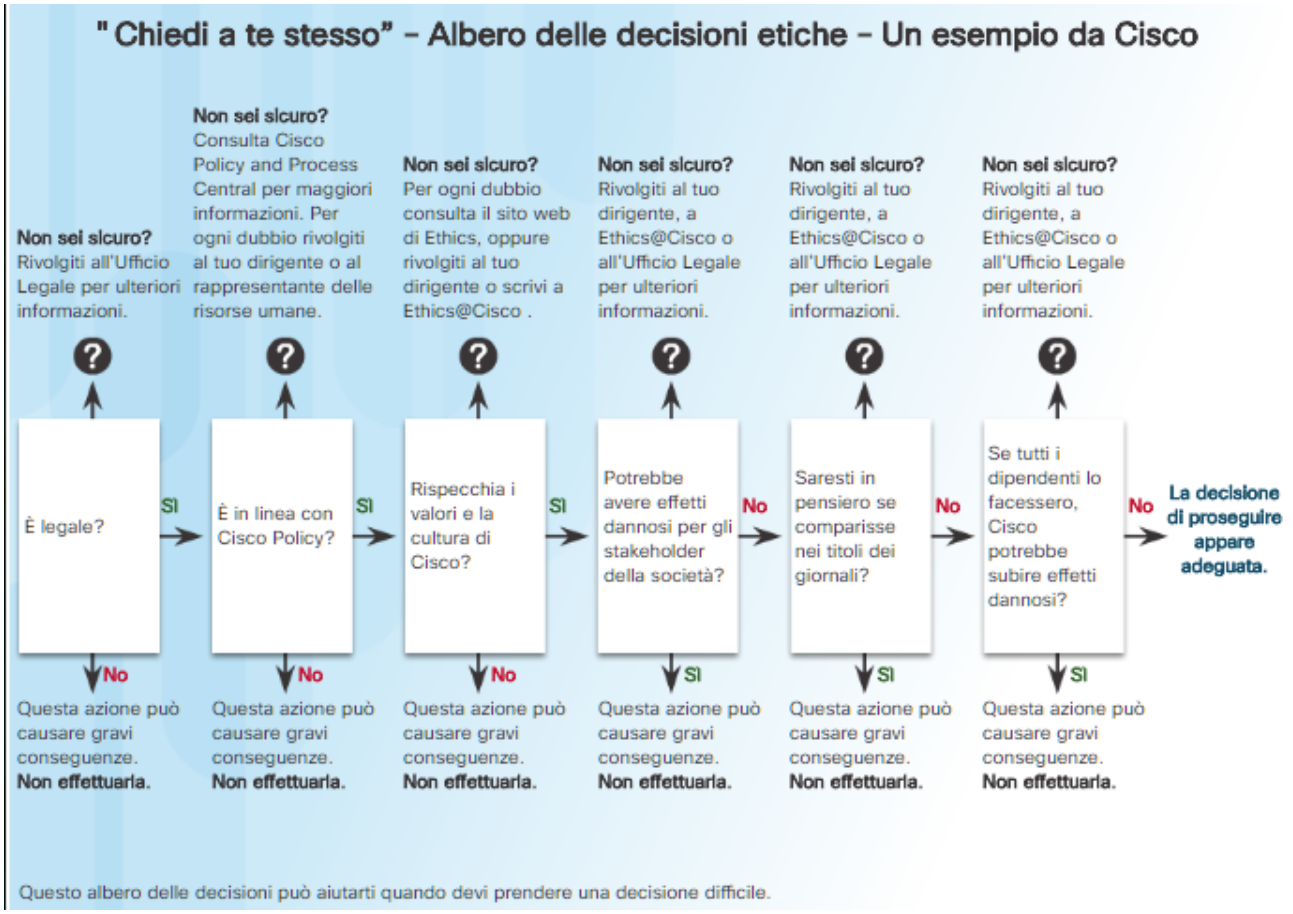
L'etica consiste in codici e comportamenti talvolta imposti per legge. Esistono molte aree della cybersecurity non coperte dalla legge. Ciò significa che qualcosa di tecnicamente legale potrebbe non essere etico. Dato che così tante aree della cybersecurity non sono coperte dalle leggi (o non ancora), molte aziende di professionisti informatici hanno creato codici di etica per le persone del settore. Segue un elenco di tre aziende con codici di etica:

- Il CyberSecurity Institute (CSI) ha pubblicato un codice etico consultabile qui.
- L'Information Systems Security Association (ISSA) ha un codice etico disponibile qui.
- L'Information Systems Security Association (ISSA) ha un codice etico e uno standard di condotta disponibile qui.

Cisco ha un team dedicato esclusivamente alla condotta etica degli affari. Vai qui per maggiori informazioni.
Questo sito contiene un eBook sul Codice di condotta aziendale di Cisco e un file pdf. In entrambi i file è incluso un "Ethics Decision Tree" (albero delle decisioni etiche) come mostrato nella figura. Anche se non lavori per Cisco, le domande e le risposte riportate in questo albero decisionale possono facilmente essere applicate al tuo posto di lavoro.

Come per le questioni legali, in generale, se hai dubbi sull'eticità di un'azione o un comportamento, presupponi che non sia etico e non procedere. Forse nel reparto delle risorse umane o nell'ufficio legale della tua azienda puoi trovare qualcuno in grado di chiarire la tua situazione prima che tu agisca in un modo considerato non etico.

Eseguendo una ricerca online troverai altre aziende con codici di etica. Prova a identificare i punti comuni.



Attività – Identificare il colore del cappello (hat)

Caratteristiche dell'hacker	White Hat	Grey Hat	Black Hat
Dopo aver piratato dei bancomat da remoto con un portatile, ha aiutato il produttore del sistema a risolvere le vulnerabilità.			
Dal mio portatile ho trasferito 10 milioni di dollari sul mio conto bancario usando i dati e i PIN del conto delle vittime, che ho registrato mentre immettevano il codice.			
Il mio lavoro è individuare le debolezze nei sistemi informatici dell'azienda.			
Usando dei malware sono riuscito a compromettere diversi sistemi aziendali, per sottrarre i dati delle carte di credito e rivendere queste informazioni al migliore offerente.			
Mentre stavo cercavo gli exploit della sicurezza, mi sono imbattuto in una vulnerabilità della sicurezza su una rete aziendale a cui sono autorizzato ad accedere.			
Collaboro con aziende del settore tecnologie per risolvere un errore con DNS.			

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.

Il bisogno di cybersecurity

Sono state spiegate le funzionalità e le caratteristiche della cybersecurity. Sono stati inoltre illustrati i motivi per cui la domanda di professionisti della cybersecurity continuerà a crescere. Nel contenuto sono stati spiegati i motivi che rendono l'identità e i dati online vulnerabili agli attacchi dei criminali informatici. Sono stati offerti alcuni suggerimenti su come proteggere l'identità e i dati online personali.

Sono stati inoltre trattati i dati aziendali: cosa sono, dove sono e i motivi per cui devono essere protetti. Sono stati descritti gli autori di attacchi informatici e cosa vogliono. I professionisti della cybersecurity devono avere le stesse competenze degli autori degli attacchi. I professionisti della cybersecurity devono rispettare le leggi locali, nazionali e internazionali. I professionisti della cybersecurity devono anche utilizzare le loro capacità in modo etico.

Infine é stata trattata brevemente la guerra cibernetica e i motivi per cui nazioni e governi necessitano di professionisti della cybersecurity per aiutare a proteggere cittadini e infrastrutture.