Capitolo 1

Questa cosa che chiamiamo sicurezza informatica

E così volete aiutare a proteggere questo nuovo mondo digitale in cui viviamo, gettandovi in una carriera nel campo della sicurezza informatica. Se avete studiato qualcosa su come dare avvio a una carriera in un qualsiasi settore legato alla cyber security, probabilmente avrete sentito e letto molte discussioni sul gap da colmare in termini di competenze nel campo della sicurezza informatica. Forse avrete anche letto studi che ventilano la possibilità che potrebbero essere necessari fino a quattro milioni di posti di lavoro nel campo della sicurezza informatica. Tuttavia, se state cercando il vostro primo impiego, probabilmente siete in cerca di lavoro da più di sei mesi.

Se siete prossimi alla laurea o state cercando di cambiare carriera, probabilmente vi sarete chiesti: "Come faccio a iniziare a lavorare nel campo della sicurezza informatica?". Sfortunatamente, se avete affrontato quella domanda, probabilmente avrete scoperto che non esiste un'unica risposta, universalmente accettata.

In qualità di professionista della sicurezza informatica, con oltre quindici anni di esperienza, ho assunto alcune persone di grande talento al loro primo impiego. Ho visto sbocciare i team che ho costruito: dalle loro origini si sono trasformati in team sempre più efficaci. Eppure, nonostante tutto il successo che ho riscontrato nell'assunzione e nello sviluppo di talenti, ho anche visto la community della sicurezza faticare a definire un percorso di carriera preciso, dal livello base ai ruoli avanzati. Ho assistito al peggio, nei

In questo capitolo

- **Che cos'è la sicurezza informatica**
- **Il ruolo della sicurezza informatica**
- **La cultura della sicurezza informatica**
- **Il "settore" della cyber security**
- **Il valore della diversità umana nel campo della sicurezza informatica**
- **Riepilogo**

processi di assunzione: cattivi consigli elargiti ai principianti e veri e propri respingimenti da parte dei professionisti di lunga data.
Ma avete acquistato una copia di questo libro. Nelle prossime pagine, vi aiuterò a comprendere la natura unica di ciò che viene comunemente definito *settore della sicurezza informatica*. Vi accompagnerò in un percorso che inizia definendo il campo di cui state cercando di entrare a far parte. Userò interviste con vari membri della community della sicurezza informatica per dimostrare come anche competenze e background apparentemente disparati possano rappresentare una risorsa per una carriera nel settore della cyber security. Sfrutterò i sondaggi che ho condotto fra oltre 1.500 professionisti della sicurezza informatica e aspiranti professionisti per analizzare i percorsi che potete seguire per accelerare la vostra transizione verso un lavoro nel campo della cyber security.
Nel corso di questo libro, analizzerò il valore dell'istruzione, della formazione, delle certificazioni e dei mentoring nell'ottenere un lavoro. Condividerò approfondimenti utili per interpretare gli annunci di lavoro per le posizioni di sicurezza e per analizzare e ottimizzare la vostra specifica esperienza, per posizionarvi al meglio con lo scopo di essere assunti in quel vostro primo impiego. Vi darò un'idea dei tipi di interviste che vengono generalmente condotte nel processo di assunzione e condividerò tecniche utili per massimizzare le vostre prestazioni. Vi propongo anche i miei suggerimenti per garantire il vostro successo nel percorso di carriera che avete scelto, dopo aver ottenuto il vostro primo lavoro.
Il primo passo nel processo per ottenere quel lavoro nel campo della sicurezza informatica è capire che cos'è la sicurezza informatica, quali sono le professionalità disponibili nel campo della sicurezza informatica e il loro impatto nei diversi contesti della nostra vita quotidiana.

Che cos'è la sicurezza informatica

Cyber security è un termine ormai onnipresente nella società moderna. Dai mezzi di informazione, alla politica, al mondo aziendale, la *sicurezza informatica* è un argomento che emerge quotidianamente nella vita della maggior parte delle persone. Per tutta questa discussione, tuttavia, può essere abbastanza difficile trovare una risposta definitiva a una domanda apparentemente semplice: che cos'è la sicurezza informatica?
Non esiste un'unica definizione universalmente accettata. La maggior parte sarà d'accordo, tuttavia, sul fatto che la sicurezza informatica è un'estensione di quella che spesso viene ancora definita sicurezza delle informazioni. Nel 1961, i ricercatori del MIT (*Massachusetts Institute of Technology*) hanno creato il primo sistema protetto da password, noto come CTSS (*Compatible Time Sharing System*). Per molti, questo è considerato l'atto di nascita della *sicurezza delle informazioni*, che consiste nella pratica di proteggere da accessi non autorizzati le informazioni e i sistemi elettronici che le elaborano.
Avanzando rapidamente di circa un decennio da quei primi giorni, i ricercatori stavano iniziando a collegare più reti di computer all'ARPANET (*Advanced Research Projects Agency Network*). Questa rete è stata progettata per consentire a più reti di computer, distribuite su vaste aree geografiche, di comunicare e condividere dati in modo rapido e affidabile. ARPANET, a quanto pare, fu l'inizio di ciò che oggi chiamiamo Internet.
Nel 1988, tuttavia, tre anni prima che la rete Internet fosse resa disponibile al pubblico, il ricercatore Robert Morris voleva evidenziare i rischi per la sicurezza dei computer

connessi a Internet. Ha progettato un software che si è poi diffuso nei sistemi di calcolo connessi. Il software sfruttava alcune falle della sicurezza del sistema operativo UNIX per installarsi e replicarsi, continuamente. A tutti gli effetti, Morris aveva creato il primo *worm* per Internet. Sfortunatamente per Morris, il worm si è diffuso in modo incontrollabile e ha reso inutilizzabili i sistemi infetti. Ciò non solo ha portato Morris a essere la prima persona condannata per un reato ai sensi del *Computer Fraud and Abuse Act* del 1986, ma ha anche portato alla creazione del CERT (*Computer Emergency Response Team*) presso la Carnegie Mellon University, con il finanziamento diretto del governo degli Stati Uniti. La creazione del CERT può essere considerata come la nascita di quella che oggi chiamiamo *cyber security*. Pertanto, una definizione operativa ragionevole del termine sicurezza informatica è quel dominio della ricerca, delle tecnologie e delle tecniche utilizzate per proteggere i sistemi tecnologici connessi, i dati e le persone da attacchi, usi non autorizzati e/o danni.

Il ruolo della sicurezza informatica

Gli obiettivi della cyber security cambiano significativamente a seconda del contesto in cui viene applicata. Quando nei media si parla di sicurezza informatica, spesso essa viene considerata dal punto di vista della protezione delle imprese e del commercio da criminali informatici e hacker. Tuttavia, quasi altrettanto comuni sono le discussioni su come la sicurezza informatica viene applicata nella società in generale. Dalla protezione del voto, alla sicurezza nazionale/internazionale, alla protezione della privacy individuale online, la sicurezza informatica è il filo conduttore che ha la responsabilità di garantire che tutti gli aspetti della società funzionino senza problemi.
Una solida comprensione della vera ampiezza del mondo della sicurezza informatica deve partire dalla comprensione di come essa si colloca in questi e altri aspetti della nostra vita. La sicurezza informatica è ormai così radicata in tutto ciò che facciamo che spesso può essere data per scontata o del tutto trascurata. Fare un passo indietro ed esaminare in dettaglio alcuni dei diversi modi in cui si fa affidamento sulla sicurezza informatica ci consentirà di affrontare una discussione più concreta quando parleremo delle discipline e dei ruoli lavorativi che attengono a questo dominio.

La sicurezza informatica nel mondo aziendale

Nelle organizzazioni aziendali, l'obiettivo della sicurezza informatica consiste, in genere, nel proteggere gli interessi finanziari dell'azienda. Le aziende operano su un modello di *asset*, elementi dell'azienda che detengono o creano valore finanziario, e passività, elementi che riducono o comportano il rischio di diminuzione del valore finanziario degli asset dell'azienda.
A partire dalla metà del XX secolo, le aziende hanno sempre più adottato la *tecnologia dell'informazione (IT)* per abilitare funzionalità più rapide e avanzate. L'IT consiste nell'uso di sistemi digitali per gestire ed elaborare le risorse informative di un'azienda. Con l'evoluzione dei sistemi IT, e in particolare con gli sviluppi nell'ultimo decennio, sempre più risorse aziendali sono entrate a far parte del dominio digitale.
Per descrivere questo fenomeno, tale per cui le aziende digitalizzano le proprie risorse critiche e si rendono più dipendenti dai sistemi IT, è stato coniato il termine *trasforma-*

zione digitale. Per esempio, le cartelle cliniche, che un tempo erano archiviate in cartelle cartacee e sotto forma di immagini su pellicola fisica, sono state sempre più trasferite su sistemi elettronici. L'archiviazione digitale di tutte queste informazioni semplifica l'accesso, la visualizzazione e la condivisione delle informazioni. In effetti, attorno a questa trasformazione digitale è nato un intero mercato di prodotti e servizi IT, per assistere le aziende che effettuano queste conversioni in quasi tutti i settori, dall'assistenza sanitaria all'istruzione ai trasporti.

Ma, a mano a mano che le aziende trasformano le proprie risorse nella direzione del digitale, aumenta il rischio che i criminali informatici attacchino i sistemi a caccia di tali risorse. Queste minacce di attacco possono variare, da tentativi di furto di dati, a tentativi di rendere inutilizzabili i sistemi. Le risorse informative fisiche, che un tempo erano a basso rischio di attacco, ora, nel nuovo mondo digitale, corrono il rischio di attacchi da parte di entità di tutto il mondo. La connettività e l'immediatezza dell'accesso ai dati e delle interazioni su Internet hanno offerto da un lato una crescita esplosiva delle risorse nel dominio digitale, ma dall'altro hanno anche consentito l'emergere di nuove minacce. Le tecnologie, le tecniche e le risorse di sicurezza informatica sono a loro volta utilizzate per garantire che i rischi rappresentati da tali minacce siano ridotti al minimo. Quindi, l'obiettivo principale della sicurezza informatica all'interno delle aziende diventa la difesa di questo panorama, in continua crescita, di risorse digitali.

Come ho detto, le aziende operano secondo modelli di contenimento del rischio per garantire il proprio successo complessivo. I dirigenti di aziende grandi e piccole valutano sempre i rischi che l'azienda possa essere influenzata negativamente da un evento o da un cambiamento delle condizioni; quindi, cercano di ridurre al minimo i rischi. Per esempio, un'azienda come Facebook potrebbe dover soppesare le potenziali entrate derivanti dalla vendita dei dati degli utenti a un partner rispetto alla potenziale accusa di violazione delle leggi sulla privacy. Inoltre, un'azienda e i suoi dirigenti devono considerare il costo potenziale del fatto che una minaccia sfrutti con successo una risorsa rispetto al costo del contenimento di tale rischio. Si tratta di decisioni complesse che guidano le decisioni finanziarie e altre strategie organizzative. Quindi, poiché le risorse digitali sono sempre più parte di questo panorama, non sorprende che anche la sicurezza informatica sia soggetta a quelle stesse forme di analisi del rischio.

In tal modo, la sicurezza informatica diventa un input cruciale per il processo di contenimento del rischio all'interno di un'azienda. I professionisti della sicurezza informatica sono spesso valutati in base alla loro esperienza nella valutazione del livello di rischio per specifiche risorse aziendali rispetto alle varie minacce che potrebbero prendere di mira tali risorse. Ciò attribuisce responsabilità ai team responsabili della cyber security, che vanno ben oltre le semplici competenze tecnologiche. Chi si occupa della sicurezza deve essere in grado di considerare l'intero panorama delle minacce e comunicare in modo efficace le caratteristiche di tali minacce ad altre aree dell'azienda che non hanno lo stesso livello di competenza tecnica. Noi dobbiamo essere in grado di spiegare agli altri quali sono gli attori delle minacce, in termini di Stati, attivisti, minacce interne e così via: tutti rientrano nel panorama delle minacce. Il personale addetto alla sicurezza deve anche essere in grado di comprendere come si collocano le risorse strategiche a livello dell'intera azienda, per individuare in modo più accurato i rischi che le minacce rappresentano per l'azienda.

Poiché i sistemi IT sono diventati una parte così intrinseca del modello aziendale, è aumentata anche la loro criticità per le aziende. Un guasto a un sistema che lo mette

fuori uso può avere un impatto enorme sull'azienda. Pensate ai grandi rivenditori e quanto costerebbe loro se i loro registratori di cassa rimanessero fuori uso anche solo per mezz'ora. Strutture sanitarie, istituzioni finanziarie, società di logistica e quasi tutti i settori immaginabili sono ormai dipendenti dai sistemi IT per le loro attività di base.
A causa della criticità di questi sistemi, che nella nostra epoca sono sempre interconnessi, in qualche modo, anche la sicurezza informatica gioca un ruolo chiave nel garantire la stabilità e la disponibilità di tali sistemi. Gli hacker che cercano di danneggiare un'azienda potrebbero tentare un attacco DoS (*Denial of Service*), cercando di rendere inaccessibili i sistemi aziendali per un certo arco di tempo. I professionisti della sicurezza informatica hanno il compito di impedire il successo di questi tipi di attacchi, ma questo è solo uno di un lungo elenco di responsabilità.
In genere, questo tipo di approccio difensivo viene svolto insieme a un team che è il principale responsabile del funzionamento quotidiano dei sistemi. Nell'IT, questi team sono generalmente chiamati *team operativi* (*operations team*). Per quanto riguarda la sicurezza informatica, i team che si occupano del funzionamento quotidiano dei sistemi di sicurezza sono chiamati *team operativi di sicurezza* (*security operations team*).

Esempi di responsabilità quotidiane nel campo della sicurezza informatica

Di seguito trovate alcune delle responsabilità tipiche dei professionisti della sicurezza informatica.

- Monitoraggio degli attacchi a vari sistemi.
- Risposta agli attacchi che sono riusciti a violare uno o più sistemi.
- Valutazione dei sistemi e delle persone, alla ricerca dei punti deboli della sicurezza (le *vulnerabilità*).
- Monitoraggio, convalida e report sulla correzione di tali vulnerabilità.
- Collaborazione con gli sviluppatori in termini di tecniche per lo sviluppo di software sicuro.
- Progettazione e implementazione delle misure di sicurezza (i controlli di accesso).
- Collaborazione con i dirigenti esecutivi, per garantire la disponibilità del budget per la cyber security.
- Fornitura delle prove dei controlli di sicurezza per gli auditor.
- Manutenzione dei vari sistemi di sicurezza (account utente, firewall e così via).

Poiché i modelli aziendali sono sempre più fortemente dipendenti dalle risorse digitali e dai sistemi IT, è emersa un'altra tendenza. Il livello delle normative governative e dei requisiti di conformità del settore relativi all'uso dei sistemi IT è cresciuto a un ritmo vertiginoso. Molte di queste normative e standard di conformità includono requisiti dettagliati per il modo in cui le aziende sono tenute a proteggere i propri sistemi, a reagire alle violazioni ed esposizioni di dati e a proteggere la privacy dei loro clienti.
Ancora una volta non sorprende, quindi, che il personale che si occupa della sicurezza informatica all'interno di un'azienda svolga un ruolo importante nel dimostrare come l'azienda raggiunge, mantiene e dimostra la conformità a questi regolamenti e standard. Tanto per cominciare, tale personale è spesso chiamato a studiare e perfino interpretare

l'effettivo significato dei requisiti. Questo compito può essere svolto in collaborazione con altri settori dell'azienda, come il team legale, il team di contenimento dei rischi o il team di audit, ma l'esperienza che la sicurezza può apportare a queste discussioni è fondamentale.
In base a questa interpretazione, è necessaria un'elevata competenza in materia di sicurezza nella progettazione e nell'attuazione dei vari controlli che, in ultima analisi, garantiranno la conformità dell'azienda a tali requisiti. Questi controlli possono assumere la forma di processi, tecniche, politiche e tecnologie tutte intese ad aiutare l'azienda a proteggere in modo adeguato i propri dati e sistemi, in base ai requisiti.
Osservando il ruolo della sicurezza informatica all'interno di un ambiente aziendale, diventa chiaro che il personale addetto alla sicurezza è coinvolto in praticamente ogni aspetto dell'azienda. Mentre, spesso, un tempo i team responsabili della sicurezza delle informazioni potevano concentrarsi esclusivamente sui controlli e sulle contromisure, il moderno mondo digitale costringe la sicurezza a far parte di ogni ambito aziendale.

La sicurezza informatica a difesa della società

Il passaggio dal mondo aziendale alla prospettiva più ampia della società cambia il focus dei professionisti della cyber security. Se da un lato la sicurezza informatica è intrecciata nella conduzione delle attività aziendali, è ugualmente o anche più un elemento chiave della nostra vita quotidiana. Il funzionamento del governo, della sicurezza nazionale, delle forze dell'ordine e delle loro capacità di prevenire i crimini, e perfino le interazioni personali, nel ventunesimo secolo dipendono tutti dal mondo digitale.
Tutti i livelli di governo sono diventati incredibilmente dipendenti dai computer e dalle app mobili, dai dati digitali e da altre funzionalità tecnologiche che attengono tutte al mondo digitale. Se avete qualche dubbio su quanto siano diventati importanti i sistemi IT nel funzionamento quotidiano del governo, considerate anche solo gli attacchi *ransomware*, tramite i quali un software dannoso viene installato su un computer per "tenere in ostaggio" i dati, fino al pagamento di un riscatto.
Uno degli attacchi più importanti contro un governo locale è avvenuto a Baltimora, Maryland, nel maggio del 2019. Parti intere della gestione della città sono state bloccate, alcune per più di un mese, poiché le e-mail, i pagamenti e altri sistemi erano stati messi improvvisamente fuori uso. La perdita in termini di entrate più gli sforzi per il recupero sono costati alla città oltre 18 milioni di dollari. Molti altri governi locali, statali e nazionali in tutto il mondo hanno subito attacchi simili.
Naturalmente, l'operatività quotidiana non è l'unico modo in cui le amministrazioni fanno affidamento sui sistemi IT. Anche l'uso di sistemi elettronici per gestire il voto sta crescendo rapidamente. Il pubblico richiede un accesso sempre più rapido e accurato ai risultati, e così i governi degli Stati Uniti e di tutto il mondo si stanno rivolgendo ai terminali di voto digitale. Tuttavia, sono ben documentate anche le minacce a questi terminali di voto. Problemi di sicurezza e potenziali tentativi di hacking sono stati identificati in varie elezioni passate, in particolare le elezioni presidenziali statunitensi del 2016 e del 2020. In definitiva, il governo statunitense, la CISA (*Cybersecurity and Infrastructure Security Agency*) e varie società di sicurezza indipendenti sono tutte giunte alla conclusione che, grazie agli sforzi dei professionisti della sicurezza informatica, nessun tentativo di hacking di quei sistemi ha avuto successo.

I professionisti e ricercatori nel campo della sicurezza sono regolarmente reclutati dagli enti governativi per la difesa contro gli attacchi. La posta in gioco non potrebbe essere più alta. Quasi nulla, in ambito governativo, può essere considerato "a basso rischio" se viene colpito da un attacco informatico. Anche quando a essere colpiti dall'attacco sono parchi, musei o altri servizi "statali", la reazione negativa del pubblico può essere rapida e potente. Nessun candidato vuole che il proprio nome venga associato a un attacco informatico verificatosi sotto la sua sorveglianza. Di conseguenza, sta crescendo l'esigenza di mettere in campo sforzi concertati, che molti professionisti della sicurezza considererebbero in ritardo, per rafforzare la sicurezza degli enti governativi.
Ma il problema va ben oltre le questioni amministrative. Anche i militari di tutto il mondo sono diventati sempre più dipendenti dai sistemi tecnologici nei loro sforzi per difendere le loro nazioni e quelle dei loro alleati. Tutto, dai veicoli militari alle comunicazioni ai sistemi di monitoraggio, sfrutta livelli crescenti di tecnologie di connettività. Al di là di qualsiasi altra applicazione, la sicurezza informatica nell'operatività delle forze armate è una vera questione di vita o di morte. Con l'introduzione delle nuove tecnologie, sia i governi sia i produttori si rivolgono a ricercatori e professionisti della sicurezza per garantire che tali sistemi siano sufficientemente protetti dagli attacchi, e questo dalla progettazione fino al loro utilizzo sul campo.
Un'estensione naturale dell'uso militare è l'applicazione del rispetto delle leggi a livello nazionale. Dalle pattuglie, alle indagini e alla giustizia penale, i computer e altri dispositivi elettronici connessi svolgono un ruolo chiave. Gli attacchi contro questi sistemi potrebbero avere effetti dannosi sulle forze di polizia e rendere impossibile l'applicazione delle leggi e il perseguimento delle violazioni. Inoltre, data la crescente interconnessione della nostra società, molti crimini vengono commessi utilizzando mezzi elettronici. Avere professionisti della sicurezza qualificati non solo per difendere i sistemi del dipartimento o dell'ente, ma anche per assistere nelle indagini sui crimini diventa pertanto estremamente importante.
Infine, la vita quotidiana dei singoli cittadini in tutto il mondo è ormai fortemente intrecciata con la tecnologia e la connettività. Dai social media, alle comunicazioni elettroniche, alle app mobili e perfino ai dispositivi smart, molti esseri umani sono ormai diventati in gran parte inseparabili dalle tecnologie. Ciò crea un pool sempre crescente di obiettivi che i criminali informatici possono tentare di sfruttare. Molti di coloro che utilizzano queste tecnologie non hanno familiarità con le tecniche per utilizzarle in sicurezza e per non esporsi ad attacchi. Di conseguenza, i ricercatori e i professionisti della sicurezza sono ancora più richiesti per la loro esperienza. Che si tratti di aumentare la consapevolezza o di sviluppare e implementare contromisure o perfino di identificare le vulnerabilità della sicurezza negli apparecchi elettronici di consumo e nel software, la sicurezza informatica è diventata la soluzione per proteggere chiunque sia connesso, in qualche modo, attraverso la tecnologia.

La cultura della sicurezza informatica

Per decenni è cresciuta e si è evoluta una vera e propria "comunità" di persone impegnate nell'obiettivo di analizzare, studiare e difendere la tecnologia. Questa comunità ha sviluppato una cultura e varie sottoculture che hanno plasmato gran parte della struttura della sicurezza informatica odierna. Vari hacker, ricercatori, professionisti e dirigenti aziendali

nel campo della cyber security, hanno sviluppato un insieme peculiare e complesso di norme e valori, associati alla community della cyber security.
Sarebbe impossibile anche solo elencare ogni valore o ideologia adottati dalla community della cyber security. Non solo sono troppo numerosi e, in alcuni casi, evanescenti, ma essi non sono nemmeno universalmente adottati da tutti coloro che si possono ritenere membri della comunità che si occupa della cyber security. Tuttavia, alcuni valori sono ampiamente riconosciuti degni di essere esaminati, per offrire un contesto migliore a chiunque cerchi di entrare a far parte di questa comunità.

Privacy e libertà

Gli elementi chiave, secondo l'ideologia di coloro che fanno parte della community della sicurezza sono la libertà personale e la privacy. Agli albori della cultura hacker, strani individui di tutto il mondo si riunivano in community su server dial-up (i famosi BBS o *Bulletin Board System*) per condividere informazioni e raccontarsi le nuove scoperte. Per ottenere l'accesso a questi sistemi, spesso i partecipanti dovevano dimostrare la prova di un attacco che avevano condotto.
Ciò, spesso, significava mostrare i dati che avevano sottratto a un'azienda di cui erano riusciti a violare i sistemi, o dimostrare di essere in grado di manipolare altre tecnologie per farle funzionare in modi non convenzionali. Poiché spesso queste attività erano considerate illegali, la capacità di proteggere la propria identità e di rimanere "a piede libero" mantenendo l'anonimato nonostante gli occhi vigili di governi e forze di polizia era molto apprezzata.
Molti dei membri di queste comunità erano trattati da emarginati nella loro vita quotidiana. Ciò che essi hanno trovato nell'anonimato di queste prime comunità è, secondo le loro parole, "una sensazione di essere tra uguali". Saltavano tutte le etichette di genere, etnia, classe sociale o altre caratteristiche accessorie, che li avevano portati a essere rifiutati dalla società tradizionale. Ciascuno veniva invece valutato quasi esclusivamente in base alle conoscenze e alle abilità che offriva. Questo li portava ad avere discussioni significative su argomenti condivisi con altri che avevano interessi simili, senza intoppi legati a stereotipi o pregiudizi.
Quando Internet ha iniziato a diffondersi, i primi limiti progettuali e di capacità della nuova tecnologia hanno consentito di proseguire nell'anonimato e hanno offerto una maggiore comodità nel connettersi a grandi comunità di individui che vedevano le cose allo stesso modo. Tuttavia, in molti casi la natura segreta e spesso clandestina di questi primi gruppi di hacker iniziò a sgretolarsi. Divennero più visibili agli occhi del grande pubblico e crebbe così l'interesse per le loro attività.
Allo stesso tempo, come ho già detto, all'interno delle aziende e degli enti governativi, si sviluppavano nuove idee e tecniche per la messa in sicurezza delle informazioni. Gruppi industriali, forze dell'ordine e governi si sono concentrati sulle tecniche di sicurezza delle informazioni e hanno iniziato a sviluppare le proprie comunità di professionisti della cyber security.
Nel corso del tempo, questi due gruppi di individui, così diversi fra loro, hanno sviluppato una relazione difficile, e a volte tesa. Attraverso incontri, organizzazioni e perfino conferenze formali sulla cyber security, i due gruppi hanno trovato il modo di condividere

le informazioni, apparentemente con l'obiettivo comune di migliorare le tecnologie e aumentare la sicurezza per tutti. Il fatto è spesso la visione ideologica di ciò che rende "migliore" una tecnologia differisce molto per questi due gruppi.
Ciò porta a una continua sfiducia e talvolta aperta animosità tra le due fazioni. Di conseguenza, la parte più idealista di hacker/ricercatori della comunità ha privilegiato il valore della protezione della privacy e della libertà. Ancora oggi, molti nella comunità della sicurezza utilizzano *pseudonimi* e soprannomi volti a proteggere l'identità effettiva della persona e operano in un generale anonimato.

Condivisione aperta delle informazioni

Uno degli elementi chiave che ha unito i primi hacker è stata la capacità di *condividere liberamente le informazioni*. Non si trattava dei criminali informatici di cui sentiamo parlare oggi; erano semplicemente persone che cercavano di studiare le tecnologie per poter apprendere cose nuove e sviluppare tecnologie ancora più innovative. Tuttavia, questa condivisione delle informazioni è stata talvolta accompagnata da una certa qual arroganza. Vantarsi di un certo attacco significava acquisire una maggiore credibilità nella comunità. Indipendentemente da ciò, il valore della condivisione delle informazioni e dello sviluppo della conoscenza grazie alle scoperte condotte da altri era e rimane un aspetto importante per la comunità.
Questo tipo di condivisione delle informazioni non è legato esclusivamente alla cultura hacker. Da sempre anche i ricercatori accademici apprezzano il concetto di condivisione aperta delle informazioni, e in effetti questo si estende al campo della ricerca sulla sicurezza informatica.
Questa cultura della condivisione delle informazioni per contribuire a migliorare la tecnologia per il bene di tutti si manifesta, in particolare, nel numero di conferenze sulla sicurezza indipendenti organizzate annualmente. In tutto il mondo si tengono migliaia di conferenze, nell'interesse della condivisione di informazioni su vulnerabilità, contromisure e molti altri argomenti. A Las Vegas si svolge ogni agosto una settimana di cicli di conferenze incentrate sulla sicurezza, colloquialmente denominata *Hacker Summer Camp*, che attrae dalle 30.000 alle 40.000 persone da tutto il mondo.
L'importanza di questa ideologia all'interno della community della sicurezza si manifesta nel modo in cui i suoi membri hanno reagito alla commercializzazione di Internet. Nella sua infanzia, Internet era una sorta di "nuova frontiera", che avrebbe consentito la libera condivisione delle conoscenze a un livello mai visto prima. Per un po', quell'ideologia sembrò avverarsi. Tuttavia, non ci è voluto molto perché le aziende si rendessero conto che potevano sfruttare Internet per ottenere nuovi flussi di entrate e per raggiungere i clienti in modi precedentemente impossibili.
Per proteggere i loro vantaggi competitivi e fidelizzare i loro mercati, le aziende hanno mantenuto i propri segreti aziendali e allo stesso tempo hanno sfruttato al massimo ogni potenzialità di Internet. Le nuove tecnologie che hanno consentito una maggiore segretezza e una strenua difesa di alcuni diritti di proprietà intellettuale erano in conflitto con l'ideologia di apertura e condivisione delle informazioni. La community della cyber security, a sua volta, ha cercato continuamente di abbattere queste barriere e di ottenere una maggiore trasparenza dalle aziende, in termini di pratiche commerciali su Internet.

Non nuocere

I primi hacker hanno subito capito che le loro capacità potevano essere messe al servizio del miglioramento della qualità della tecnologia, per tutti. Quando hanno iniziato a individuare falle nella sicurezza dei sistemi, hanno cercato dei modi per condividere queste informazioni con i proprietari di tali sistemi. Sfortunatamente, i proprietari di tali sistemi (e anche le forze dell'ordine) consideravano criminali e non utili le attività di questi hacker.
Lentamente, tuttavia, le aziende e anche le forze dell'ordine hanno iniziato a rendersi conto che, comprendendo il punto di vista e le capacità degli hacker amichevoli, potevano difendersi dalle azioni degli hacker veramente dannosi. Nacque così la figura dell'*hacker etico*: un individuo che utilizza tecniche di hacking per aiutare a individuare falle di sicurezza, allo scopo di segnalarle perché possano essere riparate. Sebbene questo termine sia caduto in disuso, il concetto è ancora vivo e vegeto.
Per poterne stabilire la legittimità, l'etica dell'hacking amichevole doveva essere attentamente stabilita e rispettata. Ciò ha consentito agli hacker etici di definire regole, tecniche e standard che li differenziassero dagli hacker dannosi. L'imperativo di questo codice etico era *non nuocere*. Questo imperativo governava le regole di ingaggio per sottoporre a test i sistemi, assicurando che le vulnerabilità scoperte non sarebbero state sfruttate in modo da causare danni né ai sistemi né alle persone.
Nell'odierno mondo della sicurezza informatica, questo codice etico sopravvive e viene impiegato in molte delle attività svolte quotidianamente dai ricercatori, dagli hacker etici e dai professionisti della cyber security. Naturalmente, però, infuriano dibattiti, quando le attività di sicurezza offensiva e di guerra informatica sembrano travalicare il limite e iniettare comportamenti davvero dannosi, pur in nome della protezione della cyber security.

Il "settore" della cyber security

Che si tratti del mondo aziendale, dei media o dell'androne politico, spesso viene usato il termine *settore* per descrivere l'insieme delle persone, delle tecnologie e delle tecniche che operano a difesa del mondo digitale. La cyber security, fin dagli albori, è stata vista come una disciplina a parte.
Ma parliamo del concetto di *carriera nel campo della sicurezza informatica*, il motivo per cui, probabilmente, state leggendo questo libro. Governi, aziende ed enti hanno creato *team interni* responsabili della sicurezza informatica. Le case produttrici di software e hardware hanno rilasciato ogni genere di *prodotti per la sicurezza informatica*, con lo scopo di difendere da ogni tipo di attacco immaginabile. Ma cresce l'incertezza sul fatto che la sicurezza informatica debba essere considerata un settore a sé.

La sicurezza informatica è un settore?

La sicurezza informatica si è affermata come un mercato commerciale. Vari studi indicano che, a livello globale, nel 2019 sono stati spesi dai 170 ai 250 miliardi di dollari per soluzioni di sicurezza informatica. Inoltre, anche college e università hanno creato corsi di laurea incentrati sulla sicurezza informatica. Le società che si occupano di formazione offrono laboratori e corsi sulla sicurezza informatica. Per anni, poiché i team

responsabili della sicurezza delle informazioni sono stati considerati come silos solitari all'interno degli organigrammi aziendali, considerare la sicurezza come un settore era opportuno e aveva senso.
Tuttavia, la sicurezza informatica si è evoluta in qualcosa di più della semplice protezione dei sistemi IT da accessi non autorizzati e danni. L'attuazione delle sue pratiche non è più solo una questione di contromisure tecniche. L'attenzione alla sicurezza si è diffusa in ogni area del commercio, degli affari internazionali e del dialogo sociale. Definire la sicurezza informatica un *settore* connota un silo autonomo, qualcosa che esiste e interagisce semplicemente con altri aspetti del nostro mondo. Ma tale connotazione non coglie il fatto che la sicurezza è un concetto fondamentale in ogni ambito del mondo digitale.

DEFINIZIONE

La sicurezza informatica è più di un settore. È importante comprendere che la sicurezza informatica si lega a ogni aspetto del nostro mondo digitale. Pertanto, considerarla un *settore* perpetua una visione antiquata della cyber security, come una funzione isolata e separata all'interno delle aziende e della società.

Gli effetti della trasformazione digitale

Come ho detto in precedenza, la trasformazione digitale ha trasferito molti elementi della vita quotidiana nel regno elettronico e digitale. La tecnologia non è più solo parte della nostra vita; nelle parole di una collega e buona amica della community della cyber security, Keren Elazari, la tecnologia è ormai il nostro stile di vita. Non stiamo più difendendo solo sistemi, tecnologie e dati, ma stiamo difendendo aspetti fondamentali del nostro mondo.
Man mano che la trasformazione digitale procede e sempre più elementi tangibili del nostro mondo vengono digitalizzati, la sicurezza informatica si radica in quell'aspetto del mondo. Le minacce crescono esponenzialmente, per numero e complessità. Nessun singolo gruppo, nessuna singola disciplina, nessun singolo dominio di competenza può, ragionevolmente, essere chiamato a difendersi da tutto ciò. I vettori di attacco risultanti sono troppo differenti ed espansivi.

L'elemento umano

Lo sviluppo del nostro mondo digitale attraverso la trasformazione di tutto ciò che conosciamo in dati e sistemi ha messo in luce un altro concetto chiave: la necessità di proteggere l'*elemento umano*. Un'idea spesso citata all'interno della community della sicurezza è che il più delle volte è l'elemento umano l'anello più debole. Per quanto siano solide le nostre difese, per quanto sia efficace la tecnologia, un singolo errore commesso da un singolo essere umano può comunque consentire a un malintenzionato di portare a termine un attacco.
Con lo sviluppo di questo concetto, abbiamo assistito all'introduzione di esperti di ingegneria sociale nelle discipline della sicurezza informatica. Le aziende pagano questi operatori per valutare la prontezza del loro personale nel difendersi dai tentativi di attacco. Gli esperti di comportamenti umani e di formazione alla sensibilizzazione sono diventati elementi cruciali in questo tipo di strategia di sicurezza. Questi esperti si concentrano

sul rimodellamento del modo in cui gli esseri umani reagiscono ai tentativi di attacco di ingegneria sociale, come il phishing, la frode telefonica e perfino le manipolazioni di persona. Nel 2020, la RSA Conference (una delle conferenze sulla sicurezza informatica più grandi e longeve al mondo) ha caratterizzato lo "Human Element" come un tema del suo evento annuale (di una settimana) a San Francisco.
L'inclusione della difesa dell'elemento umano dagli attacchi estende ulteriormente l'idea del concetto di sicurezza informatica. Costringe i professionisti a ragionare anche oltre la semplice tecnologia, e a considerare anche i modelli comportamentali, le tecniche di manipolazione e le contromisure a contrasto della disinformazione.

L'Internet di tutto

La trasformazione digitale ha cambiato molto nel modo in cui vediamo il nostro mondo in modi che stiamo appena iniziando a capire. Un esempio è l'*Internet of Things* (IoT), anche se oggi si preferisce parlare di *dispositivi smart*. Entrambi i termini descrivono prodotti e tecnologie che un tempo operavano in modo autonomo e ora sfruttano la connettività per offrire nuove funzionalità.
I frigoriferi possono rilevare quando gli articoli si stanno esaurendo e ordinarli autonomamente in negozio. Le auto sono connesse al Web per vari scopi, dall'assistenza stradale alla navigazione alla chiamata in caso di necessità. Nel febbraio 2020 è stata perfino annunciata una campagna Kickstarter per una candela da accendere a distanza utilizzando un'app su uno smartphone. Ormai tutto sembra essere connesso a Internet.
Tuttavia, questa esplosione nei dispositivi connessi ha anche causato, prevedibilmente, una crescita esplosiva delle minacce e dei vettori di attacco. Le considerazioni sulla sicurezza ora entrano a far parte di tecnologie che in precedenza non si pensava potessero rientrare nel panorama delle minacce digitali. Ancora una volta: la sicurezza sta permeando ogni aspetto della nostra vita.
Quindi, possiamo davvero considerare la sicurezza ancora come un settore? Non dovremmo, invece, considerare la sicurezza informatica semplicemente come un aspetto di ogni ambito del nostro mondo, come, del resto, la sicurezza è stata per generazioni? Certo, alcuni si specializzano nella progettazione di ambienti sicuri. Esistono le migliori tecniche, sono stati creati standard e vengono impiegati concetti. Ma alla fine, dal luogo di lavoro alle strade, alle case e a tutto il resto, la sicurezza è un aspetto intrinseco di tutto. Forse, considerando i percorsi professionali e le specializzazioni, potrebbe essere utile pensare alla sicurezza informatica in questo stesso modo.

Quindi, la sicurezza informatica è un settore?

Come abbiamo visto, il campo della sicurezza informatica è ampio e si estende non solo al mondo in continua espansione delle tecnologie, ma anche alla protezione delle persone. Il nostro stile di vita, in quasi ogni suo aspetto, è ormai parte integrante di questo mondo digitale.
Quindi, sostenere che la sicurezza informatica è solo un settore è troppo limitante. È un elemento cruciale del modo stesso in cui affrontiamo la vita quotidiana e non qualcosa di facilmente separabile. Mentre nei decenni passati la sicurezza delle informazioni poteva

essere considerata solo una disciplina sotto il più ampio ombrello della tecnologia dell'informazione, la sicurezza informatica, oggi, è sempre più un'impostazione concettuale e sempre meno un'abilità specifica o di un insieme di tecniche.

Il valore della diversità umana nel campo della sicurezza informatica

Ho appena parlato dell'elemento umano e di come gli sforzi che compiamo nell'ambito della sicurezza informatica per difendere il nostro stile di vita con mezzi tecnologici possano essere vanificati da errori umani. Pertanto, la risoluzione dei problemi, che è lo scopo ultimo di ciò che facciamo in termini di sicurezza informatica, deve includere quegli esseri umani che stiamo cercando di difendere. Ma in un mondo che ha così tante culture, così tanti ideali e così tanti livelli di istruzione e abilità, come possiamo sperare di trovare le risposte in grado di difendere tutti?

Di conseguenza, un grande passo che deve essere compiuto a tal fine è garantire la *diversità* di coloro che sono chiamati a erigere tali difese. Per proteggere il nostro stile di vita digitale, dobbiamo migliorare la qualità della nostra risoluzione dei problemi attraverso la diversità dei pensieri, delle prospettive e delle idee. Inoltre, dobbiamo conoscere le popolazioni che stiamo cercando di proteggere.

Nessuna di queste cose può essere realizzata se i nostri team di difesa impiegano persone con background simili, livelli di istruzione simili, culture simili e progressi di carriera simili (e molto altro ancora). Perché l'idea della sicurezza informatica funzioni davvero, dobbiamo diventare accoglienti e cercare attivamente di includere persone provenienti da ceti sociali tanto vari quanto le società in cui viviamo. Ciò significa che c'è posto per tutti nelle professionalità legate alla sicurezza informatica. Inoltre, abbiamo davvero bisogno di avere quanta più rappresentatività possibile in questi ruoli.

Il divario della diversità della sicurezza informatica

Nel suo *Diversity and Inclusion Report* del 2020 (`http://mng.bz/PW92`), la società di sicurezza informatica Synack ha intervistato centinaia di professionisti sulle loro esperienze di lavoro in attività di sicurezza informatica. Il sondaggio ha chiesto se gli intervistati ritenessero di avere le stesse opportunità di carriera di altri, appartenenti ad altri generi o etnie. Fra le donne, il 34% ha risposto di no. Ancora più allarmante: ha risposto di no ben il 53% delle persone appartenenti a minoranze etniche. Questi risultati sono indicativi del problema della diversità, che da anni affligge il settore tecnologico e, in particolare, la sicurezza informatica.

Nel 2017, l'(ISC)^2 (*International Information System Security Certification Consortium*), più Frost & Sullivan e altri, hanno pubblicato un *Global Information Security Workforce Study* (`http://mng.bz/J1Op`). Il sondaggio ha rilevato che, in Nord America, solo il 14% degli intervistati era costituito da donne. In tutte le altre aree del globo, quel numero era ancora più piccolo. La stampa e molte analisi si sono concentrate sul tema della rappresentanza femminile nella cyber security, ma il problema persiste. Lo stesso studio ha rilevato che solo il 23% degli intervistati con sede negli Stati Uniti si identifica in una minoranza etnica, un valore al di sotto delle percentuali complessive delle popolazioni nel Paese.

Per esempio, mentre a livello nazionale il 13,4% della popolazione si identifica come nero o afroamericano, solo il 9% del campione di questo studio si identifica come tale. Per spiegare questo divario spesso vengono portate ragioni contrastanti. Non discuterò in questo libro le motivazioni di queste teorie. Tuttavia, è importante capire che queste problematiche in termini di diversità esistono, in particolare per quanto riguarda la diversità di genere, e questo ha un impatto sul successo che possiamo avere nelle nostre attività. È altrettanto importante capire che finalmente questo problema è stato riconosciuto e che la nostra comunità, nel suo insieme, sta lavorando per cambiare lo stato di cose.

Perché la diversità è importante

La diversità è spesso propagandata come *political correctness* o un impegno "*woke*". Ma il mondo della tecnologia e della sicurezza informatica stanno lentamente individuando un valore tangibile nella diversità, il quale va ben oltre gli ideali di moralità ed equità. Come ho affermato poche pagine fa, abbiamo bisogno di professionisti in grado di comprendere la mentalità e le prospettive di coloro che cerchiamo di difendere, soprattutto quando proprio l'elemento umano è alla base di così tante problematiche al riguardo. Questa capacità di comprendere gli esseri umani cui sono rivolti i nostri sforzi ci consente di identificare meglio le soluzioni più efficaci per difenderli.

A titolo di esempio, nel 2014 il GAO (*Government Accountability Office*) degli Stati Uniti ha pubblicato un rapporto (`https://www.gao.gov/assets/gao-14-357.pdf`) che descriveva in dettaglio i casi anomali di falsi allarmi nei body scanner aeroportuali. Tra gli aspetti particolari di questo numero elevato di falsi allarmi c'erano copricapi, turbanti e parrucche. Eppure, nel 2017, ProPublica ha riportato (`http://mng.bz/wnd7`) che gli scanner hanno continuato a produrre livelli elevati di falsi allarmi, in particolare associati alle acconciature comuni tra le donne afroamericane e nere. Questo secondo i dati raccolti in modo indipendente da ProPublica.

In questi scenari, dobbiamo chiederci come mai tali problemi non vengano identificati prima. Forse le donne di colore non sono state coinvolte nello sviluppo e nei test di questi dispositivi? Forse un team di progettazione più diversificato avrebbe potuto riconoscere in modo proattivo questi potenziali problemi e assicurarsi che i progetti ne tenessero conto? In definitiva, questo è il motivo per cui la diversità è così importante. Il brainstorming e la risoluzione dei problemi si avvantaggiano del fatto che le persone coinvolte offrano prospettive ed esperienze ad ampio raggio cui attingere. Quindi, quando parliamo di sicurezza informatica, dove la risoluzione dei problemi è il fulcro della nostra stessa vocazione, anche noi dobbiamo cercare di promuovere una significativa diversità all'interno della nostra comunità.

In che modo riguarda il vostro percorso professionale

Tutto questo è bellissimo, ma sembra un problema che riguarda la comunità e l'industria nel suo insieme. Anche se quanto abbiamo appena visto è vero, per chi cerca di avviare una carriera nel campo della sicurezza informatica, è importante tenere a mente che queste problematiche esistono. Nei Capitoli 8 e 9, discuterò le varie problematiche che possono far deragliare il vostro sviluppo professionale. Per il momento, l'importante è

che questo concetto sia ben compreso per iniziare a capire l'attuale composizione della community della sicurezza informatica, come siamo arrivati fin qui e dove siamo diretti. All'inizio del percorso professionale che vi ha portato a questo libro, potreste avere difficoltà a entrare nella comunità, se non vi sentite rappresentati nei volti di coloro che già vi operano. Questo è il motivo per cui dovrete attingere alle informazioni di questo capitolo, per capire che non solo siete i benvenuti ma siete anche necessari. Armati di queste informazioni, nel prossimo capitolo analizzeremo tutti i posti in cui potreste trovare impiego nell'ambito della sicurezza informatica.

Riepilogo

- La sicurezza informatica è il dominio della ricerca, delle tecnologie e delle tecniche volte a proteggere i sistemi tecnologici connessi, i dati e le persone da attacchi, usi non autorizzati e/o danni.
- Il ruolo della sicurezza informatica cambia in base al contesto, ma nel nostro mondo digitale interconnesso si occupa di proteggere l'intero nostro stile di vita.
- La sicurezza informatica può trarre grandi vantaggi dalla diversità di esperienze e culture, e la comunità continua a lavorare per migliorare l'attuale carenza di diversità.