Introduzione

Il nostro mondo è dominato dall'informazione, questo è dimostrato dal fatto che tutte le società che attualmente hanno le maggiori capitalizzazioni di mercato sono legate alle informazioni (Apple, Microsoft, Alphabet, Amazon, Nvidia, Meta).

Chi fa cybersecurity si occupa di fare in modo che chi possiede delle informazioni di valore non le perda e che non gli vengano rubate.

La tecnologia informatica è l'elemento chiave che fa funzionare ogni attività, se l'infrastruttura informatica viene attaccata e smette di funzionare correttamente questa subirà dei danni. Sorge quindi la necessità di prendere contromisure per fare in modo che questo non accada.

Storia degli attacchi più importanti

I seguenti attacchi hanno caratterizzato l'evoluzione del mondo dell'hacking e hanno segnato un punto di svolta sulle metodologie e sulle tecniche usate per attaccare i calcolatori.

Lawrence Berkeley Laboratory - 1986

Il primo attacco di cui si ha traccia è avvenuto nel 1986, all'epoca nessuno sapeva ancora niente sulla cybersecurity, internet aveva solo 2000-3000 nodi ed i collegamenti dall'Europa non erano molti.

L'attacco fu effettuato da Markus Hess, un programmatore della Germania dell'Ovest che aveva come obiettivo il furto di alcuni progetti di ricerca in ambito militare, realizzati da dei ricercatori in accordo con il ministero della difesa statunitense e memorizzati in dei calcolatori situati nel Lawrence Berkeley Laboratory (LBL) in California, al fine di rivenderli al KGB (il servizio segreto russo).

Clifford Stoll, l'amministratore di sistema dell'LBL, scoprì che qualcuno aveva ottenuto l'accesso da amministratore sfruttando una vulnerabilità presente in GNU Emacs, iniziarono quindi delle indagini che coinvolsero la CIA (Central Intelligence Agency), l'FBI (Federal Bureau of Investigation), l'NSA (National Security Agency) e l'Interpol. Quando scoprirono che l'attaccante proveniva dalla Germania dell'Ovest gli tesero una trappola in collaborazione con la polizia tedesca: caricarono dei file apparentemente allettanti di grandi dimensioni (che quindi richiedevano parecchio tempo per essere scaricati, a quel tempo un modem casalingo arrivava a 64kb/s quando andava bene), in modo da avere abbastanza tempo per riuscire a risalire alla fonte dell'attacco, ovvero la casa di Hess ad Hanover.

Una volta arrivati sul posto lo arrestarono. Dopo il processo fu condannato a 20 mesi di prigione e al pagamento di una multa da 10.000 marchi tedeschi.

Internet Worm - 1988

Nel 1988 erano pochi quelli che sapevano dell'attacco di Hess, ma in quell'anno avvenne un grande attacco che si guadagnò l'attenzione dei media e che diede inizio alla cybersecurity: l'Internet Worm di Robert Tappan Morris, allora studente del Massachusetts Institute of Technology (MIT).

Questo attacco è una pietra miliare perché rese inutilizzabili circa 6000 computer (il 10% della rete) in poche ore, inoltre per la prima volta fu realizzato un attacco che faceva uso del buffer overflow, una vulnerabilità

conosciuta ma che nessuno prima di allora era mai riuscito ad utilizzare per questo scopo. I sorgenti di questo worm vennero resi disponibili in internet e da allora chiunque fu in grado di realizzare un attacco che faceva uso del buffer overflow, dando così inizio al delirio in rete.

Morris venne catturato perché fu denunciato dal collega che l'aiutò a scrivere il codice del worm. Durante il processo disse di aver fatto partire l'attacco involontariamente ma fu comunque condannato a 3 anni di carcere, al pagamento di una multa da 10.050 dollari e a 400 ore di servizio alla comunità. Ora è professore associato di sistemi operativi al MIT.

San Diego Supercomputer Center - 1994

Nel 1994 il Supercomputer Center di San Diego venne attaccato (probabilmente) da Kevin Mitnick, un cracker esperto che fin da giovane riuscì ad ottenere l'accesso non autorizzato a diversi sistemi. Questo fu il primo attacco ai protocolli di rete: il TCP/IP hijacking.

Nel 1995, dopo aver passato 2 anni e mezzo da fuggitivo, venne arrestato e condannato a 5 anni di prigione. Dopo il suo rilascio creò una sua società di consulenza e sicurezza informatica, ricoprendo il ruolo di amministratore delegato fino al 2023, anno della sua morte.

Citibank - 1995

Questo è un attacco importante perché è il primo attacco noto ad una banca. Le banche sono uno dei principali obiettivi degli attacchi informatici perché hanno tanti soldi e difficilmente denunciano di essere state attaccate (tutti i clienti spaventati andrebbero a ritirare i loro soldi).

Gli autori di questo attacco furono dei ragazzi di San Pietroburgo, esperti nella compromissione dei router. Questi riuscirono ad accedere a dei router che smistavano il traffico per una filiale della Citibank, una banca di Londra. Il traffico di allora era trasmesso in chiaro e quindi intercettando le sessioni di collegamento dei clienti riuscirono ad ottenere i dati per il login di diverse centinaia di persone, che usarono per farsi dei bonifici su dei conti aperti in Svizzera. Dopo 15 minuti dal trasferimento del denaro, dei complici andavano a prelevare.

Citibank se ne accorse grazie a dei meccanismi di rilevamento dell'intrusione (che sono in uso ancora adesso). Ognuno di noi ha un profilo presso la banca che dice quali sono le operazioni più frequenti che facciamo e con quali persone interagiamo più spesso. Quando viene rilevata un operazione diversa dalle solite la banca s'insospettisce. Questo è esattamente quello che successe quando Citibank vide diversi bonifici verso conti in Svizzera di clienti che non avevano mai lasciato Londra. Per verificare chiamarono diversi clienti chiedendo conferma a scoprirono che questi bonifici erano fraudolenti.

Contattarono l'Interpol che gli suggerì di stare al gioco per un paio di giorni, in modo da poter mettere i sistemi sotto controllo e tracciare gli attaccanti. In questo modo riuscirono a risalire al gruppo di ragazzi e ad emettere dei mandati di cattura internazionale. Non essendoci l'estradizione dalla Russia all'Europa questi erano al sicuro. Però, non essendo a conoscenza dei mandati, il capo del gruppo, Vladimir Levin, decise di andare a farsi una vacanza ad Amsterdam con i soldi guadagnati. Quando atterrò all'aeroporto e gli controllarono il passaporto, gli addetti si accorsero del mandato e lo fecero arrestare per 3 anni.

Come si può notare, in questi anni le pene erano scarse perché non era ancora stato introdotto il reato di compromissione fraudolenta di sistema informatico. Ad oggi sono solo 91 i paesi che firmando un trattato internazionale riconoscono l'hacking come reato.

Stuxnet - 2010

Stuxnet è considerato uno dei malware più complessi mai realizzati nella storia. È un virus che infettava le macchine Windows con installato Siemens Step7, un software usato per controllare i PLC (controllore logico programmabile), dei computer specializzati nella gestione e nel controllo dei processi industriali.

Questo attaccava solo i sistemi con particolari requisiti, in particolare i macchinari che controllavano le centrifughe usate per l'arricchimento dell'uranio. Stuxnet riusciva ad accedere a queste macchine e a modificare la velocità di rotazione delle centrifughe, causandone la rottura. Allo stesso tempo faceva credere agli addetti al controllo che andava tutto bene.

Data la scarsa reperibilità di queste centrifughe, si stima che Stuxnet abbia causato 2 anni di ritardo al programma nucleare iraniano. Ad oggi nessuno se ne assume la paternità ma sembra che sia stato il risultato di uno sforzo congiunto tra la NSA e Mossad (i servizi segreti israeliani). Per questo motivo la stampa gli diede l'appellativo di "prima arma digitale".

Possiamo notare che i servizi segreti hanno sempre un ruolo fondamentale in tutte queste vicende.

WannaCry - 2017

WannaCry è il primo ransomware (un malware che crittografa l'intero disco e chiede il pagamento di un riscatto per decrittografarlo) famoso della storia, la sua fama è dovuta al fatto che ha infettato numerosissimi sistemi in tutto il mondo in poche ore.

Per diffondersi utilizzava una vulnerabilità che affliggeva i sistemi Windows chiamata EternalBlue, realizzata dalla NSA ma scoperta e diffusa dal gruppo hacker The Shadow Brokers (probabilmente russo).

SolarWinds - 2020

SolarWinds è una società che si occupa di realizzare strumenti per il controllo di sistemi informatici. Nei primi mesi del 2020, degli attaccanti riuscirono ad accedere ai loro sistemi e a modificare il codice della patch successiva di Orion, uno dei loro prodotti, inserendo una backdoor.

A Maggio SolarWinds distribuì la patch, infettando così 18.000 dei suoi clienti. Tra i soggetti coinvolti troviamo: l'Arma dei Carabinieri, il Ministero dell'Interno, l'Agenzia Italiana per la Pubblica Amministrazione Digitale, vari ministeri statunitensi e molti altri ancora. L'attacco è stato scoperto solo nel Dicembre del 2020, cosa sia successo nei 6 mesi che sono trascorsi non è dato saperlo.

Le minacce che intercettano informazioni o che alterano sistemi mentre rimangono invisibili per lunghi periodi di tempo vengono chiamate APT (Advanced Persistent Threat).

Human Hacking

Le informazioni che alcune società raccolgono su di noi possono essere usate per determinare in modo veloce, preciso, automatico e poco costoso una serie di attributi personali sensibili (personalità, interessi, orientamento sessuale, religione, appartenenza politica, intelligenza, felicità, ...). I profili psicologici che vengono generati possono essere usati per cercare d'influenzare in modo più efficace le scelte delle persone.

Cambridge Analytica - 2013/2018

Nel 2013 Cambridge Analytica pubblicò un applicazione per Facebook a scopo di ricerca chiamata "This Is Your Digital Life", questa permetteva di rispondere ad una serie di domande per ricevere una piccola somma

di denaro.

Facebook però, oltre a dare all'applicazione l'accesso ai dati delle persone che risposero, le permise anche di accedere a quelli di tutte le loro persone amiche. Partendo dalle 270.000 persone che usarono l'applicazione, Cambridge Analytica fu in grado di ottenere i dati di 87 milioni di persone.

Tutti i dati raccolti furono dati in pasto a degli algoritmi di profilazione e usati per influenzare le opinioni delle persone attraverso delle pubblicità mirate, che invogliavano gli utenti a votare per Ted Cruz e Donald Trump nelle rispettive campagne presidenziali e per l'uscita del Regno Unito dall'Unione Europea.

Terminologia

Hacker: sono persone appassionate alla programmazione, interessate ad approfondire anche i più piccoli dettagli e che cercano di spingere al limite le loro conoscenze informatiche.

Cracker: sono quelle persone interessate a compromettere la sicurezza dei sistemi informatici.

Script Kiddie: sono la più bassa forma di cracker, fanno dispetti eseguendo degli script che scaricano dalla rete, spesso senza neanche conoscerne il funzionamento.

Oggi comunemente si associa alla parola hacker il significato di cracker, per questo motivo sono stati coniati altri termini prendendo ispirazione dal colore dei cappelli indossati dai personaggi dei film western americani.

White Hat: sono quegli hacker che cercano di trovare vulnerabilità e falle nella sicurezza dei sistemi informatici avendo il permesso dei proprietari. Hanno buone intenzioni e se trovano delle vulnerabilità non ne divulgano pubblicamente l'esistenza fino a che non sono state rimosse.

Gray Hat: fanno lo stesso lavoro dei white hat ma non sempre hanno il permesso dei proprietari. Hanno comunque buone intenzioni, infatti non sfruttano le vulnerabilità trovate per fare attacchi e non ne divulgano pubblicamente l'esistenza.

Black Hat: sono i cracker, cercano e sfruttano vulnerabilità per accedere ai sistemi informatici senza il permesso dei proprietari al fine di spiare, rubare informazioni e distribuire malware.

Computer Security

La computer security (sicurezza informatica) è l'insieme delle misure e dei controlli che garantiscono la confidenzialità, l'integrità e la disponibilità degli asset di un sistema d'informazione (ovvero l'hardware, il software, il firmware e le informazioni processate, memorizzate e trasmesse).

Questa ha il compito d'individuare gli strumenti utili a garantire le 3 proprietà che caratterizzano un sistema sicuro:

- **Confidenzialità** (**Confidentiality**): un sistema garantisce la confidenzialità se permette l'accesso alle informazioni memorizzate al suo interno solo alle persone autorizzate. In alcuni testi viene anche chiamata privacy.
- **Integrità** (**Integrity**): un sistema garantisce l'integrità se è in grado di impedire la modifica o la distruzione non autorizzata delle informazioni memorizzate al suo interno.
- **Disponibilità** (**Availability**): un sistema garantisce la disponibilità se è in grado di fornire l'accesso alle informazioni memorizzate al suo interno a fronte di qualsiasi cosa possa accadere. È la proprietà più difficile da garantire.

Possibili attacchi a queste proprietà nel caso dei vari asset:

Asset	Confidenzialità	Integrità	Disponibilità
Hardware	Rubando una memoria contenente dei dati non crittografati	-	Rubando o rompendo del materiale e causando un'interruzione del servizio
Software	Facendo una o più copie di un programma senza autorizzazione	Modificando un programma in modo da non farlo funzionare o per fargli svolgere compiti indesiderati	Cancellando un programma ed impedendo che possa essere usato
Dati	Leggendo dei dati senza autorizzazione o analizzando dei dati statistici per rivelare dei dati sottostanti	Creando nuovi dati o modificando quelli memorizzati	Cancellando dei dati ed impedendone l'utilizzo
Linee di comunicazione e reti	Intercettando e leggendo dei messaggi o effettuando l'analisi del traffico	Creando dei messaggi falsi oppure modificando, ritardando, riordinando o duplicando quelli autentici	Eliminando dei messaggi o rendendo indisponibili le linee di comunicazione

La computer security si divide in due categorie:

- **Defensive security**: si occupa di salvaguardare gli asset evitando che vengano compromessi. I proprietari degli asset che hanno valore adottano delle **contromisure**, ovvero dei meccanismi utili a ridurre il **rischio** di compromissione degli asset (non garantiscono il 100% di sicurezza ma rendono gli attacchi molto più complessi).
- **Offensive security**: si occupa di provare ad ottenere l'accesso non autorizzato ai sistemi informatici sfruttando le vulnerabilità. I threat agents (o threat actor) sono gli individui o i gruppi che vogliono abusare e/o danneggiare l'asset attaccandolo.

Superficie d'attacco

Il problema dei sistemi informatici è che contengono numerose **vulnerabilità** (o debolezze), queste possono essere sia a livello software che hardware. Individuare una vulnerabilità non è facile, esistono degli strumenti automatici che permettono di trovarne alcune ma in generale è necessario studiare il codice sorgente o i progetti.

La **superficie d'attacco** è l'insieme delle vulnerabilità presenti in un sistema, il lavoro di chi si occupa di cybersecurity dal punto di vista defensive è quello di minimizzarla. Il problema è che questa non è nota, va scoperta, studiata ed analizzata e questo non è un compito facile. Potrebbero esserci vulnerabilità che sfuggono agli analisti e che invece vengono notate dai cracker.

La superficie d'attacco può comprendere tutti i componenti di rete, software, hardware e soprattutto la parte più delicata: la **componente umana**. Possiamo avere gli strumenti di sicurezza più avanzati ma se urliamo la

password ai quattro venti o la scriviamo su un foglietto attaccato al monitor questi diventano inutili (il phishing fa leva proprio sul fattore umano).

Attacco

L'**attacco** è lo sfruttamento di una o più vulnerabilità da parte di una **minaccia** (gli hacker o cracker), mentre il modo con cui la vulnerabilità viene sfruttata si chiama **exploit**. La sola presenza di una vulnerabilità non crea problemi, è necessaria anche una minaccia interessata a sfruttarla.

Gli attacchi si possono dividere in due categorie:

- **Passivi**: comprendono diverse tipologie d'intercettazione, sono particolarmente insidiosi perché il sistema non viene intaccato e quindi non possono essere rilevati.
- **Attivi**: avvengono quando l'attaccante cerca di modificare il comportamento del sistema, ma proprio per questo motivo possono essere rilevati.

Alcuni esempi di attacco con relative conseguenze:

Attacchi	Conseguenza
Exposure: un entità non autorizzata rilascia direttamente dei dati sensibili. **Interception**: un entità non autorizzata accede direttamente a dei dati sensibili che viaggiano tra sorgenti e destinazioni autorizzate. **Inference**: un entità non autorizzata accede indirettamente a dei dati sensibili (non necessariamente i dati contenuti nelle comunicazioni) ispezionando le caratteristiche e i sottoprodotti della comunicazione. **Intrusion**: un entità non autorizzata ottiene l'eccesso a dei dati sensibili aggirando le protezioni di un sistema.	**Unauthorized disclosure**: circostanza o evento con cui un entità ottiene l'accesso a dei dati sensibili senza autorizzazione.
Masquerade: un entità non autorizzata ottiene l'accesso ad un sistema ed effettua degli atti malevoli fingendosi autorizzata. **Falsification**: un entità autorizzata viene ingannata da dei dati falsi. **Repudiation**: un entità ne inganna un altra negando falsamente la propria responsabilità riguardo ad un certo atto.	**Deception**: circostanza o evento che potrebbe indurre un entità autorizzata a credere che dei dati falsi siano veri.
Incapacitation: si previene o interrompe lo svolgimento delle operazioni di un sistema disabilitandone un componente. **Corruption**: si alterano in modo indesiderato le operazioni svolte da un sistema modificandone negativamente le funzioni o i dati. **Obstruction**: si interrompe lo svolgimento dei servizi di un sistema ostacolandone le operazioni.	**Disruption**: circostanza o evento che interrompe o previene la corretta operatività dei servizi e delle funzionalità di un sistema.

Attacchi	Conseguenza
Misappropriation: un entità non autorizzata assume il controllo logico o fisico delle risorse di un sistema. **Misuse**: si causa lo svolgimento di una funzione o di un servizio dannoso per la sicurezza di un sistema da parte di un componente dello stesso sistema.	**Usurpation**: circostanza o evento che risulta nell'assunzione del controllo di servizi o funzioni di sistema da parte di un entità non autorizzata.

Contromisure

Le **contromisure** servono a ridurre il rischio di attacco, nello specifico possono far parte delle seguenti attività:

- **Prevenzione** (**Prevention**): consiste nell'individuazione di meccanismi che garantiscono che una certa forma di attacco non si possa più verificare. È la cosa migliore in cui possiamo sperare. Ci sono alcuni attacchi che non è possibile prevenire, in questi casi si passa ad una strategia di rilevamento.
- **Rilevamento** (**Detection**): consiste nell'individuazione di misure che segnalino al system manager la presenza di un attacco in corso. Purtroppo non sempre è possibile fare detection, quindi è fondamentale fare affidamento anche sul ripristino.
- **Ripristino** (**Recovery**): consiste nell'ideazione di vere e proprie **strategie** che consentano di ripristinare il sistema il prima possibile. Per un singolo computer basta avere un backup su un disco esterno, ma quando si parla di una rete aziendale è necessario realizzare meccanismi più complessi.

Analisi dei rischi

Bisogna tener presente che quando si crea un architettura di sicurezza in ambito aziendale non si dispone di risorse illimitate (mediamente il budget per la cybersecurity è il 6-10% del budget dedicato al sistema informativo, ben poco), è quindi fondamentale essere capaci di capire quali sono le vulnerabilità più importanti effettuando l'**analisi dei rischi**.

Durante questa operazione si cerca di capire che impatto hanno le vulnerabilità presenti sul sistema, sugli asset dell'organizzazione e sugli individui. L'impatto può essere:

- **Basso**: se le perdite sono limitate.
- **Medio**: se le perdite sono serie.
- **Alto**: se le perdite sono severe o catastrofiche.

Dopo questa fase si procederà con l'eliminazione delle vulnerabilità che hanno un impatto alto, seguiranno quelle che hanno un impatto medio e infine quelle che hanno un impatto basso.

Variazione del rischio complessivo in base alla dimensione della superficie d'attacco e al budget messo a disposizione:

-	Superficie d'attacco piccola	Superficie d'attacco grande
Budget scarso	Rischio medio	Rischio alto
Budget elevato	Rischio basso	Rischio medio

Security policy

La sicurezza informatica in ambito aziendale viene prima progettata e formalizzata attraverso una **security policy**, per poi essere implementata solo successivamente. La security policy scelta non deve necessariamente garantire il massimo delle protezioni, ad esempio se un azienda ha un sito web statico (usato solo per divulgare alcune informazioni) può tranquillamente decidere di non proteggerlo perché non ci sono dati sensibili e può limitarsi ad effettuare dei backup per ripristinarlo in caso di necessità. In ogni caso il compito di prendere queste scelte spetta al manager e non all'esperto di cybersecurity.

Recentemente è iniziata a nascere nel mondo della security la richiesta di avere un ente certificatore che garantisca la qualità delle protezioni in uso (soprattutto da parte delle banche). Una volta che i sistemi di protezione sono stati realizzati arriva un ente superpartes che va a verificarli, se superano dei test e vengono considerati idonei viene rilasciato un bollino di qualità (assurance and evaluation).

Standard di sicurezza

Negli ultimi anni sono nati degli standard di sicurezza che guidano le aziende alla progettazione e alla realizzazione dei loro sistemi informatici. I principali sono:

- NIST SP 800: il NIST (National Institute of Standards and Technology) è un agenzia del governo statunitense che si occupa della gestione delle tecnologie. Nel loro sito (nist.gov) sono disponibili una serie di pubblicazioni facenti parte dello standard SP 800 che danno delle linee guida, delle raccomandazioni e delle specifiche tecniche da seguire.
- ISO/IEC 27000: è uno standard sviluppato dall'ISO (International Organization for Standardization) e dall'IEC (International Electrotechnical Commission). Fornisce raccomandazioni utili alla creazione e al mantenimento di un sistema per la gestione della sicurezza informatica.
- X.509: l'ITU-T (International Telecommunication Union - Telecommunication Standardization Bureau) è il settore dell'ITU (un'agenzia specializzata dell'ONU) che si occupa di definire gli standard per le telecomunicazioni. Questo standard definisce il formato dei certificati digitali, dei documenti elettronici usati per provare la validità delle chiavi crittografiche pubbliche.
- MANRS (Mutually Agreed Norms for Routing Security): l'ISOC (Internet Society) è un organizzazione internazionale che promuove l'accesso, l'utilizzo, lo sviluppo e l'evoluzione di Internet per il bene di tutto il mondo. Oltre alle norme MANRS, fondamentali per evitare alcune minacce all'infrastruttura di routing di Internet, pubblica periodicamente dei rapporti con raccomandazioni utili a migliorare l'uso di Internet.

Torna all'indice delle lezioni
Lezione successiva: Linux e processi