Cyber security: cos'è, tipologie di attacco e difesa, questioni legali e normative

Cyber security: cos è, tipologie di attacco e difesa, questioni legali e normative
Home Cultura cyber
Ecco tutte le necessarie nozioni di cyber security per comprenderne gli obiettivi, imparare a riconoscere le differenti tipologie di attacco e difesa, costruire una necessaria architettura di sicurezza per i propri sistemi e conoscere le differenti questioni legali e normative
7 minuti fa
Network and security administrator
Nel 1948 Norbert Wiener, matematico statunitense, definì la cibernetica come "lo studio del controllo e della regolazione (e autoregolazione) della macchina tramite la trasmissione e l'elaborazione di informazioni provenienti dall'esterno".
Nel tempo sono state proposte estensioni di definizione di cibernetica: fra esse l'identificazione fra la cibernetica e la teoria dell'informazione e lo studio del linguaggio, come strumento di comunicazione, sottolineando il ruolo chiave che il "messaggio" e la sua "comunicazione o trasmissione" ricoprono in tutti i processi che interessano la cibernetica.
Ecco, quindi, che il moderno uso dei messaggi (o comunicazione), le informazioni che riportano e la loro protezione in tutte le fasi di creazione, conservazione, invio e ricezione, hanno dato vita ad una infrastruttura che esponenzialmente cresce di anno in anno e della quale ci si deve occupare se vogliamo comunicare con i nostri interlocutori senza che altri interferiscano volontariamente o meno, danneggiando, modificando o intercettando la nostra comunicazione in maniera fraudolenta o meno.
La sicurezza informatica o cyber security, come va molto di moda chiamarla oggigiorno secondo inclinazioni esterofile sempre più invadenti ma talvolta più "comode", si occupa della protezione dei sistemi, delle reti informatiche e delle informazioni che queste custodiscono e la loro divulgazione, da furti o danneggiamenti, interruzione o indirizzamento errato dei servizi che forniscono, secondo gli standard di disponibilità, confidenzialità e integrità (C.I.A.)
Volendo dare una definizione ufficiale, secondo l'enciclopedia Treccani, con il termine sicurezza informatica ci si riferisce a quel "ramo dell'informatica che si occupa di tutelare i sistemi di elaborazione, siano essi reti complesse o singoli computer, dalla possibile violazione, sottrazione o modifica non autorizzata di dati riservati in essi contenuti".
Nel calderone della cyber security spesso intendiamo inclusi sicurezza informatica e sicurezza delle informazioni che però va bene se e solo se abbiamo bene in mente che si tratta di due cose ben distinte e che per brevità non ne sottolineiamo la differenza. Si possono declinare e differenziare diversi aspetti sulla sicurezza, quali la sicurezza fisica (degli edifici), sicurezza del dato, sicurezza hardware, distinzione degli attacchi e relative difese e molte altre cose, ma non è questo lo scopo, al momento.
La sicurezza informatica è una sfida significativa e determinante, nel mondo contemporaneo, a causa della complessità dei sistemi informativi, sia in termini di utilizzo tecnologico che geopolitico ed economico. Il campo è diventato importante anche a causa della maggiore dipendenza delle attività quotidiane da sistemi informatici e Internet, nonché per la sempre maggiore diffusione di dispositivi "intelligenti" (smart) come telefoni, televisori e i vari dispositivi che costituiscono l'Internet delle cose (IoT) come ad esempio apparecchi medicali, auto, elettrodomestici e chissà che altro.
Come si impara la cyber security: ecco le nozioni di base necessarie
Indice degli argomenti

Cyber security: un accenno di storia
Si sa, è attività comune creare sistemi e cercare di valutarne robustezza e affidabilità: si creano automobili ma prima di metterle in commercio si fanno crash test e si provano le auto con i percorsi dell'alce; si progettano centrali nucleari ma prima di iniziare a costruirle si studiano sistemi di contenimento in caso di rischio di fusione del nòcciolo (ad esempio); si studiano virus per guerra batteriologica e si cerca di avere un vaccino in caso di pandemia dovesse mai sfuggire al controllo. Il mondo IT non è diverso.

Si creano sistemi di salvataggio dati e configurazioni delle macchine (backup) e poi si testano con i piani di ripristino (recovery

Cyber security: cos'è, tipologie di attacco e difesa, questioni legali e normative

plan); si installano sistemi di anti-intrusione (firewall) e poi si verificano con tentativi di penetrazione (penetration test).
Quindici o venti anni fa si vociferava che i virus venissero messi in circolazione da aziende produttrici di programmi antivirus per vendere meglio i propri prodotti.
Convenzionalmente si fa risalire il primo programma Worm al 1971 con il nome Creeper ideato da Bob Thomas e al 1972 Reaper, il primo programma ideato per bloccare Creeper, creato da Ray Tomlinson.
Sempre convenzionalmente, perché le vere azioni di spionaggio rimangono segrete per sempre, perché se ne è parlato sui giornali e anche perché è entrato nel Guinness dei primati, si fa risalire il primo caso documentato di spionaggio informatico ad opera di un gruppo di "hackers" tedeschi tra il settembre 1986 e il giugno 1987.
Il gruppo violò le reti di appaltatori della difesa, università e basi militari americane e passò le informazioni al KGB, il servizio segreto russo. Leader del gruppo era Markus Hess che fu arrestato il 29 giugno 1987 ma formalmente incriminato nel 1989 e condannato per spionaggio il 15 febbraio 1990.
E l'hacker più famoso, sicuramente il più noto al grande pubblico, è Kevin Mitnick che iniziò giovanissimo a studiare e sfruttare le vulnerabilità tecniche delle macchine e quelle umane con l'ingegneria sociale (ramo in cui è considerato un vero maestro); fu arrestato dall'FBI nel 1995 e sembra che a lui s'ispiri il famoso film del 1983 Wargames in cui un ragazzino di Seattle riesce ad entrare nei sistemi del NORAD (il sistema di difesa aerea statunitense): solo delle voci, naturalmente, anche perché lo stesso Mitnick ha negato di averlo mai fatto.
Studiare la tecnologia informatica per metterla in sicurezza
La volontà e il dovere di rendere i prodotti sempre più sicuri nonché l'innata curiosità umana sono le molle che spingono a studiare sempre più a fondo e sperimentare nuovi aspetti della tecnologia.
E se la tecnologia che si prende in esame è composta da diversi aspetti che vanno dalla componentistica alla trasmissione dei dati e dalle diverse filosofie di costruzione e assembramento alla interazione degli essere umani che la gestiscono, non deve sorprendere se gli aspetti dei quali si deve verificare la sicurezza e affidabilità sono molteplici, se lo spettro e le diverse angolazioni con cui si possono sfruttare certe vulnerabilità sono solo inferiori all'inventiva umana.
Ecco, quindi, che la superficie di attacco potenzialmente sfruttabile e di contro il terreno e le competenze necessarie per la sua difesa aumentano notevolmente.
Riporto qui sotto delle tabelle (nessun copyright ma libere immagini scaricabili da internet) dove sono visualizzati i livelli nei quali la tecnologia informatica viene convenzionalmente suddivisa per poterla meglio studiare, migliorare e gestire.
Ogni livello è composto da diverse tecnologie, ogni livello è legato e connesso al suo immediato vicino inferiore o superiore tramite protocolli standard di collegamento. Per ogni livello, che prende in esame un passo che va dalla produzione dei dati alla loro trasmissione e ricezione, ci sono protocolli di funzionamento, potenziali vulnerabilità, impatti e contromisure che si possono o devono sfruttare, studiare, controllare, rafforzare e gestire con altrettanti protocolli, macchine e programmi.
Senza naturalmente contare che si dovrebbe anche valutare tutto ciò che gira intorno la tecnologia informatica e ai dati, cioè le persone, gli accessi all'edificio, continuità energetica e così via. Normalmente s'includono nel tema della sicurezza informatica diversi aspetti che però tecnicamente parlando si dovrebbero distinguere tra sicurezza e protezione (security & safety).
Sicurezza più appropriato se si parla di attacchi, tipologie di attacco, mezzi di attacco (o di difesa); se invece vogliamo sapere come siamo organizzati se perdiamo un dato, se ci tagliano la luce, se inondano con acqua la sala macchine, se perdiamo una chiavetta USB allora dovremmo parlare di protezione.
Per approfondire i diversi aspetti da prendere in considerazione possiamo leggere qui.
Volendo quindi avere una breve e necessariamente ridotta panoramica della molteplicità delle possibilità in gioco si può consultare il sito web del MITRE Attack Framework.
Dal sito è possibile cliccare sui vari attacchi e avere dettagli tecnici di ogni aspetto. Ogni attacco è basato su vulnerabilità dovute ad erronea progettazione, implementazione o funzionamento. La maggior parte delle vulnerabilità scoperte vengono poi catalogate ed inserite nel database Common Vulnerabilities and Exposures (CVE).
E se esiste una tabella per gli attacchi, ne esiste una per le difese che si possono implementare dove parimenti si può "giocare" con una panoramica interattiva di tabelle e definizioni. Al seguente link si può seguire un seminario offline diviso su 5 moduli di attacco e difese possibili
Vedendo una simile tabella di attacchi è chiaro e lapalissiano dedurre che non esiste la sicurezza (né informatica né di altro tipo) al 100%, ma una soglia tollerabile fatta da analisi del rischio, misure minime e azioni di mitigazione al "buco" ottenuto in caso di attacco, buco che si valuta in gradi che vanno da "nullo" a "catastrofico" in cui si può avere perdita di dati, finanziaria, vite

Cyber security: cos'è, tipologie di attacco e difesa, questioni legali e normative

umane e chissà che altro.

Le tipologie di attacco e difesa

Guardando le tabelle prima riportate già si è avuto un assaggio dei vari attacchi esistenti: DoS, DDoS, sniffing, spoofing, phishing, Man in the middle, backdoor, tampering, malware, rootkit, reverse engineering, privilege escalation, keylogging, buffer overflow, updates o patches non eseguite e via discorrendo (scusate l'inglese ma, come ho detto, talvolta più comodo).

Ho tenuto fuori volutamente dal primo elenco i tre tipi che secondo me stanno causando i maggiori danni: social engineering, ransomware e mancato aggiornamento umano.

Tralasciando ciò che di tecnico si può mettere in campo per contrastare la prima lista (a tal proposito si veda, come esempio, la seconda delle tabelle seguenti).

Per le ultime tre tipologie di attacco (social engineering, ransomware e mancato aggiornamento umano) la questione si annuncia più complicata perché hanno a che fare con la natura umana, l'una legata all'altra. Il mancato aggiornamento umano, inteso come cultura della sicurezza fornita ai dipendenti, seminari di consapevolezza, corsi di aggiornamento tecnico e comportamentale, può portare a conseguenze molto spiacevoli.

Scrivere le password sui fogliettini in vista, non chiudere i cassetti, lasciare i computer accessi senza password ("perché tanto qui ci conosciamo tutti"), fornire le password via email o al telefono, configurare la password con il nome del proprio cane o la data del matrimonio sono tutte attività che dovrebbero essere bandite e controllate al microscopio.

La cultura della sicurezza, che non deve diventare mai ossessiva ma ragionata e metabolizzata, se non è proposta divulgata e fornita al personale, porta a più facili attività di social engineering che possono portare ad attività di ransomware, cioè quando i dati vengono criptati e bloccati a fronte di pagamenti di riscatto, in diversi casi anche non seguiti dall'ottenimento della relativa password per sbloccare i propri dati.

Secondo IBM Security e il suo ultimo rapporto "Cost of a Data Breach Report - 2021", l'impatto finanziario a livello globale, a seguito di vari problemi di sicurezza che hanno portato ad una violazione dei dati, ha seguito una tendenza al rialzo negli anni, con un deciso incremento dall'inizio della pandemia COVID-19 che ha dato una spinta decisa al lavoro da remoto.

Fonte.

Inoltre, sempre dal medesimo rapporto, si può evidenziare come ben il 37% dei vettori che hanno portato ad una violazione si può ricondurre direttamente ad un errore umano (social engineering, phishing e credenziali compromesse) con una media di costi ben oltre i 4 milioni di dollari.

Fonte.

Come tutti sanno, la forza di una catena risiede nella robustezza del suo anello più debole: non dovrebbe accadere agli utenti di ricoprire questo ruolo.

Più si educano gli utenti più si riducono le opportunità di subire violazioni; e se la cultura della sicurezza viene capita, metabolizzata e condivisa, gli utenti saranno meno portati a commettere errori. I dipendenti aziendali, demotivati a seguire certe disposizioni, infatti rappresentano una buona parte delle cause di violazioni ai dati e ai sistemi, motivo per cui i dipendenti dovrebbero sempre essere parte attiva e non passiva del meccanismo della sicurezza, questo perché non siamo tutti esperti di sicurezza e spesso non è il nostro lavoro: tutto ciò porta a una mancanza di percezione del pericolo che è forse più pericoloso.

Cyber security: l'importanza di cultura e consapevolezza

Quindi cultura, consapevolezza e comportamento conseguente sono le chiavi per iniziare un percorso decisamente più appropriato per una sicurezza globale. Tutto ciò va però aggiornato in maniera costante perché la tecnologia si evolve molto rapidamente così come tecniche e protocolli. E si parte dalla prima cosa che un utente memorizza e configura quando ha a che fare con un sistema o un computer: la password.

Venti anni fa le password che si sceglievano erano corte, scontate e di facile memorizzazione (nome della moglie, data nascita del figlio e così via). Non andavano bene allora come ora, ma i sistemi le accettavano e purtroppo anche i datori di lavoro.

Dieci anni fa era ormai una prassi scegliere le password di tipo complesso e questa era cuna configurazione che si poteva scegliere ed impostare sui sistemi perché venisse imposta agli utenti: lettere minuscole, maiuscole, numeri e caratteri speciali di lunghezza preferibilmente maggiore di 8 caratteri.

Tale tipo di password oggi viene usata come obbligatoria quasi ovunque perché sistemi, velocità di calcolo sono di molto superiori e neanche comparabili alla situazione comune degli anni passati; ciò che abbiamo imparato è che più lunga è questo tipo di password più tempo impiegheranno i malintenzionati a scovarla. Più è lunga e complessa è la password, maggiore sarà la robustezza e la impenetrabilità del sistema, e i sistemi forniscono anche una valutazione della password che stiamo usando con

Cyber security: cos'è, tipologie di attacco e difesa, questioni legali e normative

una valutazione da debole a forte.
Anche la password come sistema di difesa sta comunque facendo il suo tempo dato che macchine sempre più evolute stanno abbattendo i tempi di individuazione delle giuste combinazioni di caratteri che la formano e da qualche anno si sta insistendo perché gli utenti adottino "passphrase". Il nome è esplicativo e non servono forse ulteriori definizioni.
Studi hanno indicato che frasi, magari complesse, al posto di semplici nomi o combinazioni di caratteri anche speciali, hanno una maggiore efficacia contro i tentativi di risoluzione da parte dello stesso tipo (potenza di calcolo, architettura, metodo di risoluzione) di macchine. Potete qui vedere due esempi con le tempistiche riportate.
Fonte.
Sembra quindi che una "passphrase" potrebbe essere la soluzione per fornire ai nostri computer un cancello di accesso molto difficilmente scardinabile.
L'introduzione massiva dell'intelligenza artificiale, l'uso del cloud e di macchine in calcolo parallelo però hanno fatto sorgere il dubbio che forse anche questo metodo non sarebbe così sicuro, al punto da introdurre di pari passo anche una autenticazione a due o tre fattori.
Password o passphrase diventano solo un primo passo perché l'autenticazione ai propri sistemi (computer, online banking e via dicendo) richiederebbe un secondo passaggio mandando una richiesta al proprio cellulare o alla propria email fornita all'atto della configurazione iniziale.
Se proprio non si è contenti, e certi ambienti altamente sensibili come installazioni militari, centri di ricerca biomedica o farmaceutica già lo usano, si potrebbe aggiungere anche un passaggio con l'autenticazione biometrica (viso, retina, impronta digitale, voce, comportamentale). Questa, infatti, sarebbe di difficile falsificazione poiché il sistema di autenticazione richiederebbe passaggi dal vivo come sbattere le palpebre, girare la testa.
Altri metodi passwordless, ovvero l'uso di chiavi pubbliche e private, gettoni (token) usa e getta, chiavi USB e uso di PIN, sono attualmente molto diffusi facenti parte o meno dell'autenticazione a più fattori.
A questo punto alcuni sarebbero portati ad affermare che con un tale intervallo di tempo necessario per individuare le nostre password e anche rispetto il ritmo dell'evoluzione della tecnologia, la nostra sicurezza sarebbe garantita.
Facendo l'avvocato del diavolo si potrebbe dire: state freschi.
Un computer quantistico è una macchina che non si basa sul funzionamento seriale degli stati 1 e 0 ma che usa un QUBIT, cioè, per dirla facile e veloce, uno stato che rappresenta simultaneamente una combinazione di entrambi i valori.
Recentemente, un computer quantistico ha impiegato circa 36 microsecondi per risolvere un problema stimato come risolvibile in 9000 anni, e siamo solo agli inizi.
La domanda ora è: tra 5 anni quanto impiegherà un computer quantistico a decifrare una pass-phrase che ora è stimata risolvibile in 1 milione di anni ???
Francamente al momento non mi porrei la questione: quand'anche da domani fossero disponibili tali computer quantistici non cambierei la mia passphrase ora risolvibile in 52.000.000.000.000.000.000.000.000.000.000 di anni, sempre e comunque unita all'autenticazione a più fattori.
Architettura di sicurezza
La sicurezza va pensata, implementata, verificata giorno per giorno e aggiornata. L'impalcatura su cui regge la sicurezza, la sua architettura, deve essere soggetta a valutazioni che prendono in esame ogni singolo elemento che la compongono, dalla sua visione d'insieme (il suo scopo), alla gestione, fino all'ultimo badge che apre la porta della sala server e al singolo utente che ne fa parte (lo ricordo ancora una volta: tutti gli utenti).
La struttura che regge la sicurezza e la sua gestione devono portare ad avere un ambiente che si regge su dei postulati che al momento risultano essere BASI FONDAMENTALI per avere una sicurezza che sia degna di questo nome:
robustezza resilienza reattività
Sulla resilienza, specie dall'inizio della pandemia COVID-19, si son scritti trattati "ad nauseam" utilizzando il termine neanche fosse il sale in cucina come mai prima di allora. La resilienza nella "Supply Chain", la resilienza nello sport, la resilienza nella gestione del lock-down.... C'è di buono che almeno abbiamo imparato un vocabolo nuovo e lo stiamo usando.
Secondo Treccani, la resilienza è ".... (nella tecnologia dei materiali) la resistenza a rottura per sollecitazione dinamica, determinata con apposita prova d'urto".
Secondo IBM, e personalmente è una definizione che mi piace più delle altre perché non distingue da attacchi, crash hardware, o incidenti tellurici, "La resilienza informatica è la capacità di un'organizzazione di prevenire gli incidenti di sicurezza

Cyber security: cos'è, tipologie di attacco e difesa, questioni legali e normative

informatica, resistere ad essi ed eseguire il ripristino quando si verificano.
Una volta stabilito quali sono i caratteri identificativi della nostra sicurezza, si dovrebbe gestire tutto secondo 4 macro elementi di un progetto senza scadenza (perché tale è la gestione della sicurezza), e cioè:
valutazione iniziale, analisi dei requisiti e di fattibilità; pianificazione strategica e operativa; implementazione; valutazione finale e gestione della "produzione"; (....ricominciare dal primo punto ogni qual volta si inseriscono elementi nuovi o di aggiornamento).
Se il cuore di tutto questo nostro argomentare è rappresentato dai dati, il cuore deve pulsare per avere un dato che sia SEMPRE confidenziale integro e disponibile, il famoso acronimo C.I.A.: confidentiality, integrity, availability).
Fonte.
Tutte le azioni a contorno come, e non solo, disaster recovery, business continuity, remediation plan, fanno parte di procedure atte a stabilire un vero e proprio piano di sicurezza definito macroscopicamente in 5 passi:
Identificare, proteggere, rilevare, rispondere, ripristinare
Il NIST, ente governativo statunitense che si preoccupa di codificare standard e tecnologie, elaborò nel 2014 e ha aggiornato nel 2018, un "framework", cioè una serie di passi per implementare un piano di sicurezza informatica. Il documento è consultabile qui, qui e qui.
Talvolta, per essere alla moda guardiamo fuori da casa nostra e pensiamo che l'erba del vicino sia sempre più verde ma in casa facciamo delle cose che potrebbero e dovrebbero essere apprezzate un po' di più.
Roberto Baldoni e Luca Montanari, oggi rispettivamente direttore dell'Agenzia per la Cybersicurezza Nazionale e Senior Advisor presso Agenzia per la Cybersicurezza Nazionale, partendo dalla base fornita dal NIST, già nel 2015 avevano presentato un piano che prende in esame i passi per l'attuazione di un piano per la sicurezza informatica.
Tale piano in 120 pagine, a cura del Cyber Intelligence and Information Security Center dell'università Sapienza di Roma e del Cyber Security National Lab, secondo me è degno di menzione, come dice il commento riepilogativo, per "l'approccio alla tematica. Una metodologia intimamente legata a un'analisi del rischio e non a standard tecnologici. Una tematica di grandissima rilevanza come hanno ampiamente dimostrato il supporto del DIS (Dipartimento per le Informazioni e Sicurezza della Presidenza del Consiglio n.d.r) all'intero progetto".
Filosofia borderless
Naturalmente se si parla di approcci alla tematica e non a standard tecnologici, quindi un approccio filosofico al tema, è indifferente che si parli di reti aziendali locali, in "cloud" o ibride. Gli utenti viaggiano, usano applicazioni web o VPN, usano il laptop ma anche lo smartphone o il tablet, salvano i dati sul disco, su USB o su cloud; le aziende usano Office 365 ma hanno il ERP aziendale gestito in locale, gestiscono i soldi tramite conti bancari online, il firewall è gestito localmente e hanno una connettività MPLS con le diversi sedi italiane e/o estere. Ormai il campo d'azione è diventato immenso e non più soggetto a limiti ben definiti.
Sicurezza fisica delle infrastrutture, delle applicazioni, del cloud e dello storage, cultura degli utenti, disaster recovery, business continuity e sicurezza mobile: tutto deve essere contemplato nei piani di sicurezza informatica.
Con una tale complessità di situazioni, eccezioni, attori e tecnologie presenti sul campo, l'approccio più sensato che forse era (ed è) comune nell'àmbito dello spionaggio (cioè un approccio paranoico) è ZERO TRUST (nessuna fiducia) NETWORK: io presumo cioè che il dato sia compromesso e imposto una serie di controlli per convalidare l'autenticità e l'accesso di cose e persone, nonché le ragioni delle richieste e azioni pervenute all'ufficio IT. Dove anni fa si faceva affidamento a VPN o DMZ basandosi semplicemente su username-password, ora si "fanno le pulci" anche agli accessi che avvengono alle 02:00 quando invece è normale che avvengano tra le 08:00 e le 20:00, anche se a richiedere l'accesso è l'amministratore di rete o il CIO (Chief Information Officer).
Al già presente e non più sufficiente insieme di protocolli noti con la terna A.A.A (autenticazione, autorizzazione e accounting) si aggiunge in maniera sempre più diffusa il principio del minimo privilegio assegnato per il minor tempo possibile (least privilege), strumento rivelatosi molto efficace per il contenimento del rischio.
Questo nuovo paradigma della sicurezza che tanto coinvolge il business del campo, è anche oggetto di seminari che si possono seguire online, in diretta o in differita.
Prendendone uno ad esempio da me molto seguito, possiamo citare la divulgazione scientifica e didattica svolta dal GARR: "..rete nazionale a banda ultra-larga dedicata alla comunità dell'istruzione e della ricerca. Il suo principale obiettivo è quello di fornire connettività ad alte prestazioni e di sviluppare servizi innovativi per le attività quotidiane di docenti, ricercatori e studenti

Cyber security: cos'è, tipologie di attacco e difesa, questioni legali e normative

e per la collaborazione a livello internazionale".

L'istituzione è da tempo impegnata a diffondere la cultura della sicurezza informatica con seminari online e in presenza. Per chi fosse curioso può avere una idea della materia, della persona e della istituzione seguendo tre moduli su "ZERO TRUST: fidarsi è bene, ma non fidarsi è meglio":

Zero Trust - Fidarsi è bene, ma zero fiducia è meglio: modulo 1 - 18 ottobre 2021

Watch this video on YouTube

Zero Trust - Fidarsi è bene, ma zero fiducia è meglio: modulo 2 - 20 ottobre 2021

Watch this video on YouTube

Zero Trust - Fidarsi è bene, ma zero fiducia è meglio: modulo 3 - 22 ottobre 2021

Watch this video on YouTube

Scientifica è la preparazione ad un incidente così come scientifica deve essere la risposta che deve seguire un incidente: approccio organizzato, analitico, reattivo per affrontare e gestire le conseguenze di un incidente ma anche con l'obiettivo di prevenire una violazione o contrastare un futuro attacco informatico.

Tale attività viene svolta secondo quattro fasi principali:

preparazione; rilevamento e analisi; contenimento, eradicazione e ripristino; attività analisi post incidente.

Stesso piano, molti bersagli e molti attori

Diverso campo d'applicazione, uguale filosofia di approccio. Dopo aver definito quali caratteristiche dovrebbe avere e a quali principi dovrebbe ispirarsi, alcuni dei passi iniziali alla corretta declinazione del piano potrebbero essere i seguenti: identificare i beni dell'azienda, immateriali e le risorse tecnologiche; definire una strategia di cyber security in base all'azienda: cioè cosa faccio per proteggere la mia azienda; attuare la protezione più idonea per l'azienda: inutile forse mettere la scansione della retina in un'azienda locale con 50 dipendenti che fattura 500k euro/annui mentre magari è d'obbligo metterla in un'azienda farmaceutica con 200k dipendenti nel mondo e un fatturato di 20 mld di euro/annui; controllare regolarmente il sistema di sicurezza

Un piano indipendentemente dal settore merceologico, non curante il fatto se siamo un'azienda che fornisce consulenza di sicurezza o se siamo un ospedale, cioè indipendentemente dal fatto se possiamo svolgere il ruolo di "attaccanti" o semplici vittime.

E questo perché come si è visto nel tempo e dall'esperienza, vittime possono esserlo sia gli ospedali, le piccole amministrazioni comunali o enti governativi o aziende del settore: ENAC (2020), Luxottica (2020), SolarWinds (2021), KIA (2021), Microsoft Exchange Server (2021), solo per citarne pochissimi negli due anni.

I settori a rischio sarebbero tutti: automobilistico, finanziario, medicale e farmaceutico, governativo, militare, informatico, energetico e via discorrendo. E non solo: la gestione dei fornitori, la cosiddetta supply chain cyber security è anch'essa vitale. Se rimango senza un firewall o se una parte di ricambio tarda ad arrivare o se mi affido a discutibili fornitori (connettività, hardware o software che potrebbero installare backdoor, boe di sorveglianza o altro) la robustezza della mia catena viene meno con relative conseguenze.

La dimensione dell'azienda, il suo fatturato e il suo àmbito lavorativo, determinano (o dovrebbero determinare) solo il numero delle persone e i ruoli dedicati al suo ufficio di Sicurezza Informatica. Ma la tecnologia è così diversificata, la sua modalità d'ingaggio così variegata e i suoi aspetti molteplici, che nessuno può gestire da solo l'ufficio IT, a meno di non esternalizzare i servizi di cui ha bisogno. Le figure richieste in questo campo sono, ad esempio:

Security specialist Security Administrator Security manager Security analyst Chief information security officer (CISO) Security architect Security engineer Data Protection Officer (DPO)

Ho detto dovrebbero perché il budget riservato alla sicurezza informatica in Italia è stimato essere intorno al 10%, (2021) cresciuto leggermente nel corso degli ultimi 4/5 anni ma ancora lontano da una ragionevole percentuale, salvo poi farlo schizzare in alto esponenzialmente in caso di danni, sempre se non viene addirittura ridotto così come il personale IT (circa il 30% secondo il rapporto CLUSIT Marzo 2022 a causa del lavoro da remoto).

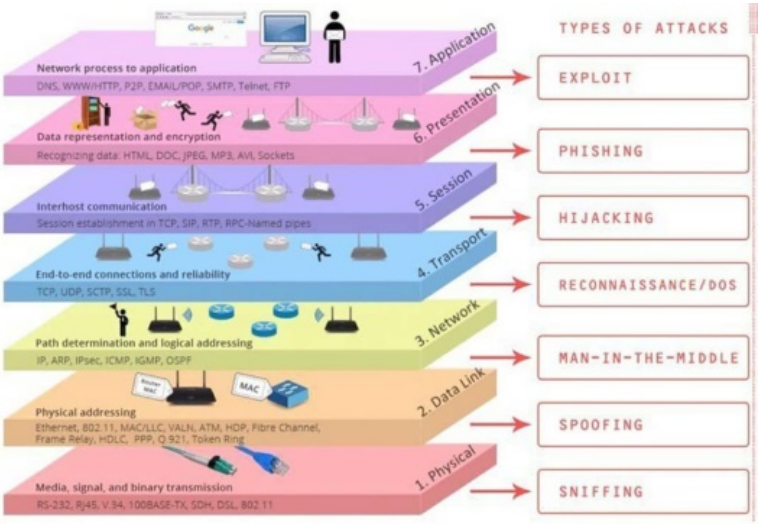
Questioni legali e normative: il ruolo delle istituzioni

Come se non bastasse tutto questo, a complicare il campo ci sono anche le questioni legali che se non sono asfissianti sono sempre ben accette.

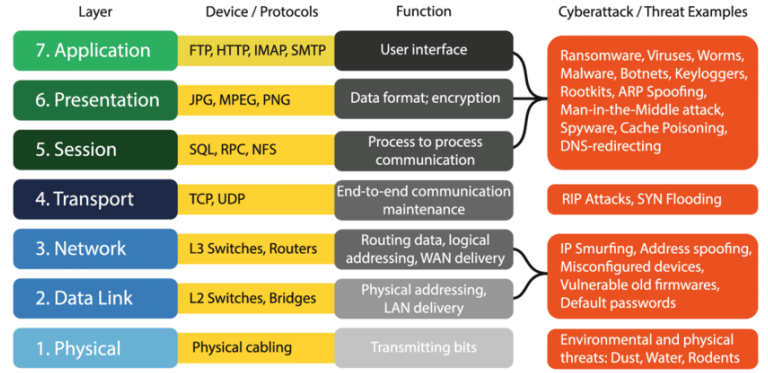
Non basta avere un genio Ethical Hacker per gestire la sicurezza in azienda, ma ci vogliono anche protocolli di gestione che forse il nostro hacker tralascerebbe.

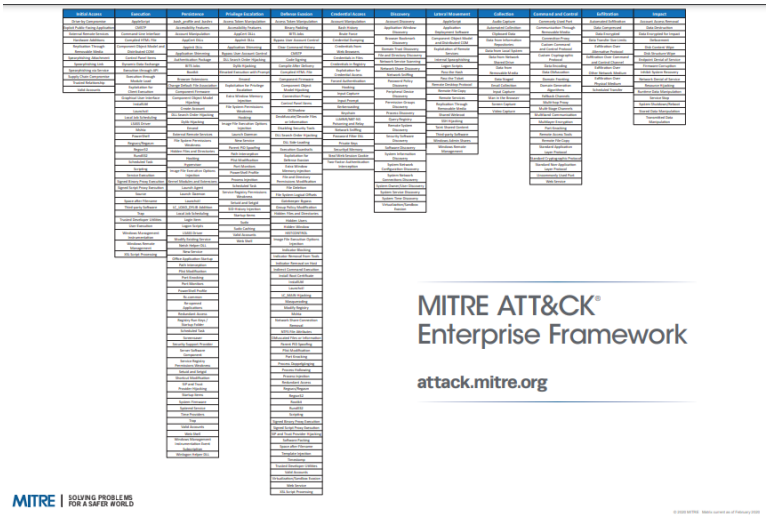
Cyber security: cos'è, tipologie di attacco e difesa, questioni legali e normative

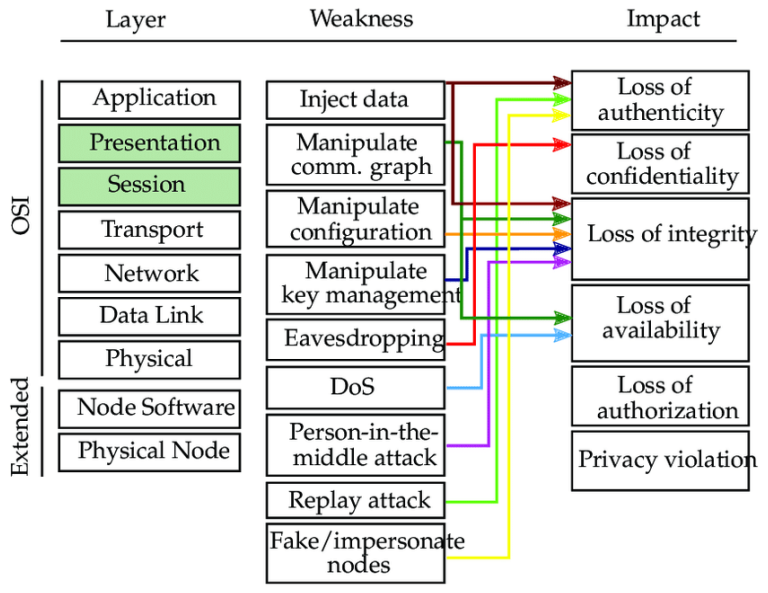
Non serve la ISO/IEC 27001 o 27701 per sapere che l'azienda deve avere i sistemi aggiornati, sistemi preposti per l'antiintrusione o la loro individuazione, fare i backup almeno in duplice copia e conservarlo in una sede che NON SIA la stessa dell'azienda. Serve però per capire ad esempio come gestire utenze ed i permessi e soprattutto come gestire i fornitori.
Non serve avere il GDPR per capire che i dati dei dipendenti non devono essere divulgati ma serve per capire che devono essere protetti con certe modalità e tempistiche.
Con l'aumentare dei casi di cyberbullismo, violazione dei dati personali, furto d'identità, globalizzazione degli scambi commerciali e diverse realtà legislative in campo, enti nazionali e sovranazionali si sono attivati per legiferare, codificare e cercare di mettere un po' di ordine: AGID, Unione Europea, Parlamento Italiano, ENISA, ACN, CINI e diverse altre e in altri paesi dell'EU similmente (ma ce ne sono altre a livello globale come il NIST ad esempio).
La pandemia COVID-19 ha messo sì in subbuglio il globo a livello organizzativo e saccheggiatolo a livello economico, ma ha portato anche aspetti positivi e dato un forte impulso a diversi settori del campo informatico a cominciare come si è detto dal livello legislativo e normativo.
Si è assistito inoltre ad un incremento del lavoro da remoto con relative conseguenze tecniche e organizzative (sembra che una buona percentuale del personale vorrebbe non tornare in ufficio o quanto meno incentivare il lavoro da casa - procedure di sicurezza), seminari di aggiornamento e percorsi di certificazione online, congressi e molto altro, spesso anche in forma gratuita.
Alla vista di tutto ciò, il ruolo delle istituzioni, siano esse governative o private, è essenziale. Norme, codici, protocolli, manuali, seminari tecnici e di consapevolezza, facilitazione della divulgazione della cultura di massa: tutto contribuisce a formare un ambiente più sicuro e affidabile.
I Servizi d'Informazione e Sicurezza come da loro compiti istituzionali e nel Quadro Strategico Nazionale hanno elaborato un piano, poi aggiornato nel 2017, che prende in considerazione rischi, cooperazione a livello internazionale, supporto allo sviluppo industriale, standard, protocolli e PROMOZIONE E DIFFUSIONE della CULTURA, quale tassello fondamentale di uno sviluppo organico della sicurezza. Lo potete leggere qui.
Inoltre, anche a livello della pubblica amministrazione, sintomo di un avvenuta ricezione non solo del messaggio ma anche della sua importanza, si sta provvedendo in tal senso, partendo naturalmente dai vertici delle istituzioni che devono dare il buon esempio e veicolare la partecipazione dei dipendenti pubblici.
La guerra cibernetica è uno strumento di pressione e d'influenza al pari della diplomazia, della armi da fuoco e degli accordi commerciali, per i più disparati motivi (politici, economici o ideologici). La sicurezza cibernetica è quindi un misto di architettura tecnologica, cultura e valutazione del rischio
Ci sono terabyte di libri, pdf e articoli che si possono consultare in merito. Ci sono decine di seminari, corsi online che si possono seguire come mai prima. Ci sono decine di attori che si possono seguire. Solo per (ri)citarne alcuni: GARR, NIST, ACN, CLUSIT, ITSEC, UNISA, NSA, SANS.
WHITEPAPER
GUIDA PRATICA contro il Phishing: scopri come tutelare la tua azienda!
CIC



Cyber security: cos'è, tipologie di attacco e difesa, questioni legali e normative







Cyber security: cos'è, tipologie di attacco e difesa, questioni legali e normative

Layer	Security Threat	Solution
Application	Static Password, SNMP Private Community Strings	Anti Virus software, OS Hardening, Patching
Presentation	Viruses, Worm	Intrusion Detection, Auditing
Session	Personal Information Retrieval, Root Privilege Access, Net Bios, DOS	Patches, Encryption, Authentication
Transport	Endpoint Identity	Firewall access control list
Network	Preventing unauthorised access to internal system	VPN network based intrusion detection and content filtering
DATA	ARP spoof, MAC Flooding	Private VLANs, Static ARP (address resolution protocol) entries, STP (Spanning Tree Protocol) root priority
Physical	Inadequate Power, Unfettered access, Open wall ports	Managed Power through UPS, Restricted Access, Close down open wall ports

Figure 1

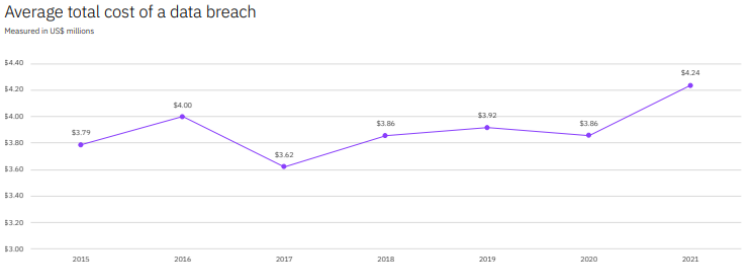
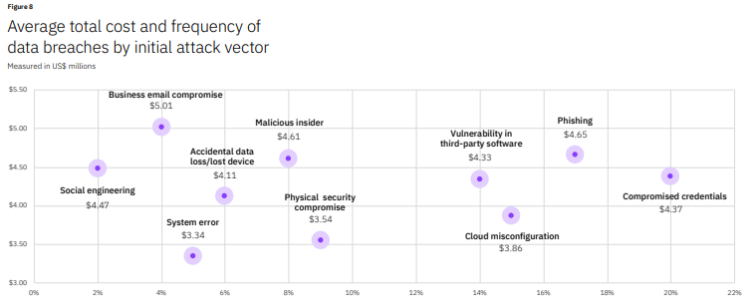


Figure 8



Cyber security: cos'è, tipologie di attacco e difesa, questioni legali e normative

Password:	tU.w@b3e	**Password:**	thisisasimplephrase
Strength:	47%	**Strength:**	89%
Evaluation:	Medium	**Evaluation:**	Excellent!

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 2 years
Fast Desktop PC	About 6 months
GPU	About 2 months
Fast GPU	About 1 month
Parallel GPUs	About 4 days
Medium size botnet	About 1 minute

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 3 trillion years
Fast Desktop PC	About 739 billion years
GPU	About 296 billion years
Fast GPU	About 148 billion years
Parallel GPUs	About 15 billion years
Medium size botnet	About 3 million years