TEMA SULLA SICUREZZA INFORMATICA

Definizione e obiettivi della sicurezza informatica

E' l'insieme dei prodotti, dei servizi, delle regole organizzative e dei comportamenti individuali che proteggono i sistemi informatici di un'azienda.
Ha il compito di proteggere le risorse da accessi indesiderati, garantire la riservatezza delle informazioni, assicurare il funzionamento e la disponibilità dei servizi a fronte di eventi imprevedibili

(C.I.A. = Confidentiality, Integrity, Availability).

L'obiettivo è custodire le informazioni con la stessa professionalità ed attenzione con cui ci si prende cura di gioielli o certificati azionari depositati nel caveau. Il sistema informatico è la cassaforte delle nostre informazioni più preziose; la sicurezza informatica è l'equivalente delle serrature, combinazioni e chiavi che servono a proteggerla.

Emma Lorin Kara

Terminologia

ASSET = l'insieme di beni, dati e persone necessarie all'erogazione di un servizio IT

VULNERABILITA' = debolezza di un asset
es. pwd = username; sensibile alle inondazioni

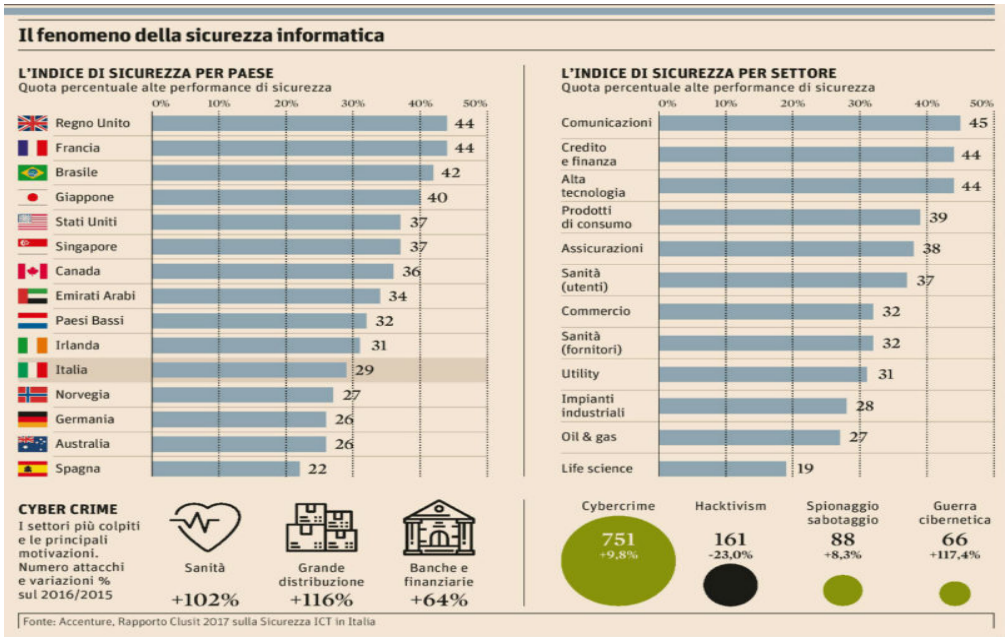
MINACCIA = evento intenzionale o accidentale che può causare la perdita di una proprietà di sicurezza

ATTACCO = verificarsi di una minaccia di tipo "evento intenzionale"

EVENTO (NEGATIVO) = verificarsi di una minaccia di tipo "evento accidentale"

Livello di sicurezza in Italia rispetto al resto del mondo

Secondo il Global Threat Impact Index di luglio di Check Point® Software Technologies Ltd., l'Italia sale di altre otto posizioni nella classifica dei Paesi più attaccati al mondo piazzandosi al 34esimo posto. Secondo una ricerca effettuata da Cybersecurity Italia, il settore della sicurezza informatica ha raggiunto un valore di 1,4 miliardi di Euro ma solo il 3% delle aziende e ' disposta a spendere per contrastare gli attacchi. Questi dati sono stati evidenziati a Milano della EY Global Information Security Survey 2018/19 attraverso un rapporto sulle tendenze in atto della cybersecurity a livello nazionale e globale. Un sondaggio smpre sullo stesso argomento e dalle stesse fonti fa emergere che solo il 14% degli itnervistati in italia ritiene che il proprio sietema di sicurezza informatica soddisfi pienamente le loro esigenze. Il 38% delle aziende su base globale e il 42,5% delle aziende italiane ha dichiarato che non riuscirebbe a identificare un attacco cyber sofisticato e il 62% delle aziende italiane ha dichiarato di aver avuto almeno un incidente significativo nel sistema di sicurezza informatica. Ad oggi la maggior parte delle aziende sta puntando su tecnologie avanzate di intelligenza artificiale, automazione di processi robotici e gli analytics, che consentono di ottimizzare la capacita' di identificare la vulnerabilita' degli attacchi. L'aspetto positivo e' che la domanda di cybersecurity in Italia e' cresciuta a partire dal 2017 del 10,8%.



Emma Lorin Kara

GDPR

A partire dal 25 maggio 2018 è direttamente applicabile in tutti gli Stati membri il **Regolamento Ue 2016/679**, noto come **GDPR** (General Data Protection Regulation) – relativo alla protezione delle persone fisiche con riguardo al **trattamento e alla libera circolazione dei dati personali**.

Il GDPR nasce da precise esigenze, come indicato dalla stessa Commissione Ue, di certezza giuridica, armonizzazione e maggiore semplicità delle norme riguardanti il trasferimento di dati personali dall'Ue verso altre parti del mondo.

In estrema sintesi col GDPR:

- Si introducono regole più chiare su informativa e consenso;
- Vengono definiti i limiti al trattamento automatizzato dei dati personali;
- Poste le basi per l'esercizio di nuovi diritti;
- Stabiliti criteri rigorosi per il trasferimento degli stessi al di fuori dell'Ue;
- Fissate norme rigorose per i casi di violazione dei dati (data breach).

Le norme si applicano anche alle imprese situate fuori dall'Unione europea che offrono servizi o prodotti all'interno del mercato Ue. Tutte le aziende, ovunque stabilite, dovranno quindi rispettare le nuove regole. Imprese ed enti avranno più responsabilità e caso di inosservanza delle regole rischiano pesanti sanzioni.

Perché il GDPR è (anche) un investimento

L'attuazione del GDPR non come un costo ma come un investimento essenziale per la tutela stessa della loro attività istituzionale e, per le aziende, della loro capacità di reggere alle sfide del mercato, anche ben oltre il rispetto del diritto.

La nostra società vive sempre più grazie ai dati e ogni giorno di più non vi sarà ramo dell'attività produttiva e dei servizi che non sia coinvolto nelle attività di Big Data, di Data analysis, di machine learning e, infine nell'uso molteplice e poliforme dell'Intelligenza artificiale e dell'Internet delle cose.

Emma Lorin Kara

Come un hacker attacca un'azienda: le 5 fasi di un attacco informatico

Per potersi realmente **difendere da attacco informatico** da parte di un hacker, bisogna conoscere in che modo può avanzare la sua strategia, fase per fase.

Ci possono aiutare in questo i *White Hacker,* dei veri e propri *Black Hat* che agiscono per aiutare le aziende a rimuovere i virus o a difendersi da eventuali intrusioni, spesso eseguendo dei penetration test nel sistema aziendale per provare la sua vulnerabilità o meno. Essi vengono definiti anche *Ethical Hacker* e possono certificarsi tramite l'EC-Council < Caution-https://www.eccouncil.org/ > .

Sono state individuate 5 fasi che un hacker segue nella sua intrusione in un sistema aziendale:

1. **Ricognizione**
2. **Scansione**
3. **Ottenere l'accesso**
4. **Mantenimento dell'accesso**
5. **Tracce di copertura**

Fase 1: ricognizione

La fase di ricognizione si riferisce a quel momento di preparazione e strategia in cui un hacker raccoglie quante più informazioni possibili sull'obiettivo prima di attaccare.

Le tecniche di ricognizione possono essere categorizzate generalmente in ricognizione attiva e in quella passiva.

Quando un attaccante utilizza tecniche di ricognizione **passiva**, non lo fa interagire direttamente con il sistema: usa informazioni disponibili pubblicamente, sfruttando la *social enginering* o il *dumpster diving* per raccogliere informazioni. Mentre la *social engineering* usa una serie di tecniche per manipolare le proprie vittime con

lo scopo di ottenere informazioni sensibili, il *dumpster diving* è il processo di ricerca attraverso il cestino di un'organizzazione per recuperare le informazioni sensibili scartate.

Quando un hacker invece utilizza tecniche di ricognizione **attive**, tenta di interagire con il sistema utilizzando strumenti per rilevare porte aperte, host accessibili, posizioni router, mappatura di rete, dettagli di funzionamento di sistemi e applicazioni.

Fase 2: scansione

La scansione è il metodo che un hacker esegue prima di attaccare la rete. Nella scansione, usa i dettagli raccolti durante le ricognizioni per identificare specifiche vulnerabilità. Spesso vengono utilizzati strumenti automatizzati come scanner di rete/host e war dialer per individuare i sistemi e tentare di scoprire le vulnerabilità.

In questo modo un hacker può raccogliere informazioni di rete come la mappatura di sistemi, router e firewall utilizzando strumenti semplici come Traceroute o Cheope.

Gli scanner di porte possono essere utilizzati per rilevare le porte di ascolto per trovare informazioni sulla natura dei servizi in esecuzione sulla macchina di destinazione. La tecnica di difesa primaria a questo proposito è quella di chiudere i servizi che non sono richiesti.

Un hacker segue una particolare sequenza di passaggi per scansionare qualsiasi rete, tuttavia i metodi di scansione possono differire in base agli obiettivi di attacco.

Fase 3: accesso

Ottenere l'accesso è la fase più importante di un attacco in termini di danno potenziale. Gli hacker non hanno bisogno di ottenere sempre l'accesso al sistema per causare danni. Ad esempio, gli attacchi denial-of-service possono esaurire le risorse o interrompere i servizi di esecuzione sul sistema di destinazione. Mentre

quest'ultimo può essere effettuato terminando i processi o anche riconfigurando e bloccando il sistema, le risorse possono essere invece esaurite localmente riempiendo i collegamenti di comunicazione in uscita.

Ad esempio l'*exploit* può avvenire localmente, offline, tramite LAN o Internet come inganno o furto.

Gli aggressori usano anche una tecnica chiamata *spoofing* per sfruttare il sistema fingendo di essere estranei o sistemi diversi. Possono usare questo tecnica per inviare un pacchetto deformato contenente un bug al sistema di destinazione in modo da sfruttare le vulnerabilità. L'inserimento di questi pacchetti può essere utilizzato per interrompere a distanza la disponibilità di importanti servizi.

I fattori che influenzano le possibilità di un hacker di accedere a un sistema di destinazione includono architettura e configurazione del sistema di destinazione, livello di abilità dell'autore del reato e livello di accesso ottenuto. Il tipo più dannoso degli attacchi è l'attacco denial-of-service (DoS), in cui un hacker utilizza un software zombie attraverso Internet su più macchine per innescare un arresto dei servizi su larga scala.

Attacco all'Unicredit Ottobre 2016

Il primo tra settembre e ottobre 2016, il secondo tra giugno e luglio 2017. È stato colpito un vasto numero di clienti, che però appartiene a una specifica categoria: quelli che hanno richiesto prestiti personali.

In una nota ufficiale: https://www.unicreditgroup.eu/it/press-media/press-releases-price-sensitive/2017/comunicato-stampa7.html

la banca precisa che *"non è stato acquisito nessun dato, quali le password, che possa consentire l'accesso ai conti dei clienti o che permetta transazioni non autorizzate. Potrebbe invece essere avvenuto l'accesso ad alcuni dati anagrafici e ai codici IBAN"*.

Sono salvi, secondo quanto emerge, i soldi dei correntisti: le informazioni sottratte non sono sufficienti per entrare nei conti correnti bancari e svuotarli, ma potrebbero essere usate in altri modi: per esempio per attacchi mirati di *phishing*, ovvero mail inviate ai clienti con il logo contraffatto della banca. Nella nota diffusa, Unicredit spiega anche che l'intrusione non è avvenuta direttamente sul sistema informativo della banca, ma attraverso un partner esterno italiano. Di che tipo di partner si tratti, al momento, non è dato sapere. Per affrontare l'emergenza, la banca ha informato le autorità competenti e ha avviato uno specifico audit sul tema. Ha inoltre presentato un esposto alla procura di Milano. La polizia postale è al lavoro per effettuare i primi accertamenti. La banca assicura inoltre di aver adottato*"tutte le* **azioni necessarie** *volte a impedire il ripetersi di tale intrusione informatica"*. Nell'ambito del recente piano industriale Transform 2019,*"il gruppo sta investendo 2,3 miliardi di euro per rafforzare e rendere sempre più efficaci i propri sistemi informatici"*.

Che tipo di attacco è stato commesso?

Possiamo solo fare ipotesi: può essere che gli hacker fossero nella rete del partner, magari hanno bucato un sito o un database, o semplicemente una casella di posta elettronica che conteneva alcune informazioni. Per ora lo scenario è ampio: può andare dall'attacco mirato alla semicasualità".

Quali sono stati i rischi per i correntisti?

"*Se fosse appurato che tra i dati sottratti ci sono solo informazioni anagrafiche, alcuni dati personali e Iban* – dichiara in un'intervista all'agenzia *Cyber Affairs* http://www.cyberaffairs.it/ Corrado Giustozzi, esperto di sicurezza cibernetica presso l'AgID (Agenzia per l'Italia digitale) - *si può dire che i conti dei clienti non corrono rischi. Semmai, il pericolo è che chi ora ha queste informazioni (...) le possa utilizzare per condurre truffe o attacchi mirati di phishing, che proprio in virtù dei dati acquisiti risulterebbero più credibili".*

La soluzione è fare ancora più attenzione.

Quali sono gli attacchi più diffusi in Italia?

Secondo un report di Kaspersky Lab si tratta proprio di attacchi di phishing finanziario: lo scorso anno il loro numero è aumentato del 13,14% rispetto al 2015, rappresentando il 47,48% di tutti gli attacchi di phishing. Anche il budget destinato alla spesa in sicurezza informatica da parte delle banche è in forte ascesa, in uno scenario di continua rincorsa. Tra tutti i tipi di phishing finanziario, quello bancario è il più diffuso. Un attacco su quattro (25,76%) ha usato false informazioni per l'online banking.

Software per la sicurezza informatica: Firewall

Firewall è un dispositivo per la sicurezza della rete che permette di monitorare il traffico in entrata e in uscita utilizzando una serie predefinita di regole di sicurezza per consentire o bloccare gli eventi.

Da oltre 25 anni, i firewall rappresentano la prima linea di difesa per la sicurezza della rete. Costituiscono una barriera tra le reti interne, sicure e controllate, e le reti esterne che possono essere affidabili o meno, come Internet.

Un firewall può essere costituito da un componente hardware, software o di entrambi i tipi.

Tipi di firewall

Firewall proxy

Uno dei primi tipi di dispositivi firewall sviluppati è il firewall proxy, che funge da gateway tra le reti per una specifica applicazione. I server proxy possono offrire funzionalità aggiuntive come il caching e la protezione dei contenuti che impediscono connessioni dirette dall'esterno della rete. Questa soluzione può tuttavia avere ripercussioni sulla velocità di trasmissione e sulle applicazioni supportate.

Firewall Stateful Inspection

Il firewall Stateful Inspection, oggi considerato un tipo di firewall "tradizionale", consente o blocca il traffico secondo regole basate sullo stato, sulle porte e sul protocollo. Monitora tutta l'attività dal momento in cui viene stabilita una connessione fino alla sua chiusura. L'applicazione del filtro viene decisa sulla base delle regole definite dall'amministratore e del contesto, ovvero su informazioni relative a connessioni precedenti e pacchetti appartenenti alla stessa connessione.

Firewall Unified Threat Management (UTM)

Un dispositivo UTM in genere combina, senza una correlazione diretta, le funzioni di un firewall Stateful Inspection con le funzionalità di prevenzione delle intrusioni e dell'antivirus. Può anche includere servizi aggiuntivi e spesso prevede la gestione tramite cloud. I firewall UTM sono concepiti per garantire semplicità e facilità di utilizzo.

Le opportunità economiche di Internet e del mercato digitale sono sempre più a rischio cyber crime. Se attuata con successo, la Strategia per il mercato unico digitale Ue promette di contribuire ben 415 miliardi di euro all'anno allo sviluppo dell'economia europea, grazie ad un migliore accesso al libero flusso di beni, dati, servizi e capitale tra paesi europei, alla creazione di nuovi posti di lavoro, ad un mercato digitale ancora più esteso ed alla progressiva trasformazione dei servizi pubblici. Paesi come la Francia, il Regno Unito, la Polonia e la Danimarca hanno perfino istituito la carica di Ministro dell'Economia Digitale, responsabile per le strategie di sviluppo e promozione del mercato digitale.

La stessa struttura di Internet – per sua natura aperta, flessibile ed in continua evoluzione – che ha permesso ai paesi di prosperare, di migliorare le operazioni governative, e facilitare l'accesso alle informazioni, ha anche esposto la nostra società a nuovi rischi tra cui l'abuso dei dati personali, l'hacktivism, la violazione della sicurezza delle infrastrutture stesse, la distruzione di servizi e proprietà digitali, e le campagne di influenza e spionaggio digitale. Più di 100 nazioni e un numero sempre più grande di attori non-statali ed individui oggi hanno le capacità di **distruggere o degradare infrastrutture critiche e servizi essenziali attraverso attacchi cibernetici** di alto impatto come la campagna di ransomware, denominata **WannaCry,** che colpì oltre 150 paesi nel maggio 2017 o il cyber attacco più distruttivo e costoso della storia, denominato NotPetya, che si diffuse rapidamente nel mondo nel giugno 2017, causando miliardi di dollari di danni. Questi attacchi hanno avuto un impatto globale significativo in termini di **perdite e danni economici**, ma in realtà i virus utilizzati in sé non erano qualcosa di particolarmente elaborato, né tanto meno sconosciuto, e infatti chi aveva un sistema operativo aggiornato non ha dovuto temere nulla da WannaCry. Il numero di attacchi mirati contro settori critici, come energia, telecomunicazioni, trasporti e sistemi finanziari, si è quasi quintuplicato negli ultimi cinque anni, un trend che mette a rischio sia la sicurezza nazionale sia il benessere economico e crescita di tutti i paesi sviluppati del mondo.

Proteggere Internet, pertanto, è un imperativo sia economico che di sicurezza nazionale. I paesi europei riconoscono che la loro infrastruttura digitale, i servizi e la diffusione di informazioni – e potenzialmente di disinformazione – sono vulnerabili alle interferenze e alla manipolazione, ma le loro strategie per proteggere il futuro della loro innovazione economica, modernizzazione e sviluppo non sempre sono allineate alle loro priorità in materia di sicurezza nazionale. Deve, invece, diventare prioritario bilanciare il bisogno di sicurezza nazionale con la necessità di avanzamento economico ed investire ugualmente nella sicurezza e nella resilienza di questa infrastruttura di base – Internet – e del suo valore e potenziale intrinseco.