al futuro dico sì

+INNOVAZIONE +SERVIZI +OPPORTUNITÀ

SICUREZZA DIGITALE

I RISCHI PRESENTI IN RETE

Sommario

SICUREZZA DIGITALE: COSA C'E' DA SAPERE

Frodi online, dati personali a rischio, violazione di privacy: sono solo alcuni dei pericoli che si possono incontrare online.
Nella categoria delle frodi online, molto comune è il phishing che non è altro che una tipologia di truffa a scapito degli utenti, solitamente effettuata tramite messaggi e posta elettronica. Molto diffuso è il phishing finanziario, ovvero falsi messaggi o email provenienti dalla banca presso cui si possiede il conto.
La stessa procedura può avvenire per siti di e-commerce o, in generale, da siti web che richiedono la registrazione e quindi l'immissione di dati come username e password. Il copione resta lo stesso: false e-mail con finti link, apparentemente per risolvere problemi di registrazione o di altra natura, da cui poi i criminali della rete effettuano il furto di dati.
La Polizia Postale avverte che con la stessa finalità di carpire dati personali, esistono altre truffe che si basano sull'infezione da parte di un virus informatico. La più diffusa è sempre il classico allegato al messaggio di posta elettronica; oltre i file con estensione .exe, i virus si diffondono celati da false fatture, contravvenzioni, avvisi di consegna pacchi, che giungono in formato .doc .pdf .
Il 2020, insieme alla pandemia da Covid-19, ha portato un considerevole aumento della criminalità informatica. Le frodi negli acquisti si sono avvalse, per esempio, di falsi annunci concernenti medicine e vaccini, prodotti per l'igiene, kit per effettuare test del virus oppure mail apparentemente inviate da un ministero che annunciavano contributi a fondo perduto da riscuotere, bonus o sospensione di imposte che rimandavano all'indirizzo internet di un sito clone.
In Italia, l'analisi del Servizio Analisi Criminale della Direzione Centrale della Polizia Criminale sull'andamento della delittuosità nel periodo della pandemia ha confermato che le truffe informatiche nel 2020 risultano superiori a quelle del 2019 del

17,8%, in controtendenza rispetto alla maggior parte dei reati commessi nel 2020.
Per quanto riguarda alcuni dati relativi alla Regione Lazio nel corso del 2020, il Compartimento Polizia Postale e delle Comunicazioni per il Lazio, nell'ambito delle truffe on line e Financial Cybercrime ha trattato 1831 casi, eseguito 33 perquisizioni e monitorati circa 7.000 spazi virtuali, principalmente siti di e-commerce e portali che offrono opere dell'ingegno o servizi di investimento.
Questi dati sono solo alcuni esempi di una cornice molto più ampia in cui di fronte alle crescenti minacce sorte in rete, divenute anche più sofisticate e pericolose data la mole di dati che si condividono online, richiede interventi mirati sia delle forze dell'ordine competenti sia dei cittadini in termini di informazione ed educazione al riconoscimento dei mezzi più comuni di frode online, al fine di proteggere i loro dati e quindi loro stessi da queste minacce.
Nelle prossime pagine saranno presentati nel dettaglio i principali fenomeni legati alla sicurezza digitale e le iniziative politiche a livello europeo e nazionale per il contrasto di tali fenomeni.

I RISCHI

FURTO DELL'IDENTITA' DIGITALE

Il furto dell'identità digitale è uno dei nuovi problemi emersi a seguito del percorso di transizione digitale avviato negli ultimi anni e che ha subito un'accelerata a causa della pandemia da COVID-19.
Il furto di identità da parte di un malintenzionato viene portato avanti per attribuire alla vittima stessa le azioni svolte dal malintenzionato.
Una problematica divenuta di assoluta rilevanza in tempi di protezione dati, soprattutto per le aziende che questi dati devono trattarli e proteggerli da minacce di ogni tipo, anche per soddisfare

a necessità di gestire correttamente i requisiti posti dal Regolamento UE sulla privacy.
Con l'avvento di Internet, il furto di identità è diventato molto più facile. Su Internet non c'è più una persona fisica che possa essere verificata; la nostra identità online è costituita esclusivamente da informazioni, facilmente riproducibili e spesso altrettanto facili da raccogliere e duplicare: indirizzi di posta elettronica, username, profili.
Internet ci permette di avere una identità, o anche tante, in questo contesto immateriale, completamente scollegate a quella nel mondo materiale. Se questo costituisce una grande libertà, dall'altra è anche una debolezza: chiunque può creare un indirizzo di posta elettronica con il nostro nome e cognome, o un profilo associato al nostro nome su un social network, mettendoci magari informazioni e foto che noi stessi abbiamo caricato su altri profili. Ma questo tipo di furto di identità è meno comune: molto più comune è invece cercare di impossessarsi di una nostra identità autentica, abusandone.
Collegare un'identità immateriale ad una persona fisica non è semplice. L'unico vero collegamento è con il possessore delle credenziali di autenticazione, tipicamente una password: chi controlla quella password controlla la nostra identità. Il malintenzionato cercherà quindi di acquisire le nostre credenziali per ottenere il controllo di una nostra identità reale, per quanto immateriale, ed utilizzarla per i propri scopi.
L'ingegneria sociale è uno dei mezzi più sofisticati - e di successo - con cui gli aggressori possono ottenere l'accesso ai dati personali e sensibili. Questi attacchi sfruttano l'errore umano e prosperano in tempi di incertezza. Tra febbraio e marzo dello scorso anno, quando le organizzazioni di tutto il mondo si sono confrontate con il primo picco della pandemia del Coronavirus, il numero di tentativi di truffa tramite gli strumenti digitali è aumentato in maniera esponenziale, in quanto gli aggressori si sono affrettati a sfruttare il periodo di paura e incertezza.

Ci sono molti metodi diversi di ingegneria sociale utilizzati dai criminali informatici per ottenere l'accesso ai dati personali: Phishing, Vishing, Smishing, Whaling e Pharming sono alcuni dei più comuni.
Difendere i tuoi dati dall'ingegneria sociale non è complicato e non deve essere costoso. Ci sono una serie di soluzioni sul mercato progettate per mantenere sicure le comunicazioni via e-mail, ma prima di poter esplorare le soluzioni, è necessario comprendere la natura del problema stesso.

PHISHING

È una particolare tipologia di truffa realizzata sulla rete Internet attraverso l'inganno degli utenti. Si concretizza principalmente attraverso messaggi di posta elettronica ingannevoli:
Attraverso una e-mail, solo apparentemente proveniente da istituti finanziari (banche o società emittenti di carte di credito) o da siti web che richiedono l'accesso previa registrazione (web-mail, e-commerce ecc.). Il messaggio invita, riferendo problemi di registrazione o di altra natura, a fornire i propri riservati dati di accesso al servizio. Solitamente nel messaggio, per rassicurare falsamente l'utente, è indicato un collegamento (link) che rimanda solo apparentemente al sito web dell'istituto di credito o del servizio a cui si è registrati. In realtà il sito a cui ci si collega è stato artatamente allestito identico a quello originale. Qualora l'utente inserisca i propri dati riservati, questi saranno nella disponibilità dei criminali.
Con la stessa finalità di carpire dati di accesso a servizi finanziari on-line o altri che richiedono una registrazione, un pericolo più subdolo arriva dall'utilizzo dei virus informatici. Le modalità di infezione sono diverse. La più diffusa è sempre il classico allegato al messaggio di posta elettronica; oltre i file con estensione .exe, i virus si diffondono celati da false fatture, contravvenzioni, avvisi di consegna pacchi, che giungono in formato .doc .pdf .

Nel caso si tratti di un c.d. “financial malware” o di un “trojan banking”, il virus si attiverà per carpire dati finanziari. Altri tipi di virus si attivano allorquando sulla tastiera vengono inseriti “userid e password”, c.d. “keylogging”, in questo caso i criminali sono in possesso delle chiavi di accesso ai vostri account di posta elettronica o di e-commerce.

I tentativi di phishing tradizionali prendono di mira centinaia o addirittura migliaia di destinatari alla volta. A causa di questo, il contenuto del messaggio è impersonale, quindi gli attacchi possono essere abbastanza facili da individuare, poiché il contenuto del messaggio non sarà sempre rilevante per il destinatario. Per esempio:

Le persone stanno interagendo con il tuo ultimo post su LinkedIn! Clicca qui per visualizzarlo.

Se il destinatario del messaggio di cui sopra non ha LinkedIn, o non ha postato di recente, capirà subito che il messaggio è fraudolento. Per questo motivo, gli aggressori hanno sviluppato un modo più sofisticato per ottenere ciò che vogliono dalle loro vittime: lo spear phishing.
Gli attacchi di spear phishing prendono di mira un utente alla volta. L'aggressore si impegna molto di più per conoscere la sua vittima, compresi i dettagli del suo ruolo lavorativo e le persone con cui si collega regolarmente. Questo permette all'attaccante di inviare una mail altamente personalizzata che è molto più difficile da rilevare.
Questi tipi di mail sono spesso abbastanza sofisticati da eludere le tradizionali soluzioni di filtraggio e richiedono un'architettura di sicurezza a più livelli per mitigare - inclusa la sicurezza a livello umano.

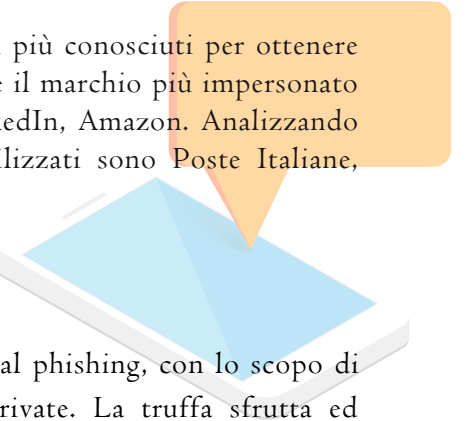
SMISHING

La parola smishing deriva dall'unione di "SMS", ovvero i messaggi di testo che si inviano tramite cellulare, e "phishing", cioè truffa. Quando i cybercriminali fanno phishing, inviano e-mail fraudolente che cercano di ingannare il destinatario inducendolo a far aprire un allegato pieno di malware o ad aprire un link dannoso. Lo stesso avviene per lo smishing, che semplicemente usa gli SMS al posto delle e-mail.

I tentativi di SMiShing generalmente seguono uno dei due modelli:

- Il truffatore incoraggia il suo obiettivo ad aprire un indirizzo web (URL) inviato in un testo. L'URL li porta poi a una pagina fraudolenta di registrazione delle credenziali o a una pagina di download che installa malware sul dispositivo dell'utente.
- Il truffatore incoraggia il suo obiettivo a chiamare un numero specificato, riguardo al contenuto del messaggio. Queste chiamate hanno come risultato che il cybercriminale richiede informazioni sensibili al telefono o sono ad un numero di telefono a tariffa maggiorata, causando all'utente una bolletta telefonica pesante.

I truffatori di solito utilizzano i marchi più conosciuti per ottenere la fiducia delle loro vittime: Microsoft è il marchio più impersonato a livello globale, seguito da DHL, LinkedIn, Amazon. Analizzando la situazione italiana, i marchi più utilizzati sono Poste Italiane, INPS e i diversi fornitori di energia.



VISHING

Il Vishing è una forma di truffa simile al phishing, con lo scopo di carpire, con l'inganno, informazioni private. La truffa sfrutta ed automatizza la persuasione tipica delle tecniche di frode ed è effettuata tramite servizi di telefonia. In particolare, gli aggressori effettuano delle telefonate simulando l'esistenza di un call center (di

una banca ad esempio) e chiedendo alla vittima di fornire i propri dati ad un operatore. Per prevenire efficacemente il vishing, è consigliabile interrompere immediatamente le telefonate che richiedono informazioni personali. Inoltre, è necessario effettuare una chiamata alla società interessata per verificare se esiste effettivamente una richiesta.
Differentemente dal phishing classico (via posta elettronica) il vishing fa leva sulla maggiore fiducia che l'essere umano tende a riporre in una persona che sembra essere autorizzata a richiedere tali informazioni.
Questa minaccia è tipica soprattutto degli Stati Uniti d'America, ma ultimamente è sbarcata nel resto dell'Europa ed anche in Italia. Un esempio di vishing è il seguente:
Salve signora, la chiamo dal suo ufficio bancario: un malintenzionato ha tentato di rubare i dati della sua carta di credito. Per maggior sicurezza, ci fornisca le sue informazioni originali, in modo da confermare che i suoi dati siano ancora protetti.

WHALING

Il whaling è il phishing per un obiettivo più redditizio. Nei tentativi di whaling, gli aggressori utilizzano tecniche di spear phishing per colpire dipendenti di alto profilo, come i dirigenti, e manipolarli per inviare bonifici di alto valore all'aggressore.
Gli aggressori possono effettuare tentativi di whaling come un attacco autonomo, o possono prendere di mira le loro "whales" (balene) tramite l'accesso a un account di posta elettronica aziendale, od ottenendo la password del proprietario dell'account usando la forza bruta, o usando l'ingegneria sociale per rubare le sue credenziali. Una volta all'interno dell'account, l'aggressore impersona il vero proprietario dell'account e manipola altri membri dell'organizzazione e i suoi stakeholder per inviare loro denaro o dati sensibili. Questa tipologia di truffa richiede più tempo per essere portata a termine, ma possono avere più successo quando

ll'e-mail proviene dall'interno della loro organizzazione ed è quindi (erroneamente!) considerata più affidabile.

PHARMING

Ultimo ma non meno importante, veniamo al pharming, noto anche come "phishing senza esca". Il pharming è una forma avanzata di ingegneria sociale in cui l'attaccante crea un sito web falso, come un portale di accesso "Microsoft", e poi inganna il server per reindirizzare i loro obiettivi a questo sito web. Una volta arrivati sulla pagina, all'obiettivo viene richiesto di inserire le proprie credenziali o informazioni finanziarie, che vengono poi inviate direttamente al truffatore. Il pharming non prende di mira una persona in particolare - semplicemente reindirizza il traffico da un sito web genuino a una pagina apparentemente identica, ma falsificata, al fine di rubare le informazioni dei visitatori.

LE STRATEGIE DI INTERVENTO E GLI STRUMENTI DI TUTELA

LA STRATEGIA EUROPEA PER LA CYBERSICUREZZA

Settori critici come i trasporti, l'energia, la salute e la finanza sono diventati sempre più dipendenti dalle tecnologie digitali per gestire il loro core business. Mentre la digitalizzazione porta enormi opportunità e fornisce soluzioni per molte delle sfide che l'Europa sta affrontando, non ultimo durante la crisi COVID-19, espone anche l'economia e la società alle minacce informatiche.
Una risposta di cybersicurezza più forte per costruire un cyberspazio aperto e sicuro può creare maggiore fiducia tra i cittadini negli strumenti e nei servizi digitali.

Nell'ottobre 2020, i leader dell'UE hanno chiesto di intensificare la capacità dell'UE di:

- proteggersi dalle minacce informatiche
- fornire un ambiente di comunicazione sicuro
- garantire l'accesso ai dati per scopi giudiziari e di applicazione della legge

I cyberattacchi e la criminalità informatica stanno aumentando in numero e sofisticazione in tutta Europa. Questa tendenza è destinata a crescere ulteriormente in futuro, dato che si prevede che 22,3 miliardi di dispositivi in tutto il mondo saranno collegati all'Internet degli oggetti entro il 2024.

L'UE sta lavorando su vari fronti per proteggere le persone e le imprese dai cyberattacchi e dalla criminalità informatica e per garantire un cyberspazio sicuro, aperto e protetto.

Analizzando i dati a livello europeo, le 5 principali minacce informatiche nel biennio 2019-2020 sono state rappresentate da:

- Malware: software maligno progettato per ottenere l'accesso a un dispositivo o danneggiarlo all'insaputa del proprietario, utilizzato anche per lo spionaggio. Il 71% delle aziende e delle organizzazioni ha sperimentato attività di malware che si diffonde da un dipendente all'altro.
- Attacchi basati sul web: varie tecniche utilizzate per reindirizzare i browser web a siti web dannosi dove possono avvenire ulteriori infezioni da malware. Gli incidenti che coinvolgono i sistemi di gestione dei contenuti (CMS) sono in aumento.
- Phishing: il tentativo fraudolento di rubare i dati degli utenti, come le credenziali di accesso o le informazioni della carta di credito, travestendosi da una fonte affidabile. Un aumento del 667% delle truffe di phishing è stato visto in un solo mese durante la pandemia di COVID-19.

- Attacchi alle applicazioni web: alimentazione di server vulnerabili e app mobili con input malevoli per ottenere dati riservati senza essere rilevati. Il 20% delle aziende e delle organizzazioni ha riportato attacchi quotidiani ai loro servizi applicativi.
- Spam: invio di messaggi non richiesti in massa - considerato una minaccia alla cybersecurity quando utilizzato come mezzo per distribuire o abilitare altre minacce. Il 66% delle minacce informatiche legate a COVID-19 provengono da e-mail di spam.

Nel dicembre 2020, la Commissione europea ha presentato una nuova strategia di sicurezza informatica dell'UE. L'obiettivo di questa strategia è quello di rafforzare la resilienza dell'Europa contro le minacce informatiche e garantire che tutti i cittadini e le imprese possano beneficiare pienamente di servizi e strumenti digitali fidati e affidabili. La nuova strategia contiene proposte concrete per il dispiegamento di strumenti normativi, di investimento e politici. Il 22 marzo 2021, il Consiglio ha adottato le conclusioni sulla strategia di sicurezza informatica, sottolineando che la sicurezza informatica è essenziale per costruire un'Europa resiliente, verde e digitale.

L'ASSETTO NAZIONALE

In Italia manca un'Agenzia nazionale per la cybersicurezza Sebbene sia presente l'AGID, l'Agenzia per l'Italia Digitale, ovvero l'Agenzia tecnica della Presidenza del Consiglio che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica, la stessa non si occupa di sicurezza digitale ed è pertanto demandata alle diverse realtà amministrative un'azione in questo settore.

Andando ad analizzare la situazione all'interno della Regione Lazio, il settore della cyber-sicurezza è stato attenzionato all'interno della nuova Agenda Digitale 2021 – 2027 della Regione Lazio, come annunciato dall'Assessore alla Trasformazione Digitale e alla Transizione Verde, Roberta Lombardi.
In particolare, gli interventi in essa previsti faranno riferimento a tre assi fondamentali: infrastrutture abilitanti (reti fisse e mobili, cloud, IA, infrastrutture di ricerca), competenze delle persone (non solo lavoratori ma anche imprenditori), accessibilità (alla rete, all'identità digitale, ai dati, alla sicurezza)".

In particolare, gli interventi in essa previsti faranno riferimento a tre assi fondamentali: infrastrutture abilitanti (reti fisse e mobili, cloud, IA, infrastrutture di ricerca), competenze delle persone (non solo lavoratori ma anche imprenditori), accessibilità (alla rete, all'identità digitale, ai dati, alla sicurezza)".
L'Agenda dovrebbe essere adottata entro il 2021 e finanziata tramite i fondi europei di sviluppo regionale, circa 320 milioni, cui vanno aggiunti i fondi previsti dal PNRR per l'attuazione, a livello regionale, delle misure.

al futuro dico sì

+INNOVAZIONE +SERVIZI +OPPORTUNITÀ

Realizzato nell'ambito delle iniziative a favore di consumatori e utenti per emergenza sanitaria da COVID-19 promosse dalla Regione Lazio, realizzate con Fondi Ministero Sviluppo Economico (riparto 2020)

ADUSBEF

ASSOUTENTI LAZIO APS

CODACONS

MOVIMENTO DIFESA del Cittadino LAZIO