“MINACCE INFORMATICHE. COME PROTEGGERE I DATI PERSONALI E ISTRUZIONI OPERATIVE PER IL PERSONALE AUTORIZZATO”

1. DESCRIZIONE DELLE PIÙ COMUNI MINACCE INFORMATICHE

Le più diffuse minacce informatiche sono rappresentate dall’attività criminale ad opera di hacker informatici, dall’azione di virus e malware, dallo spam (ovvero invio incontrollato di messaggi di posta elettronica di natura commerciale e pubblicitaria) e da tecniche di phishing, cui spesso sono associati tentativi di furto d’identità.

Attività degli hacker

Gli hacker vendono i loro servizi al miglior offerente allo scopo di recare un danno, che si può materializzare mediante: attacco verso alcuni siti, sequestro di dati, installazione di programmi malevoli per consentire il controllo di una rete, distribuire spam, lanciare attacchi di DDoS, rubare dati riservati o accedere a determinati servizi (es. home banking), ecc..

Malware: i più comuni sono virus, trojan e worm

I malware sono software malevoli del tutto autonomi o che necessitano di appropriati programmi ospite per essere eseguiti. I virus sono fatti per replicarsi e diffondersi di file a file all’interno di un PC o da un PC all’altro con lo scopo di cancellare o danneggiare i dati, i worm utilizzano la rete per diffondersi, mentre i trojan sono programmi nascosti che vengono diffusi inconsapevolmente, ad esempio effettuando il download da internet di un particolare programma di cui si necessita.

Ransomware

Il ransomware non compromette il funzionamento del dispositivo, ma rende non più disponibili i documenti contenuti nei file (immagini, musica, dati, ecc.), che vengono infatti criptati mediante appositi algoritmi di cifratura. Lo sblocco dei documenti può avvenire solo a seguito del pagamento di un riscatto preferibilmente in bitcoin.

Spam

Con questo termine s’intendono tutte quelle operazioni che in genere ostacolano la possibilità di comunicazione; più specificatamente consiste nell’invio o ricezione di posta elettronica contenente messaggi pubblicitari non richiesti. Allo spam può anche essere associata la proposta di materiale illegale e esso può celare delle vere e proprie truffe, come proposte commerciali discutibili o richiesta di dati personali (in particolare credenziali di autenticazione per ‘accesso telematico alla propria banca, o altro….).

Phishig

Cos’è

Il termine “phishing” allude all'uso di tecniche sempre più sofisticate e basate sull’ingegneria sociale per "pescare" dati finanziari e password di utenti, i quali, fornendo i dati richiesti “dal pescatore fraudolento”, “cadono letteralmente nella rete”. Insomma si tratta di una frode informatica finalizzata ad ottenere dati personali come: password, codici fiscali, informazioni relative ai conti bancari o alle carte di credito. Può concretizzarsi a danno di persone o di organizzazioni (aziende, enti, PA, ecc.).

Come si realizza

Le e-mail rappresentano senz’altro il vettore principale utilizzato dai criminali hacker per condurre i loro attacchi phishing, ma oltre ai messaggi, possono essere utilizzati anche diverse piattaforme e canali (phishing telefonico o via SMS, phishing via WhatsApp e Facebook).

La tecnica più diffusa per portare a termine un attacco di phishing, è quella classica che si attua attraverso l’invio di una grande quantità di e-mail a nome di istituti di credito, finanziari, assicurativi, tramite l’utilizzo di loghi contraffatti o indirizzi di posta verosimili, che sembrano essere riferiti ad

aziende, siti autorevoli o addirittura ad enti pubblici. L'utente può essere invitato ad inserire le proprie informazioni riservate su un sito web fasullo, apparentemente uguale a quello vero, per accedere al quale è inviato nella email un apposito link. **Oppure il messaggio di phishing invita a fornire direttamente i propri dati personali.**

2. COME PROTEGGERSI DALLE MINACCE

- Utilizzare i firewall
- Usare un efficace antivirus e anti-malware da aggiornare periodicamente
- Programmi e gestori di posta elettronica hanno spesso sistemi di protezione che indirizzano automaticamente nello spam la maggior parte dei messaggi di phishing: è bene controllare che siano attivati e verificarne le impostazioni
- Non fornire in chat o condividere in modo incontrollato i propri dati personali. Il proprio indirizzo di posta elettronica è un dato personale e deve essere utilizzato con molta prudenza
- Non cliccare su link contenuti nei messaggi ed in generale non fidarsi mai di mail ordinarie che contengono link
- Non aprire gli allegati di posta, senza prima averli fatti esaminare dall'antivirus. In questi casi, oltre al semplice phishing, potrebbero nascondersi virus dietro quei file
- Non fornire mai i propri dati personali ad esterni (anche se il loro nome può sembrare riferito ad un soggetto autorevole), che semplicemente li richiedono, senza alcuna autorizzazione verificata, anche se il soggetto richiedente può apparire attendibile, perché ad esempio l'autore della frode può celarsi dietro il nome di una PA, di un Istituto di Credito o un operatore tecnico incaricato dal MI o dalla stessa Amministrazione, ecc.
- Attenzione ad alcuni elementi caratteristici che sono riportati nei messaggi. I messaggi di phishing sono progettati per ingannare e spesso utilizzano imitazioni realistiche dei loghi o addirittura delle pagine web ufficiali di banche, aziende ed enti
- Se non si dispone di sistemi di autenticazione forte, scegliere password abbastanza sicure dotate di una certa complessità (ad esempio 14 caratteri alfanumerici) e non comunicarle a nessuno
- Scegliere password diverse per ogni servizio utilizzato
- Fare attenzione anche al tipo di richiesta, che appare spesso non fondata in questi casi, e quindi deve destare immediatamente dei dubbi, in quanto la PA, la Banca o altri non hanno certamente bisogno di dati che già detengono o comunque non effettuerebbero mai una richiesta attraverso una banale email o un form di raccolta automatica dei dati
- Effettuare copie di backup

OCCHIO AGLI INDIRIZZI E-MAIL

- Diffidare dei messaggi che contengono anche grossolani errori grammaticali, di formattazione o di traduzione da altre lingue
- È utile anche prestare attenzione al mittente (che potrebbe avere un nome vistosamente strano o eccentrico) o al suo indirizzo di posta elettronica (che spesso appare un'evidente imitazione di quelli reali)
- Meglio diffidare dei messaggi con toni intimidatori, che ad esempio contengono minacce di chiusura del conto bancario o del servizio utilizzato, di sanzioni se non si risponde immediatamente: possono essere subdole strategie per spingere il destinatario a fornire informazioni personali

CONSIGLI PRATICI PER DIFENDERSI

Tenere bene presente che i comportamenti errati, dettati da una certa superficialità degli utenti o anche dalla negligenza in alcuni casi, rappresentano una notevole fonte di pericolo, che diventano determinanti nella valutazione dei rischi totali per la protezione dei dati personali e la sicurezza dei sistemi. Il 90 % delle perdite dei dati avviene per cause accidentali (invio di informazioni a destinatari sbagliati, smarrimento di supporti, PC lasciati incustoditi, carta abbandonata sulle scrivanie, ecc.) ed il 60 % degli episodi di violazione è legata ad un fattore umano (utilizzo di password deboli o addirittura banali, e utilizzabili da soggetti non autorizzati).