Legione Carabinieri Emilia Romagna
Comando Provinciale di Bologna
Reparto Operativo – Nucleo Investigativo

COME DIFENDERE ADEGUATAMENTE LE IMPRESE DA TRUFFE DA PARTE DELLA CRIMINALITÀ CHE OPERA SU SISTEMI INFORMATICI E CON MEZZI FRAUDOLENTI DI PAGAMENTO

RELATORE: Ten. Col. Diego Polio

- Comandante del Nucleo Investigativo di Bologna;
- laurea in Giurisprudenza e Scienze della Sicurezza interna ed esterna;
- arruolato nel 1998, incarichi operativi dal 2005, dal 2010 in Emilia Romagna, precedentemente 5 anni in Sicilia;
- 42 anni, originario di Genova;
- figlio di commercianti.

SOMMARIO

1. Sicurezza informatica: cosa è e come applicarla in azienda;
2. riconoscere e prevenire le truffe informatiche moderne;
3. darkweb: il lato oscuro di internet e la truffa del CEO;
4. frodi e falsificazione dei mezzi di pagamento. Nuova direttiva UE.

La minaccia riguarda tutti!!

Sicurezza informatica: cosa è e come applicarla in azienda

- assicurare un'adeguata protezione dei propri dati digitali e processi produttivi;
- le falle di una rete aziendale sono spesso determinate da comportamenti e azioni del personale dipendente, a volte involontariamente, tal altre no (c.d. "attacchi interni")

Sicurezza informatica: cosa è e come applicarla in azienda

Errore umano

Violazione dati e sistemi

Poca accuratezza

Sicurezza informatica: cosa è e come applicarla in azienda

Introduzione di BEST PRACTICE:

- vademecum o regolamento aziendale;
- monitoraggio del flusso dei dati;
- mappatura dei dati e delle attività di trattamento (livelli di rischio ➡ misure)
- software di rilevamento e prevenzione delle intrusioni;
- firewall, antivirus, antispam e antispyware

Riconoscere e prevenire le truffe informatiche moderne

- Attacchi Phishing;
- truffe Spear Phishing;
- Truffe esca;
- Truffe di supporto tecnico;
- Proteggere i dispositivi mobili.

Riconoscere e prevenire le truffe informatiche moderne

Attacchi Phishing

Si tratta di comunicazioni – via e-mail, telefono, messaggio, ecc.- con cui i criminali informatici fingono di essere qualcun altro, con l'intento di estorcere o accedere a credenziali, dati personali o informazioni finanziarie dell'individuo colpito, o informazioni sensibili relative all'organizzazione per cui il soggetto colpito lavora.

Riconoscere e prevenire le truffe informatiche moderne

Attacchi Phishing

- Controllate i nomi dei contatti;
- cercate errori ortografici e grammatica scadente;
- fate attenzione a un atteggiamento aggressivo.

Riconoscere e prevenire le truffe informatiche moderne

Truffe Spear Phishing

I truffatori di spear phishing conducono ricerche approfondite sulle loro vittime e prendono il tempo per conoscerne l'azienda, i colleghi, gli interessi, ecc. al fine di aumentare le probabilità di successo.

Riconoscere e prevenire le truffe informatiche moderne

Truffe Spear Phishing

- usate un servizio di verifica email;
- siate discreti quando date informazioni personali;
- mantenete una corretta security-hygiene.

Riconoscere e prevenire le truffe informatiche moderne

Truffe esca

Puntano ad adescare utenti ignari portandoli a eseguire una determinata azione, come il download di un virus o l'inserimento di informazioni personali in cambio "dell'esca".

Riconoscere e prevenire le truffe informatiche moderne

Truffe esca

- Evitate offerte “gratuite”;
- evitate unità flash o hard disk esterni sconosciuti.

Riconoscere e prevenire le truffe informatiche moderne

Truffe di supporto tecnico

I truffatori si proporranno come dipendenti del supporto tecnico per l'azienda della vittima o per un servizio indipendente, con l'obiettivo di ottenere informazioni personali.

Riconoscere e prevenire le truffe informatiche moderne

Truffe di supporto tecnico

- Attenzione ai messaggi indesiderati;
- evitate di installare qualsiasi cosa proveniente da una fonte sconosciuta;
- attenzione agli accessi da remoto al dispositivo.

Riconoscere e prevenire le truffe informatiche moderne

Proteggere i dispositivi mobili

Applicazioni fasulle utilizzate per estrarre dati o ransomware sono oggi comunemente disponibili, soprattutto per i sistemi operativi Android.

Riconoscere e prevenire le truffe informatiche moderne

Proteggere i dispositivi mobili

- Occhio ai malware mascherati da applicazioni e aggiornamenti legittimi;
- usate un WiFi sicuro.

Darkweb: il lato oscuro di internet e la truffa del CEO

Dark web: cos'è, come funziona e…perché esiste.

Per definire il Dark web potremmo utilizzare il termine "lato oscuro di internet", un mondo sconosciuto ai più, dove per entrare in contatto con il sistema bisogna avere un po' di pratica informatica.

Darkweb: il lato oscuro di internet e la truffa del CEO

Dark web: cos'è, come funziona e…perché esiste.

Esiste perché tutta una serie di persone o associazioni più o meno legali vogliono rimanere anonime. All'interno di questo sistema si possono acquistare oggetti, servizi al 90% non legali, quali droghe, armi, crimeware, criptovalute, passaporti e documenti falsi, organi umani e quant'altro di lecito e illecito ci possa essere.

Darkweb: il lato oscuro di internet e la truffa del CEO

Perché questa rete virtuale parallela ci espone a rischi?

Scaricare file o navigare all'interno di queste pagine comporta un'altissima possibilità di rimanere infettati da virus o malware che possono creare non pochi problemi al privato o all'azienda che vi accede.

Darkweb: il lato oscuro di internet e la truffa del CEO

Perché questa rete virtuale parallela ci espone a rischi?

Ad esempio, la resa pubblica di un prodotto che sta per essere brevettato dall'azienda a causa di un malware, o il furto di dati personali quali carte di credito, documenti, certificati medici. Tutti questi dati, una volta rubati, vengono poi venduti nel Dark web.

Darkweb: il lato oscuro di internet e la truffa del CEO

“La truffa del CEO”: di cosa si tratta e come fare per arginare i danni.

In pratica le aziende sono vittime di furto digitale di documenti, contratti, preventivi e email aziendali, che spesso vengono venduti nel Dark web.

Darkweb: il lato oscuro di internet e la truffa del CEO

“La truffa del CEO”: di cosa si tratta e come fare per arginare i danni.

Le associazioni criminali acquistano le email rubate, leggono tutto il contenuto e cercano di capire le dinamiche aziendali interne. In questo modo, sostituendosi all’amministratore delegato, possono così iniziare a comunicare con coloro che dispongono i bonifici (spesso quindi le figure amministrative).

Frodi e falsificazione dei mezzi di pagamento. Nuova direttiva UE.

Il Parlamento e il Consiglio dell'Unione Europea hanno adottato la direttiva 2019/713, pubblicata in Gazzetta Ufficiale il 10 maggio 2019.

"Relativa alla lotta contro le frodi e le falsificazioni dei mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio".

Frodi e falsificazione dei mezzi di pagamento. Nuova direttiva UE.

Le norme del provvedimento eurounitario definiscono, pertanto, l'utilizzazione fraudolenta di strumenti di pagamento, sia materiali che immateriali, diversi dai contanti, ossia quando questi siano rubati o altrimenti illecitamente ottenuti o, altresì, siano contraffatti o falsificati.

Frodi e falsificazione dei mezzi di pagamento. Nuova direttiva UE.

La detenzione e la diffusione, al fine di un utilizzo in maniera fraudolenta, di tali mezzi di pagamento integrano delle fattispecie di reato.

L'effettuazione o l'induzione di un trasferimento di denaro è illecita, se commessa intenzionalmente, nei casi in cui si ostacoli il funzionamento di un sistema di informazione o si interferisca con esso, oppure s'introducano o si alterino dati informatici senza diritto.

Domande??

Grazie per l’attenzione!