Co-funded by the Erasmus+ Programme of the European Union

Modulo di formazione InCyT

Sicurezza delle informazioni per manager Unità 3 - Settimane 5 Nome dell'unità (modulo): Gestione della sicurezza delle informazioni 3	
Attività di apprendimento	❑ **Webinar**❑ **Esercitazioni**❑ **Workshop**❑ **Presentazione**❑ **Altro**
Apprendimento responsabile	• George Matache e altri.
Obiettivi dell'attività di apprendimento	1 Terminologia generale 2. Riservatezza, integrità e disponibilità (CIA) 3. Regole e standard 4. Gestione della sicurezza delle informazioni 5. Come funziona il malware? 6. Le principali minacce informatiche 7. Tipi di attacchi 8. Server Web sicuro - SSL 9. Invio e ricezione di e-mail 10. Gestione del patrimonio
Competenze da acquisire	-Sicurezza di reteTS3 -TS4 Test di penetrazione (vulnerabilità sfruttabili) - SS3 Analisi cognitiva e del comportamento
Durata dell'attività di apprendimento	2 settimane
Apprendimento requisiti	***Cosa serve?***
	• Accesso a Internet • Browser Internet • MS Office365

Informazioni sintetiche sul modulo

Descrizione
La sicurezza informatica è la pratica di difendere computer, server, dispositivi mobili, sistemi elettronici, reti e dati da attacchi dannosi. È nota anche come sicurezza informatica o sicurezza delle informazioni elettroniche. Il termine si applica a diversi contesti, dalle aziende al mobile computing, e può essere suddiviso in alcune categorie comuni. Spesso le aziende sono così preoccupate delle loro operazioni quotidiane che dimenticano di investire pesantemente nella sicurezza della rete. Altre comprendono la necessità di una sicurezza di rete completa, ma adottano una strategia indulgente nei confronti dell'IT, che può essere altrettanto dannosa in caso di fuga di dati. Capire cosa comporta la sicurezza di rete e quali sono le migliori pratiche da seguire per garantire che la rete aziendale sia al sicuro dalle numerose minacce esterne che cercano di infiltrarsi nella rete è essenziale per mantenere al sicuro i dati e, in ultima analisi, l'azienda. È estremamente importante che la formazione sulla sicurezza informatica per le PMI - manager e dipendenti - sia concreta e interattiva, oltre che pratica, perché le piccole PMI non hanno tempo, motivazione e risorse da dedicare a questo tema, per cui è molto importante che la formazione sia rilevante e gestibile per i manager che vi partecipano. Per questo motivo, il presente modulo è stato progettato sulla base di queste considerazioni. La gestione della sicurezza delle informazioni (ISM) definisce e gestisce i controlli che un'organizzazione deve implementare per garantire la protezione della riservatezza, della disponibilità e dell'integrità delle risorse da minacce e vulnerabilità. Malware, o "software dannoso", è un termine generico che descrive qualsiasi programma o codice dannoso per i sistemi. Ostile, intrusivo e intenzionalmente cattivo, il malware cerca di invadere, danneggiare o disattivare computer, sistemi informatici, reti, tablet e dispositivi mobili, spesso assumendo il controllo parziale delle operazioni di un dispositivo. Come l'influenza umana, interferisce con il normale funzionamento. Le motivazioni alla base del malware sono diverse. Il malware può avere lo scopo di fare soldi, sabotare la capacità di lavorare, fare una dichiarazione politica o semplicemente vantarsi. Sebbene il malware non possa danneggiare l'hardware fisico dei sistemi o delle apparecchiature di rete, può rubare, crittografare o cancellare i dati, alterare o dirottare le funzioni principali del computer e spiare le attività del computer senza che l'utente lo sappia o ne abbia il permesso.

Il malware viene descritto e definito, introducendo i suoi diversi tipi e spiegando come funziona. Vengono inoltre descritti i segnali di allarme di un dispositivo infetto e viene spiegato come prevenirlo. I discenti possono essere informati su questi aspetti leggendo il testo corrispondente, guardando i webinar in streaming e risolvendo esercizi al proprio ritmo e attraverso l'interazione con il pubblico dal vivo con feedback continuo e verifica delle conoscenze tramite gamification.

Contenuto del materiale didattico

Soprattutto se avete un'azienda che dipende molto dal funzionamento e dalla sicurezza dei vostri sistemi IT. Le minacce alla sicurezza informatica sono in aumento.

Gli attacchi informatici hanno continuato ad aumentare nell'UE nel 2020 e nel 2021 e soprattutto nel 2022, sia in termini di sofisticazione e numero, sia in termini di impatto. L'UE sta lavorando su diversi fronti per proteggere i cittadini e le imprese dalla criminalità informatica e per garantire un cyberspazio sicuro, aperto e protetto.

Nel 2022 vedremo gruppi sponsorizzati dallo Stato prendere di mira il settore delle criptovalute, mentre i criminali informatici approfitteranno degli investitori creando portafogli digitali con backdoor incorporate. È probabile che si assista a un aumento degli attacchi contro i sistemi di pagamento e a minacce mobili più avanzate.

Prendendo in considerazione uno degli Stati membri del progetto, si ha che circa la metà (47%) della popolazione di età compresa tra i 16 e gli 89 anni ha avuto a che fare con la criminalità informatica sotto forma di e-mail false, frodi, hacking o furto di identità. Lo stesso vale per l'11% delle aziende private. L'8% delle aziende ha subito il blocco dell'accesso ai servizi digitali e il 3% ha subito la cancellazione o la distruzione dei dati. Il phishing è il problema più diffuso, ma purtroppo assistiamo anche a un aumento radicale del numero di siti web falsi, dato che sempre più persone fanno acquisti e lavorano da casa.

Il nucleo dell'ISM comprende la gestione del rischio informativo, un processo che prevede la valutazione dei rischi che un'organizzazione deve affrontare nella gestione e nella protezione degli asset, nonché la divulgazione dei rischi a tutti gli stakeholder appropriati. Ciò richiede una corretta identificazione e valutazione degli asset, compresa la valutazione del valore della riservatezza, dell'integrità, della disponibilità e della sostituzione degli asset. Nell'ambito della gestione della sicurezza delle informazioni, un'organizzazione può implementare un sistema di gestione della sicurezza delle informazioni e altre best practice contenute negli standard ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27035 sulla sicurezza delle informazioni. Tuttavia, questo tipo di certificazione è

spesso troppo impegnativo per le PMI, per cui ci prepariamo a una pratica agile della sicurezza informatica:

Sicurezza delle informazioni e sistemi di controllo interno

- Terminologia generale
- Triade della CIA
- Anatomia di un attacco (riduzione della superficie di attacco)
- Quadri di sicurezza informatica

Gestione della sicurezza delle informazioni
Email e ufficio
Dispositivi
Una sfida fondamentale per le PMI è rappresentata dalle minacce informatiche, termine che indica qualsiasi tipo di "software dannoso" progettato per infiltrarsi nel dispositivo dell'utente a sua insaputa. Esistono molti tipi di malware, ognuno dei quali opera in modo diverso per raggiungere i propri obiettivi. Tuttavia, tutte le varianti di malware condividono due caratteristiche: sono subdole e lavorano attivamente contro i vostri interessi.

Il malware è un virus? Sì e no. Mentre tutti i virus informatici sono malware, non tutti i malware sono virus. I virus sono solo un tipo di malware. Si sente spesso usare i due termini in modo intercambiabile, ma da un punto di vista tecnico, virus e malware non sono la stessa cosa.
Vedetela in questo modo: Il malware è un codice maligno. I virus informatici sono codici dannosi che si diffondono attraverso i computer e le reti.

Come funziona il malware?

Tutti i malware seguono lo stesso schema di base: L'utente scarica o installa inconsapevolmente il malware, che infetta il dispositivo.

La maggior parte delle infezioni da malware si verifica quando si esegue inavvertitamente un'azione che provoca il download del malware. Questa azione può essere fare clic su un link in un'e-mail o visitare un sito Web dannoso. In altri casi, gli hacker diffondono il malware attraverso servizi di condivisione di file peer-to-peer e pacchetti di download di software gratuiti. Incorporare un po' di malware in un torrent o in un download popolare è un modo efficace per diffonderlo in un'ampia base di utenti. I dispositivi mobili possono essere infettati anche tramite messaggi di testo.

Un'altra tecnica consiste nel caricare il malware nel firmware di una chiavetta USB o di un'unità flash. Poiché il malware viene caricato sull'hardware interno del dispositivo (anziché sulla sua

memoria di file), è improbabile che il dispositivo lo rilevi. Per questo motivo non bisogna mai inserire nel computer un'unità USB sconosciuta.

Una volta installato, il malware infetta il dispositivo e inizia a lavorare per raggiungere gli obiettivi degli hacker. Ciò che distingue i vari tipi di malware è il modo in cui agiscono. Come funziona il malware? Che cos'è un attacco malware?

Le principali minacce informatiche

Gli exploit drive-by possono sfruttare automaticamente le vulnerabilità esistenti nel software installato su un PC senza interagire con l'utente legittimo; nel 2012 hanno esteso il loro campo di applicazione anche ai terminali mobili. si concentra quasi esclusivamente sulla compromissione di siti web legittimi. le vulnerabilità del browser, dei suoi plugin o del sistema operativo possono essere sfruttate per installare malware sul PC all'insaputa dell'utente l'infezione può essere avviata dalla semplice navigazione in Internet.
I worm sono programmi autoreplicanti; utilizzano la rete di computer per inviare le proprie copie ad altri nodi (computer della rete), riuscendo a farlo senza l'intervento di alcun utente; a differenza di un virus informatico, un worm informatico non ha bisogno di essere collegato a un programma esistente, ma provoca danni alla rete, anche solo occupando banda.

I trojan si presentano sotto forma di programmi legittimi che, in realtà, sono creati con l'obiettivo di rubare dati riservati o di consentire a utenti o programmi non autorizzati di accedere al sistema infetto; costituiscono la stragrande maggioranza delle infezioni (80%).

Il malware è un programma la cui funzione è quella di causare danni al software o all'hardware di un computer (ad esempio, i virus), come descritto in precedenza.

I track ware sono programmi che sfruttano alcune vulnerabilità dei browser web per inviare a un server o a persone informazioni sui siti visitati, sulle informazioni ricercate e sulle abitudini di navigazione dell'utente; i virus mirano a infettare il maggior numero possibile di personal computer, mentre gli spyware mirano a diffondersi su Internet, i virus hanno solitamente un payload pericoloso, vogliono causare danni al computer infetto, mentre gli spyware si limitano a rallentare i processi del computer, ad aggiungere popup, a destabilizzare il browser e ad avere altri effetti "fastidiosi".

L'iniezione di codice (SQL Injection) si verifica quando un aggressore può inserire qualsiasi dato in una query SQL inviata a un database; iniettando la sintassi, la logica dell'istruzione viene modificata in modo da eseguire un'azione diversa, è la vulnerabilità più comune. La migliore strategia di difesa

contro le SQL injection si basa sull'implementazione di solide routine di convalida dell'input, in modo che l'attaccante non possa inserire dati diversi da quelli necessari all'applicazione.

Lo spyware è generalmente definito come un programma che sfrutta le vulnerabilità di un sistema a vantaggio di una terza parte; può rallentare il computer, renderlo vulnerabile all'infezione di virus e raccogliere informazioni riservate come nomi utente per varie applicazioni, password e informazioni su carte di credito/conti bancari.

Un keylogger è un piccolo programma "intelligente" che gli hacker inseriscono nel vostro computer senza che ve ne accorgiate. Qui può rimanere per diversi mesi o anni e tenere d'occhio ogni singolo tasto premuto sulla tastiera. Tutti i dati vengono inviati agli hacker, che possono quindi utilizzare diversi algoritmi e strumenti per ottenere il meglio dai vostri dati. Nel corso del tempo, scoprono diverse cose sul vostro comportamento e, non da ultimo, dove utilizzate le diverse password che avete digitato sulla tastiera. Questo può essere utilizzato per impadronirsi della vostra intera identità digitale in pochi minuti.

L'adware è una sottocategoria dello spyware ed è un programma che pubblicizza prodotti o servizi. Spesso questi annunci appaiono anche dopo che il programma è stato disinstallato.
I kit di exploit sono software automatizzati che aiutano gli aggressori meno esperti a compromettere i sistemi sfruttando le vulnerabilità del lato client, in particolare quelle dei browser web o delle applicazioni a cui si può accedere dai siti web; si basano su attacchi drive-by download, in cui il codice dannoso viene iniettato nei siti web compromessi; possono sfruttare le vulnerabilità del browser o dei suoi plugin.

La botnet rappresenta un insieme di computer sotto il controllo di un aggressore; una botnet può essere utilizzata per molteplici scopi: Attacchi DDoS (Distributed Denial of Service), spamming, furto di identità, distribuzione di malware, infezione di sistemi informatici; possono essere eseguite su più sistemi operativi; nel 2012 la botnet "Flashback" è riuscita a infettare circa 600.000 computer Apple.

Il Denial of Service è un tentativo di compromettere la disponibilità di sistemi/servizi informatici o di comunicazioni elettroniche. Il sistema bersaglio viene attaccato inviando un numero molto elevato di richieste illegittime, che consumano le sue risorse hardware o software, rendendolo indisponibile agli utenti legittimi. Le motivazioni principali degli attacchi DDoS sono l'hacktivismo, il vandalismo e la frode. Compromissione di informazioni riservate; si riferisce a violazioni della sicurezza dei dati che si sono verificate attraverso la divulgazione (intenzionale o meno) di informazioni riservate da parte di agenti interni o esterni; la fuga di informazioni è solitamente ottenuta tramite hacking, distribuzione di malware, attacchi di ingegneria sociale, attacchi fisici o abuso di privilegi.

Un caso particolare di rogue ware/scareware è un falso software di sicurezza che, una volta installato nel sistema, fornisce falsi avvisi di sicurezza e invita l'utente ad acquistare uno speciale strumento di disinfezione. Questo tipo di minaccia si propaga attraverso vari metodi, quali tecniche di social engineering, trojan, sfruttamento di vulnerabilità (soprattutto java).

Il ransomware è una delle forme più pericolose e aggressive di criminalità informatica. Gli hacker utilizzano un codice estremamente complesso per bloccare la funzionalità di un computer o di un sistema controllato dal computer. Il proprietario del sistema viene quindi contattato dall'hacker con la richiesta di un riscatto per riattivare il sistema o "sbloccare" le informazioni in esso contenute. Nei casi più lievi si tratta di foto di famiglia o dei conti dell'azienda, nei casi più gravi può trattarsi di sistemi vitali, come i sistemi di controllo delle fabbriche o un pacemaker collegato a Internet.

Tipi di attacchi

Attacchi mirati

-Puntano su una persona o un'organizzazione specifica

-mirano a raccogliere dati personali/confidenziali o a compromettere i sistemi informatici dell'obiettivo

-in genere hanno una fase in cui l'attaccante si informa attraverso varie tecniche (ad esempio di social engineering) sul sistema informatico preso di mira e poi scatena l'attacco

-Spesso le sue azioni appaiono legittime perché sembrano provenire da una persona affidabile.

Furto/Smarrimento/Distruzione fisica

-A causa della maggiore mobilità offerta da laptop, smartphone o tablet, questo tipo di minaccia sta per diventare una minaccia importante.

-Il backup coerente dei dati e la crittografia dei contenuti possono essere una soluzione per limitare l'effettiva perdita di dati o la divulgazione di dati riservati a estranei.

Furto d'identità

-È una minaccia reale in un ambiente sempre più online.

-Le credenziali di accesso o i dati personali sono oggi l'obiettivo degli aggressori.

-Una volta in possesso di tali dati, l'aggressore può effettuare transazioni fraudolente (soprattutto finanziarie) o ottenere dati riservati.

Fuga di informazioni

-Divulgazione intenzionale o non intenzionale di informazioni a persone non autorizzate.

-Informazioni come la geolocalizzazione e i contatti della rubrica possono facilmente cadere nelle mani di malintenzionati ed essere utilizzate per scopi fraudolenti.

Manipolazione dei motori di ricerca (SEP)
-Manipola i motori di ricerca per visualizzare risultati di ricerca che contengono riferimenti a siti web dannosi. In questo modo, una pagina web infetta reindirizza gli utenti verso siti dannosi e, se le vittime accedono ai rispettivi siti, infestano i loro computer con il malware.
-Certificati digitali falsi
-sono utilizzati dagli aggressori per firmare digitalmente le risorse (siti web, applicazioni, codici sorgente, ecc.) utilizzate in vari attacchi informatici al fine di passare inosservati all'utente finale.
-Sono spesso utilizzati per firmare applicazioni web dannose come l'e-banking o l'e-commerce, che utilizzano il protocollo HTTPS.
-possono essere creati o rubati sfruttando le vulnerabilità dei sistemi PKI (Public Key Infrastructure) delle autorità di certificazione che rilasciano i certificati digitali per i siti web sicuri.

Server web sicuro - SSL

Il protocollo che implementa la crittografia a chiave pubblica si chiama SSL (Secure Socket Layer), sviluppato da Netscape, attualmente aggiorato in TLS. Questo protocollo è utilizzato dai browser e dai server Web per trasmettere dati in modo sicuro, quindi è stato creato per essere utilizzato dal protocollo HTTP.

La connessione a un server Web sicuro avviene citando il protocollo https anziché http nell'URL; in altre parole, l'accesso alla pagina Web sicura è indicato dal protocollo e non dal nome del server.

Un server web sicuro offre: Trasferimento sicuro delle informazioni: i dati trasmessi tra il server e il navigatore non possono essere decifrati in caso di intercettazione.
Autenticazione del server: Se il server web ha ricevuto un certificato da un'autorità di certificazione (CA).

Lista di controllo della sicurezza

Firewall desktop e mobile
Iniziate a mettere in sicurezza i vostri perimetri esterni assicurandovi che il vostro funzionamento dei firewall dei punti (dispositivi digitali). Sembra una cosa elementare, ma è proprio dalle basi che bisogna partire. In genere esistono tre o quattro tipi diversi di firewall sulla rete:
- Firewall del sistema operativo (Android, iOS, Windows, ecc.).
- Firewall sul programma antivirus/sicurezza.
- Firewall sul router Internet.
- Firewall sul box ASA o sullo switch intelligente (in genere solo per le aziende più grandi).

Backup

Il backup dovrebbe essere in cima alla lista, come non dovrebbe essere una novità. Il backup può evitare di dover pagare un riscatto per sbloccare i dati. Tuttavia, non fatevi ingannare dalle dimensioni dell'azienda: la maggior parte degli attacchi con questo tipo di malware sono rivolti a piccole imprese e privati.

Regole per una navigazione più sicura

-Utilizzare l'ultima versione del browser

-orientarsi verso altri tipi di browser (ad esempio Google Chrome, Opera, Firefox, Safari, ecc.), soprattutto quando si accede a pagine web potenzialmente non sicure;

-La maggior parte delle minacce informatiche colpisce Microsoft Internet Explorer (utilizzato da oltre il 50% degli utenti).

-Verificare la reale destinazione dei link passandovi sopra il cursore del mouse e visualizzando l'indirizzo reale nella parte inferiore sinistra del browser.

-Fare attenzione ai plugin che installate, spesso contengono software dannoso

-Non cliccate sui link delle finestre pop-up.

-Verificare la presenza di "https://" all'inizio dell'indirizzo web prima di inserire informazioni personali.

-Per quanto riguarda l' acquisto online, è necessario prestare maggiore attenzione al livello di sicurezza della pagina, se si opta per il pagamento online con carta bancaria.

Invio e ricezione di e-mail

-Evitare di inviare o ricevere informazioni sensibili via e-mail;

-Evitare i tentativi di ingegneria sociale o di phishing

-Cercate un provider di posta elettronica che offra un forte filtro anti-spam

Non rispondete allo spam ed evitate le e-mail a cascata o piramidali.

Non rispondete allo spam ed evitate le e-mail a cascata o piramidali.

-Non utilizzare lo stesso nome per l'account di posta elettronica personale e per quello di lavoro; l'uso di nomi distinti per questi account riduce il rischio che siano oggetto di un attacco informatico.

-Evitare di memorizzare informazioni critiche in account di posta elettronica personali o in altre reti esterne all'istituzione/azienda in cui si lavora.

La verità è che l'e-mail non è mai stata tradizionalmente un mezzo di comunicazione sicuro. Dopo tutto, solo i criminali devono preoccuparsi di proteggere le loro comunicazioni. Si tratta di un modo di pensare estremamente comune, ma del tutto errato, e lo stesso Snowden ha notoriamente screditato questo tipo di mentalità.

Sostenere che non ci si preoccupa della privacy perché non si ha nulla da nascondere è come sostenere che non ci si preoccupa della libertà di parola perché non si ha nulla da dire.

Sebbene molte persone siano ancora convinte di non avere nulla di cui preoccuparsi se non hanno nulla da nascondere, la realtà è che c'è molto di cui preoccuparsi e ci sono molte ragioni concrete per criptare le proprie comunicazioni e-mail e proteggere la propria privacy. Questo vale sia che siate giornalisti investigativi, dissidenti, informatori o semplici cittadini medi.

Perché qualcuno dovrebbe avere bisogno di inviare un'e-mail sicura?

Per proteggersi dalle minacce dei criminali informatici
Vi è mai capitato di inviare informazioni personali sensibili in un'e-mail e di pensare: "Spero proprio che quell'e-mail non finisca in qualche modo nelle mani sbagliate"? Si tratta di un pensiero davvero sconcertante, perché se qualcuno diverso dal destinatario (o dai destinatari) mette le mani sull'e-mail, soprattutto se si tratta di un criminale informatico, i risultati potrebbero essere potenzialmente catastrofici.

L'invio di un'e-mail contenente dati personali sensibili come informazioni mediche, informazioni sul conto finanziario, numero di previdenza sociale, indirizzo o numero di telefono, può essere estremamente rischioso perché ai criminali informatici basta una quantità minima di dati personali per ottenere il massimo del danno. Con l'accesso a dati personali sensibili come questi, i criminali informatici possono compromettere i vostri profili online, prosciugare i vostri conti bancari e persino rubare la vostra identità.

Per impedire ai provider di e-mail di monitorare le e-mail e condividere i dati con gli inserzionisti.
È noto che i provider di posta elettronica monitorano e scansionano i messaggi di posta elettronica degli utenti per facilitare gli sforzi pubblicitari mirati. Sebbene nel 2017 Gmail abbia apparentemente interrotto la pratica di scansione delle e-mail a fini pubblicitari, ciò non significa necessariamente che Google abbia smesso di scansionare le e-mail per altri scopi. Ad esempio, la funzione "Smart Reply" di Gmail offre suggerimenti pertinenti per risposte rapide e in scatola a un'e-mail ricevuta in base al contenuto del messaggio. Quindi, se non volete che il vostro provider di posta elettronica scansioni o monitorizzi i vostri messaggi di posta elettronica per scopi pubblicitari o di altro tipo, dovrete inviare messaggi di posta elettronica sicuri che mantengano effettivamente il contenuto di tali messaggi privato e inaccessibile a chiunque non sia voi e la persona con cui state comunicando via e-mail.

La sorveglianza di massa viola le nostre libertà civili e i diritti fondamentali alla privacy.
Questa sorveglianza ingiustificata è indebitamente invasiva e costituisce un affronto diretto alle nostre libertà civili e ai nostri diritti fondamentali alla privacy. Quando inviate un messaggio di posta elettronica sicuro, potete crittografare la vostra comunicazione in modo che solo voi e l'altra parte con cui state comunicando in modo sicuro possiate accedere al contenuto del messaggio.

L'invio di un messaggio di posta elettronica crittografato preserva la vostra privacy e rende di fatto impossibile agli enti governativi spiare le vostre comunicazioni e-mail sicure. Questo è particolarmente importante per coloro le cui responsabilità lavorative richiedono la totale riservatezza delle comunicazioni, ma è anche fondamentale per tutti coloro che in generale non vogliono che il governo calpesti i loro diritti alla privacy.

Per proteggersi dagli sforzi di sorveglianza del governo
Come abbiamo detto in precedenza, le pratiche di sorveglianza governativa di massa sono molto estese. E questo è vero non solo in regimi autoritari come quello cinese o iraniano, ma anche negli Stati Uniti, nel Regno Unito, in Australia, in Canada, in Germania e in altri Paesi occidentali.
La sorveglianza di massa non è un'aberrazione, è la norma e può essere perniciosa al punto da essere illegale.

Per questo motivo l'invio di e-mail sicure è fondamentale, soprattutto se l'e-mail che si sta inviando contiene informazioni personali sensibili.

Come inviare un'e-mail sicura
Ora che conoscete le ragioni per cui desiderate inviare un'e-mail sicura, immaginiamo che vogliate sapere come farlo. Ci sono un paio di modi per farlo, ognuno dei quali presenta vantaggi e svantaggi intrinseci, ma il punto fondamentale è che se volete inviare un'e-mail sicura, il vostro messaggio di posta elettronica dovrà essere crittografato. Quando si cripta un messaggio di posta elettronica, in sostanza, si rimescola il contenuto del messaggio e si rende impossibile per chiunque, senza la chiave di crittografia, decifrare il messaggio.

Quali sono le opzioni disponibili se si vuole inviare un'e-mail sicura?

Crittografia delle e-mail nei client di posta elettronica più diffusi
Molti dei principali provider di posta elettronica sul web consentono agli utenti di crittografare le proprie e-mail utilizzando uno dei due principali protocolli di crittografia delle e-mail, S/MIME o OpenPGP. L'aspetto negativo è che non sempre è un processo semplice e diretto da eseguire direttamente dall'interfaccia del provider di posta elettronica, e potrebbe essere necessario pagare per questo.

Ad esempio, se volete inviare un'e-mail sicura su Gmail, dovrete prima abilitare la crittografia S/MIME accedendo a Gmail con un account amministratore GSuite. Gli account GSuite sono principalmente per scopi aziendali, ma in teoria si potrebbe creare un account per uso personale.

L'altro problema è che anche i destinatari delle e-mail devono avere attivato la crittografia S/MIME per poter funzionare.

Allo stesso modo, Outlook supporta anche la crittografia S/MIME, che deve essere attivata manualmente, ma prima di farlo è necessario ottenere un certificato (o ID digitale) dall'amministratore dell'organizzazione. Questa non è la procedura più snella, né probabilmente una soluzione molto pratica per la maggior parte degli utenti di e-mail personali. Per ulteriori informazioni, consultate la sezione Come crittografare le e-mail di Outlook.

Tuttavia, è possibile aggirare questi problemi installando uno strumento gratuito di terze parti come Mailvelope per crittografare le e-mail con facilità. Mailvelope funziona con molti dei servizi di posta elettronica più diffusi, come Gmail, Yahoo!, Outlook, Hotmail e GMX. Anche in questo caso, però, i destinatari del messaggio e-mail crittografato dovranno utilizzare un software PGP/OpenPGP simile per decrittografare l'e-mail e leggerne il contenuto.

Utilizzate un provider di posta elettronica sicuro dedicato

Se non si vuole fare la fatica di abilitare manualmente la crittografia S/MIME o OpenPGP sul proprio account di posta elettronica tradizionale basato sul web, un modo molto più semplice per inviare un'e-mail sicura è quello di creare un account con un provider di posta elettronica sicura.

Con un provider di posta elettronica sicuro come ProtonMail, sarete in grado di inviare e-mail sicure e crittografate ad altri utenti, indipendentemente dal fatto che utilizzino lo stesso provider di posta elettronica sicuro che utilizzate voi, e anche i vostri destinatari saranno in grado di rispondere in modo sicuro. Molti provider di posta elettronica sicura implementano la crittografia OpenPGP per proteggere le e-mail degli utenti e consentono agli utenti di inviare e ricevere facilmente e-mail sicure e crittografate con altri utenti che hanno abilitato la crittografia OpenPGP nei loro client di posta elettronica. Se il vostro destinatario non ha abilitato il PGP, sarete comunque in grado di inviargli un'e-mail sicura che potrà essere aperta solo utilizzando un segreto condiviso.

In pratica, quando utilizzate un provider di posta elettronica sicura sarete in grado di proteggere facilmente i messaggi sensibili criptandoli, il tutto su una piattaforma che di solito è semplice da usare come i grandi provider di posta elettronica come Gmail, Yahoo! o Outlook. Ma a differenza di questi grandi provider, un provider di posta elettronica sicura non vi infastidirà con pubblicità o monitorerà le vostre e-mail (dato che non può nemmeno accedervi grazie alla crittografia end-to-end).

Il rovescio della medaglia è che per accedere a tutte le funzioni, all'archiviazione estesa e alla messaggistica illimitata di un provider di posta elettronica sicura, è necessario pagare. Molti dei migliori provider di posta elettronica sicura offrono tuttavia un livello gratuito (con alcune

limitazioni) che consente di inviare e ricevere e-mail sicure gratuitamente. Se avete intenzione di inviare solo un numero limitato di e-mail sicure, l'opzione gratuita potrebbe essere una soluzione valida, ma se avete intenzione di condurre la maggior parte della vostra corrispondenza e-mail in modo sicuro, sarà necessario acquistare un abbonamento premium.

Quando si riceve un'e-mail, prestare attenzione a

-L' identità del mittente non è garantita: si verifica la relazione tra il mittente e il contenuto del messaggio;

-Non aprire gli allegati provenienti da persone sconosciute o associate ad account legittimi, ma con messaggi dall'oggetto e dal contenuto sospetti. Potrebbero contenere software dannoso (malware, come worm, trojan, spyware, forme di adware, ecc.);

-Se è assolutamente necessario aprire un allegato, anche se proveniente da e-mail legittime, deve essere prima scaricato e scansionato con la soluzione antivirus installata e poi aperto con l'applicazione associata;

-Nel caso di e-mail contenenti link, non accedete direttamente al link nel corpo del messaggio; eventualmente, il link può essere copiato e aperto da un'altra scheda del browser;

-Non rispondete a e-mail contenenti richieste di dati personali o riservati (ad esempio, codice PIN e numero di carta bancaria).

Come fate a sapere che la vostra e-mail è stata "acceduta" da persone sconosciute?

I vostri contatti dicono di aver ricevuto e-mail di spam da voi;

Si ricevono molte e-mail con errori;

-I messaggi appaiono nella cartella "inviati" senza che voi li abbiate inviati;

-La cronologia della posizione dell'account nell'operazione di login non corrisponde all'attività corrente.

Sicurezza della password. Gli attacchi mirano a identificare la password e ad accedere alle informazioni limitate da tale password. I metodi di attacco più utilizzati di questo tipo sono gli "attacchi a dizionario" e la "forza bruta".

L'attacco "a dizionario" mira all'accesso non autorizzato di alcune risorse o sistemi informatici, provando successivamente le password/chiavi di decrittazione presenti in un elenco predefinito di parole o frasi.

L'attacco "a forza bruta" è un metodo di accesso non autorizzato a un sistema informatico o di decodifica di contenuti criptati (come le password) utilizzando il calcolo "a forza bruta" - attraverso programmi che applicano il metodo dell'errore per tentativi. Il metodo consiste nel provare successivamente tutte le possibili combinazioni di caratteri, senza un algoritmo elaborato.

Misure: sistema captcha, tempistica di accesso dopo un certo numero di accessi falliti.

-Utilizzare ID e password univoci e non comunicarli ad altri utenti;

-La lunghezza della password e la sua complessità devono essere scelte in modo che sia difficile da indovinare ma facile da ricordare;

-Cambio periodico delle password (con un intervallo di 1-3 mesi);

-Utilizzare password diverse per applicazioni diverse;

-l' uso di più metodi di autenticazione (PIN, impronte digitali, messaggi di avviso, ecc.);

-evitare di utilizzare password simili a casa e al lavoro.

Non utilizzare:

-Il nome vostro, di qualcun altro della famiglia o del vostro animale preferito,

-Elementi del vostro indirizzo: nome dell'edificio, via, paese,

-il nome dell'istituzione, del progetto, ecc,

-Numero di telefono , numero di registrazione

-il nome della star o del personaggio preferito (o del film, del libro, ecc.),

-parole del dizionario ;

-il nome dell'account per il quale è stata impostata la password;

Alcuni metodi per creare password forti

- Metodo della prima lettera: ***S**o **p**er **c**erto **d**i **a**vere **u**n **DVD B**lu-**R**ay!*
    - ***SpcdauDVDB-R!***

- Metodo di sostituzione (di solito vocali): *Amo le vacanze*
    - **@m0l3v4c@n23**
- E se ne possono inventare molti altri

Complessivamente in questo modulo dell'unità

Come utilizzare efficacemente la Cyber Kill Chain nella vostra strategia di sicurezza informatica

Rilevare - Analizzare e individuare i tentativi di intrusione.

Negare - Bloccare gli attacchi nel momento in cui si verificano.

Interruzione - Interrompere la comunicazione dei dati

Degradare - Ridurre e limitare l'efficacia dell'attacco.

Ingannare - Portare gli attaccanti nella direzione sbagliata.

Contenere - Nascondere e limitare la portata dell'attacco in modo che colpisca solo una parte dell'organizzazione.

Domande:

Domande Forum di discussione a cui rispondere con una breve spiegazione.

-Cos'è il malware

-Quali sono le principali minacce informatiche?

-Qual è il ruolo del server web sicuro - SSL

-Spiegare alcune regole per una navigazione più sicura

-Presentare alcune misure di sicurezza per l'invio e la ricezione di e-mail.

Domande di autovalutazione.

-Malware

- Le principali minacce informatiche

-Regole per una navigazione più sicura

-Misure per la sicurezza dell'invio e della ricezione di e-mail

Allegati (presentazione PowerPoint, dispense, stampe, link, video...):

Vedere i file Powerpoint e Video

Riferimenti:

-Che cos' è la sicurezza informatica?

URL: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

-Malware o software dannoso

URL: https://www.malwarebytes.com/malware

-Sicurezza informatica per tutti.

https://www.avast.com/c-malware

-Software di rimozione malware 2022; Protezione dei dati personali

URL: Malware

-Cosa sono le minacce alla sicurezza informatica?

URL: https://www.imperva.com/learn/application-security/cyber-security-threats/

-21 minacce principali alla sicurezza informatica e come l'intelligence delle minacce può aiutarvi

URL: https://www.exabeam.com/information-security/cyber-security-threat/

-Invio e ricezione di e-mail

URL: https://www.ibm.com/docs/en/i/7.1?topic=mail-sending-receiving-e

Creare e inviare e-mail

URL: https://support.google.com/a/users/answer/9259846?hl=en

La catena di morte informatica: Le sette fasi di un attacco informatico

URL: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/