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

Modulo di formazione InCyT

Sicurezza delle informazioni per manager Unità 3 -Settimana 6 Nome dell'unità (modulo): Sicurezza dei fornitori terzi	
Attività di apprendimento	❑ **Webinar**❑ **Esercitazioni**❑ **Workshop**❑ **Presentazione**❑ **Altro**
Apprendimento responsabile	• George Matache - et al.
Obiettivi dell'attività di apprendimento	1. I rischi delle reti sociali 2. Misure per la sicurezza e la privacy nei social network 3. Tecniche di sicurezza 4. Requisiti per l'approvvigionamento
Competenze da acquisire	• Sicurezza di rete TS3 • TS4 Test di penetrazione (vulnerabilità sfruttabili) • SS3 Analisi cognitiva e del comportamento
Durata dell'attività di apprendimento	2 settimane
Apprendimento requisiti	***Cosa serve?*** • Competenze gestionali di base • Competenze informatiche di base • Competenze di base in materia di sicurezza

Brevi informazioni sul modulo

Descrizione
I requisiti di approvvigionamento si riferiscono ai beni e ai servizi che devono essere acquisiti da organizzazioni esterne all'organizzazione esecutrice. Per una serie di ragioni, a volte le organizzazioni esecutrici si affidano a fornitori per fornire ciò che è necessario per completare un progetto. Ad esempio, si consideri un produttore di widget che intraprende un progetto per automatizzare il proprio sistema di tracciamento dell'inventario. Alcune delle attività di lavoro del progetto prevedono lo spostamento di contenitori di stoccaggio nel magazzino principale. Altre attività di lavoro prevedono lo sviluppo di software personalizzato. Per quanto riguarda le attività di sviluppo del software, il produttore di widget non dispone di risorse umane che sappiano sviluppare l'applicazione software. Per quanto riguarda le attività di sviluppo del software, il produttore di widget deve procurarsi tali servizi. Le reti sociali basate sul Web (WBSN) sono comunità online che consentono agli utenti di pubblicare risorse (ad esempio, dati personali, annotazioni, blog) e di stabilire relazioni, eventualmente di tipo diverso, per scopi che possono riguardare gli affari, l'intrattenimento, la religione, gli incontri e così via. Negli ultimi anni, l'uso e la diffusione delle WBSN sono aumentati, con circa 300 siti Web che raccolgono le informazioni di oltre 400 milioni di utenti registrati. Di conseguenza, il "modello della rete" è oggi sempre più utilizzato per comunicare, condividere informazioni, prendere decisioni e "fare affari" da parte di aziende e organizzazioni. È quindi una sfida concepire meccanismi di sicurezza per le reti sociali, in grado di proteggere le informazioni private e regolare l'accesso alle risorse condivise. In questo documento, oltre a fornire una panoramica delle caratteristiche dell'ambiente WBSN e dei suoi requisiti di protezione, si illustrano gli approcci attuali e le tendenze future alla sicurezza dei social network, con particolare attenzione alle tecnologie emergenti legate al cosiddetto Web 2.0.

Contenuto del materiale didattico (🕓 ?? minuti o 10-12 pagine)

Un fornitore terzo è una persona o un'azienda che fornisce servizi a un'altra azienda (o ai clienti di quest'ultima). Sebbene i fornitori siano considerati "terze parti", alcuni settori distinguono un "fornitore terzo" specificamente come un fornitore con contratto scritto, ma non tutti i fornitori lavorano con un contratto. Per chiarezza, in questo articolo il termine "fornitore terzo" si riferisce a qualsiasi persona o società che fornisce servizi a un'altra azienda con o senza contratto.

La cooperazione è la chiave del successo. La collaborazione con terzi aiuta le aziende ad aumentare la produttività e l'efficienza, a produrre prodotti e servizi migliori, a impiegare esperti altamente qualificati e a ridurre i costi. Ma tutti questi vantaggi hanno il prezzo di un aumento dei rischi di cybersecurity. Piccoli difetti nelle routine di sicurezza e privacy dei fornitori terzi possono trasformarsi in punti deboli per la sicurezza informatica della vostra azienda. In questo articolo analizziamo i particolari rischi di cybersecurity legati alle terze parti e come è possibile mitigarli.

I beni e i servizi ottenuti da fornitori terzi possono includere, ma non sono limitati a:

- Servizi di web hosting in cloud. Un fornitore di cloud hosting può fornire tutto, dallo spazio su disco alla larghezza di banda, fino alla crittografia e alle soluzioni di sicurezza ad alta tecnologia.
- Soluzioni software basate sul cloud. I fornitori di software SaaS forniscono l'accesso a programmi software per la vostra azienda o per i vostri clienti. Ad esempio, piattaforme di automazione del marketing, CRM, pacchetti contabili, ecc.
- Manutenzione delle apparecchiature. L'azienda che ripara la fotocopiatrice e il team che gestisce la sicurezza della rete sono fornitori terzi.
- Assistenza HVAC. L'azienda HVAC locale che si occupa della manutenzione dell'unità fornisce servizi a terzi.
- Appaltatori di qualsiasi tipo. Qualsiasi appaltatore, a breve o a lungo termine, è un fornitore terzo.
- Fornitori di call center. Se il call center viene ospitato da un'altra azienda, questa viene considerata un fornitore terzo.
- Contabilità/revisori finanziari. Qualsiasi persona o azienda assunta per la gestione delle finanze, il bilancio o la revisione delle finanze è un fornitore terzo.
- Avvocati. A volte è necessario consultare un avvocato prima di firmare contratti o fare acquisti importanti. Tutti i servizi legali sono considerati fornitori terzi.

Poiché le organizzazioni si affidano sempre più a fornitori terzi per fornire servizi essenziali, diventano anche più vulnerabili ai rischi di cybersecurity legati ai fornitori. Un recente studio ha rilevato che quasi il 60% delle aziende ha subito una violazione dei dati a causa di un fornitore terzo nell'ultimo anno. Ma quali sono le più comuni lacune informatiche dei fornitori che le organizzazioni dovrebbero conoscere?

Quali sono i vantaggi dell'utilizzo di fornitori terzi per i fornitori di servizi?
Nel mondo di oggi è impossibile evitare di ricorrere a fornitori terzi. Indipendentemente dal numero di dipartimenti creati dalla vostra azienda, non riuscirete mai a coprire tutti i servizi di cui avrete bisogno. Le aziende devono stabilire il giusto equilibrio tra le competenze essenziali per l'azienda e quelle che possono essere esternalizzate. Ecco cosa succede quando si raggiunge il giusto equilibrio:

- Risparmierete tempo. Nessuno ha il tempo di imparare tutte le abilità o di assumere tutte le persone necessarie per gestire un'azienda. I fornitori terzi fanno funzionare i processi aziendali senza intoppi, ottenendo tutti i servizi professionali necessari per operare ed evadere gli ordini per i vostri clienti.

- Risparmierete denaro. Il vantaggio maggiore è forse il risparmio sui costi. Contrattare un fornitore terzo per il lavoro necessario può essere molto meno costoso che avere sempre dei professionisti sul libro paga dell'azienda. Per esempio, è molto meno costoso assumere un avvocato quando se ne ha bisogno, piuttosto che tenerlo a contratto.

- Otterrete un'esperienza preziosa. La vostra azienda non ha il tempo di sviluppare un nuovo team di esperti. I tempi e i costi sarebbero enormi. L'assunzione di un fornitore terzo per le competenze che non avete all'interno dell'azienda darà probabilmente risultati migliori.

Quali sono i rischi dell'utilizzo di fornitori terzi?
I terzi potrebbero non prendere la sicurezza della loro rete così seriamente come vorreste. Sapendo questo, gli hacker potrebbero scegliere di non attaccare direttamente la vostra azienda. Potrebbero invece cercare un bersaglio più facile tra i vostri fornitori terzi. Un subappaltatore compromesso può facilmente trasformarsi in un punto di ingresso per i criminali informatici.

Se i vostri fornitori non riescono a consegnare, voi non riuscirete a consegnare. Tuttavia, il rischio è insito in qualsiasi relazione commerciale. L'utilizzo di fornitori terzi comporta molti rischi, la maggior parte dei quali può essere mitigata.

Il rischio maggiore è quello di scegliere un rapporto con terzi che non sia in linea con i vostri standard di sicurezza. Ad esempio, il vostro team di sicurezza di rete deve seguire protocolli di sicurezza all'altezza dei vostri standard specifici. Se la vostra azienda è vincolata da normative come quella dell'assicurazione sanitaria, non potete permettervi di assumere un'azienda di sicurezza di rete che non sia conforme alle normative dell'assicurazione sanitaria. Avete bisogno di un fornitore che comprenda le normative e sia disposto ad adattarsi per soddisfarle.

Quando si è vincolati dalle normative sulla privacy dei dati, è necessario sapere esattamente quali standard di sicurezza vengono implementati e, se i fornitori non sono in linea con essi, bisogna cercare di porvi rimedio. Altrimenti, esporrete la vostra azienda a rischi di cybersecurity, come una violazione dei dati.

Le violazioni dei dati sono estremamente dannose, soprattutto quando si tratta di proteggere informazioni personali. Purtroppo le violazioni di dati sono in aumento e sono più comuni che mai. Le violazioni dei dati possono causare interruzioni delle attività, conseguenze finanziarie devastanti, azioni legali e una reputazione danneggiata. Per evitare tutto ciò, non potete abbassare la guardia quando si tratta della vostra sicurezza o di quella dei vostri fornitori.

A seconda della natura della compromissione dei fornitori terzi, un'organizzazione può trovarsi ad affrontare rischi diversi. Vediamo le categorie di rischio più comuni e le minacce che dovete essere pronti a mitigare. La compromissione di un fornitore terzo può comportare molteplici rischi che possono essere suddivisi in quattro categorie principali: Figura 1

- Rischi di cybersecurity - I subappaltatori di solito hanno accesso legittimo a diversi ambienti, sistemi e dati dei loro clienti. Gli aggressori potrebbero utilizzare un fornitore terzo come punto di ingresso per cercare di impossessarsi dei vostri beni preziosi.

- Rischi operativi - I criminali informatici possono prendere di mira i vostri sistemi interni e i servizi che utilizzate, anziché solo i vostri dati. Questo può portare a interruzioni parziali delle operazioni o addirittura a un blocco totale.

- Rischi di conformità - Gli standard e le normative internazionali, locali e specifiche del settore stabiliscono criteri di cybersecurity rigorosi che le organizzazioni devono rispettare.

Inoltre, anche le terze parti che lavorano con queste organizzazioni devono rispettare questi requisiti. La mancata conformità comporta solitamente multe salate e danni alla reputazione.

- Rischi di reputazione: la compromissione dei vostri preziosi dati e sistemi è un segnale di allarme per i vostri partner e clienti, attuali e futuri. Riconquistare la loro fiducia richiederà molto tempo e sforzi. E purtroppo non c'è alcuna garanzia che sarete in grado di recuperare la vostra reputazione dopo un grave incidente di cybersecurity.

Requisiti per l'approvvigionamento

Per una serie di ragioni, a volte le organizzazioni che operano si affidano ai fornitori per ottenere ciò che è necessario per completare un progetto. In particolare, le PMI. I requisiti di approvvigionamento sono quindi della massima importanza per lavorare con la sicurezza dei fornitori terzi.

Se è vero che il procurement è un processo altamente personalizzato, esistono anche diverse fasi fondamentali che vengono generalmente utilizzate in modo trasversale.

I requisiti di approvvigionamento si riferiscono ai beni e ai servizi che devono essere acquisiti da organizzazioni esterne all'organizzazione esecutrice. Per una serie di ragioni, a volte le organizzazioni esecutrici si affidano a fornitori per fornire ciò che è necessario per completare un progetto.

Le fasi dell'approvvigionamento
Fase 1: identificare un bisogno di prodotti e/o servizi.
Fase 2: creare e inviare una richiesta di acquisto.
Fase 3: valutazione e selezione dei fornitori/venditori.
Fase 4: negoziare i termini di un contratto con il fornitore selezionato.
Fase 5: finalizzare l'ordine di acquisto.

Il primo passo del processo di approvvigionamento è l'identificazione dei requisiti. Tutti i requisiti per gli appalti iniziano con la percezione di un bisogno. La necessità di attraversare un corso d'acqua può creare un requisito per costruire un ponte, un traghetto o altri sistemi di trasporto.

Fase 1: **identificare un bisogno di prodotti e/o servizi**

Prima di iniziare il processo di approvvigionamento, è necessario riconoscere un'esigenza specifica. Ad esempio, un'organizzazione potrebbe essere interessata ad acquistare nuovi monitor per computer, a riordinare la fornitura mensile di prodotti cartacei o ad acquisire un software aggiornato. A seconda della struttura aziendale, questa fase può essere gestita dai proprietari, dai

capi reparto, dal team esecutivo, dal personale e/o dai responsabili degli acquisti. In questa fase si stabilisce un budget e spesso si valuta una visione globale della spesa.

In questa fase è necessario definire chiaramente l'esigenza, e ciò può essere fatto attraverso uno studio per determinare la modalità migliore per attraversare il corpo idrico (data la situazione attuale e le esigenze future previste), quindi il tipo di ponte da costruire, o un'analisi comparativa costi/benefici per determinare la soluzione migliore tra un ponte e altre alternative. Lo studio dovrebbe includere se l'esigenza può essere soddisfatta internamente o appaltata, la quantificazione della stima di bilancio iniziale e un'idea dei tempi di approvvigionamento.

Fase 2: Creare e inviare una richiesta di acquisto
Una richiesta d'acquisto (o requisizione d'acquisto) è una richiesta formale di beni o servizi e viene generalmente inoltrata utilizzando un software di approvvigionamento specializzato. Spesso la richiesta di acquisto parte da un dipendente o da un manager e viene poi esaminata dal team di approvvigionamento dell'organizzazione.

Quando una richiesta di acquisto viene approvata, diventa un ordine di acquisto. Tuttavia, se la richiesta viene respinta, di solito viene restituita al mittente con una breve spiegazione. Un ordine di acquisto rifiutato, pur non essendo l'ideale, può essere una buona occasione di apprendimento.

Fase 3: valutazione e selezione di fornitori/venditori
Il passo successivo consiste nel valutare i vari fornitori e sceglierne uno che soddisfi i requisiti principali. Alcune organizzazioni mantengono un catalogo di fornitori approvati, con vari fornitori che hanno già dato prova di sé.

La ricerca di fornitori è un processo che può variare da semplice a complesso, la cui portata è determinata dai requisiti da soddisfare. Di solito, vengono inviate diverse richieste di offerta (RFQ) a vari fornitori, in modo che l'organizzazione/il team di approvvigionamento possa confrontare prezzi e opzioni.

Ricordate che il prezzo non deve essere l'unico fattore determinante nella scelta di un fornitore. Per ottenere i migliori risultati, considerate il "quadro generale" di ciò che un fornitore può offrire, tra cui:

- Facilità di comunicazione
- Etica aziendale
- Responsabilità
- Capacità di produzione

Una volta scelto il fornitore, è importante investire tempo ed energie nel rapporto con lui. Un buon rapporto con un fornitore può sbloccare risparmi e servizi migliori, offrendo il massimo valore a lungo termine.

Fase 4: negoziare i termini di un contratto con il fornitore selezionato

Una volta scelto il fornitore più adatto, è il momento di passare alla negoziazione del contratto. In termini di successo dell'approvvigionamento, questa è una delle fasi di gran lunga più critiche. È in questa fase che dovrete delineare - e concordare - i prezzi, oltre a dettagli come i piani di consegna, i termini e le condizioni specifiche e altro ancora. Spesso può essere utile valutare i contratti precedenti per individuare le opportunità di miglioramento, in modo da adottare un approccio più consapevole in futuro.

Fase 5: Finalizzare un ordine di acquisto

Dopo l'approvazione del contratto finale, l'ordine successivo è l'ordine di acquisto (PO). Il contratto di solito regola l'intero rapporto acquirente/fornitore, mentre l'ordine di acquisto si concentra su un acquisto specifico.

Considerate questo documento come un altro contratto formale, che descrive in dettaglio quanto segue:

- Costi totali/prezzo
- Descrizione dettagliata dei prodotti e/o servizi
- Quantità
- Altri termini e condizioni specifici

Fase 6: Gestione degli ordini

Quando i beni/servizi vengono consegnati, ci deve essere un responsabile, idealmente l'utente finale del prodotto o del servizio, per verificare che tutti gli standard siano stati rispettati, i termini di consegna, le quantità dei prodotti, la qualità, ecc. In caso di problemi con gli articoli (ad esempio, prodotti danneggiati), avete la possibilità di rifiutare la consegna. Una comunicazione chiara con il fornitore è fondamentale in caso di problemi di consegna.

Con la tecnologia e le comunicazioni che consentono alle aziende di espandere le proprie catene di fornitura, la complessità della gestione del rischio fornitori aumenta. È probabile che la vostra azienda collabori con un numero maggiore di fornitori rispetto al passato e che ognuno di questi rappresenti un certo livello di rischio per la vostra organizzazione.

La gestione dei rischi per la sicurezza dei fornitori è una strategia progettata per limitare il numero di minacce, vulnerabilità e debolezze che la vostra organizzazione deve affrontare a causa dei fornitori della vostra catena di fornitura. Un fornitore è in genere un'organizzazione terza che vende un prodotto, un servizio o un'apparecchiatura di cui la vostra azienda ha bisogno per operare.

Ogni fornitore, una volta collegato alla vostra organizzazione, comporta un certo livello di rischio per la sicurezza informatica. Se non rispettano la loro parte dell'accordo o se sono vittime di un attacco informatico, potrebbero avere un impatto diretto sulla vostra organizzazione. Una valutazione del rischio efficace, come parte di un piano di gestione del rischio del fornitore, cerca di identificare questi potenziali punti deboli molto prima che diventino un problema e di risolverli.

Il ciclo di gestione del rischio dei fornitori

La gestione dei rischi per la sicurezza dei fornitori è un processo continuo, da eseguire con ogni fornitore inserito nella vostra catena di fornitura. In genere, il processo si presenta come segue:

Fase 1: analisi - L'azienda identifica il rischio intrinseco della relazione e il livello di due diligence da eseguire. Di conseguenza, l'azienda valuta la posizione di sicurezza della terza parte ed esegue un'analisi delle lacune.
Fase 2: coinvolgimento - L'azienda e la terza parte collaborano su come rimediare alle lacune.
Fase 3: rimedio - La terza parte risolve le lacune informatiche.
Fase 4: approvazione - L'azienda approva la terza parte o la rifiuta in base alla tolleranza al rischio.
Fase 5: monitoraggio - L'azienda continua a monitorare la terza parte per individuare eventuali falle informatiche.

Social network e rischi per la sicurezza dei fornitori

Le reti sociali sono molto popolari nel mondo di oggi. Di solito, una rete sociale è definita come una rete di piccoli mondi, costituita da un insieme di individui (persone, gruppi, organizzazioni) collegati da relazioni personali, lavorative o di fiducia. La rete sociale è quindi una nozione piuttosto ampia e generica, che nel contesto del Web può essere applicata a qualsiasi tipo di comunità virtuale. Ad esempio, gli utenti registrati a un servizio Web, come la posta elettronica, le riviste online o i giornali che richiedono un abbonamento, possono essere considerati una rete sociale. Di seguito adottiamo la definizione secondo cui il sito Web di una comunità online può essere considerato una rete sociale basata sul Web solo se soddisfa le seguenti condizioni:

- Le relazioni sono specificate esplicitamente dai suoi membri e non sono dedotte dalle interazioni esistenti (ad esempio, una mailing list può essere usata per dedurre relazioni implicite).
- Le relazioni vengono archiviate e gestite utilizzando tecnologie, come i sistemi di gestione dei database, che consentono l'analisi delle relazioni e regolano l'accesso e il recupero dei dati relativi alle relazioni.
- I membri sono in grado di accedere alle informazioni sulle relazioni, almeno in parte.

Termini chiave

Controllo dell'accesso basato sulle relazioni: un paradigma di controllo degli accessi specificamente adattato alle reti sociali, in base al quale i membri della rete sociale autorizzati ad accedere a una determinata risorsa sono indicati in termini di relazioni a cui devono partecipare per ottenere l'accesso.

Rete sociale: Una rete a piccolo mondo costituita da un insieme di individui (persone, gruppi, organizzazioni) collegati da relazioni personali, lavorative o di fiducia. Di solito è modellata come un grafo, dove i nodi corrispondono ai membri della rete sociale, mentre gli spigoli denotano le relazioni esistenti tra loro.

I social network. Comunicare e condividere informazioni con chi ci circonda fa parte della vita di ognuno di noi e si è evoluto dai semplici messaggi di testo alle e-mail e a quelle che oggi chiamiamo piattaforme di social media. Ciò che non è molto conosciuto o realizzato è il fatto che la nostra esposizione nell'ambiente online comporta molti rischi.

I social media e le applicazioni di social networking o di messaggistica possono comportare una serie di rischi per la sicurezza e la privacy sia per le organizzazioni che per gli individui, se utilizzati in modo inappropriato o non sicuro. Le piattaforme più popolari e diffuse sui social network:

-Facebook con oltre 1.300.000.000 di membri;
-Flickr è utilizzato per archiviare, organizzare e condividere file multimediali;
-LinkedIn con oltre 300 milioni di utenti;
-Instagram con oltre 30 milioni di utenti;
-Twitter con oltre un miliardo di iscritti;
-YouTube con oltre un miliardo di utenti;
-Tinder con circa 12 milioni di utenti;
-TikTok con oltre 800 milioni di utenti.

Controllo dell'accesso consapevole della privacy: Nel contesto delle reti sociali, indica un paradigma di controllo degli accessi in cui i requisiti di controllo degli accessi dei membri della rete sociale sono applicati senza rivelare informazioni private sulle relazioni a cui partecipano.

Rete sociale basata sul Web: Un sistema basato sul Web che consente ai suoi membri registrati di stabilire relazioni con altri membri e di condividere diversi tipi di informazioni (ad esempio, dati personali, contatti, risorse multimediali).

Analisi delle reti sociali: Disciplina che si propone di raccogliere dati statistici dall'analisi della topologia delle reti sociali.

Livello di fiducia della relazione: In una rete sociale, indica il valore associato a una relazione di fiducia, fornendo una misura di quanto un dato membro consideri un altro membro degno di fiducia. A seconda dello scopo per cui viene utilizzata, questa nozione può avere significati diversi. Ad esempio, in un ambiente di valutazione collaborativa, indica quanto un dato membro si fida delle opinioni di un altro membro rispetto a un argomento specifico (fiducia topica) o in generale (fiducia assoluta). In un contesto di controllo degli accessi, invece, presenta alcune analogie con la nozione di livello di sicurezza utilizzata nei modelli di controllo degli accessi obbligatori.

Perturbazione dei bordi: Tecnica di anonimizzazione del grafo che mira a nascondere le reali relazioni della rete sociale eseguendo una serie di cancellazioni/inserimenti casuali di bordi nel grafo della rete.

Relazione di rete sociale: Una relazione tra due membri di una rete sociale. Nelle WBSN, oltre alle relazioni personali/lavorative (ad esempio, amico/collega), possono essere supportate anche relazioni di fiducia che indicano quanto un membro si fida di un altro. Nella rappresentazione a grafo di una rete sociale, le relazioni sono solitamente denotate da spigoli, etichettati con un tipo di relazione e/o un livello di fiducia della relazione.

Anonimizzazione dei grafici: Tecnica volta a nascondere le informazioni private sui membri di una rete sociale quando si esegue l'analisi della rete sociale. L'anonimizzazione dei nodi e la perturbazione dei bordi sono le due principali tecniche di anonimizzazione dei grafi attualmente utilizzate.

Anonimizzazione dei nodi: Tecnica di anonimizzazione dei grafi che mira a nascondere l'identità dei membri della rete sociale etichettando i nodi corrispondenti con identificatori casuali (anonimizzazione naïve) o, nel caso in cui i nodi siano associati ad attributi che possono essere utilizzati per identificare l'utente corrispondente, utilizzando tecniche basate sulla k-anonimità (Sweeney, 2002).

I rischi

Geotagging

- Rappresenta l'aggiunta di dati geo-identificativi a foto, video, siti web e messaggi di testo da parte di applicazioni in grado di leggere la posizione dell'utente o autorizzate a farlo nelle impostazioni;
- Assicuratevi di disattivare le funzioni di geotagging nei luoghi sensibili per evitare di rivelare la vostra posizione esatta, il luogo di lavoro o di residenza.

"Pubblico"

- È un termine generale che si riferisce a chi può vedere e/o commentare i vostri post;
- Il vostro gruppo di amici può cambiare in qualsiasi momento ed essere in grado di visualizzare un post che contiene informazioni su di voi. Potete condividere intenzionalmente qualcosa con i vostri "amici", ma ciò che essi fanno con il post è fuori dal vostro controllo personale.

Identità

- Descrive la gamma di informazioni che riguardano specificamente un individuo;
- Occorre tenere presente che ci sono persone che utilizzano i social media come metodo di ricerca di informazioni sull'identità, con possibili intenti malevoli, come furto d'identità, frode, appropriazione indebita o intimidazione.

Misure

Password

- Si consiglia di utilizzare una password diversa per ogni account online;
- Deve essere lungo almeno 10 caratteri e contenere lettere maiuscole, minuscole, numeri e caratteri speciali;
- Non deve essere rivelato a nessuno, a prescindere dalla vicinanza o dalla fiducia della persona a cui vogliamo dirlo.
- Si raccomanda di non utilizzare informazioni personali quando si crea una password (ad esempio: nomi dei genitori, data di nascita, nome dell'animale domestico, ecc;)
- Cambiare periodicamente la password;
- Uscire dal proprio account quando si utilizza un dispositivo non proprio o utilizzato da un'altra persona.

Eseguite gli aggiornamenti di sicurezza in tempo!

- Le piattaforme di social media introducono regolarmente nuove impostazioni di privacy e sicurezza. Queste si trovano nelle impostazioni dell'account e si consiglia di controllarle regolarmente;
- Utilizzate l'opzione di autenticazione a due fattori (2FA) per assicurarvi che qualcuno non stia cercando di violare il vostro account.

Non accettate richieste di amicizia da nessuno!

- Accettate o inviate richieste di amicizia solo a persone che incontrate nella vita reale o a persone pubbliche che vi interessano, avendo cura di seguire i loro profili ufficiali;
- NON DIMENTICARE! Se vi sentite legati a determinati account, potete limitare il loro accesso ai vostri post o bloccare l'account. Avete anche la possibilità di segnalare account o post per motivi quali: account falso, nome falso, post con contenuti inappropriati, incitamento alla violenza, informazioni false, ecc.
- NON fare clic!

- Molti aggressori utilizzano l'ingegneria sociale per conquistare la fiducia di una persona e ottenere in seguito l'accesso alle informazioni;
- Non aprite link e allegati dai social media se non siete sicuri al 100% della fonte (ad esempio, i siti web che offrono premi sono spesso finalizzati al furto di informazioni);
- Se dalle chat un amico sembra comportarsi in modo diverso (fa molte domande, diventa molto curioso sulla sua vita personale, chiede soldi) è possibile che il suo account sia stato violato e che un malintenzionato lo stia usando per scopi malevoli.

Pensateci due volte prima di postare!

- I social media offrono l'opportunità di creare una reputazione online positiva tanto quanto una negativa; inoltre, anche se "cancelliamo" un post, una volta apparso online non può essere eliminato definitivamente;
- Non rivelate troppi dati personali sui social media! I campi "Chi sono" sono facoltativi.
- Il confine tra vita professionale e personale nell'ambiente online
- Non divulgate online informazioni sul vostro datore di lavoro.
- Non pubblicate foto di lavoro o messaggi negativi che mettano in cattiva luce il datore di lavoro.
- Pensate prima di postare e non rischiate il vostro lavoro.

Chiudete i vecchi account!

- Se avete vecchi account su piattaforme di social media che non utilizzate più, o anche vecchi account sulla stessa piattaforma, cercate di chiuderli. In questo modo si crea il minor numero possibile di collegamenti e gli account attuali sono più protetti da eventuali aggressori;
- I conti o le piattaforme più vecchi potrebbero non essere sicuri come quelli di oggi.

I social media comportano grandi rischi

- I social network presentano elevati rischi per la sicurezza e la privacy a causa della loro architettura centralizzata, dell'enorme quantità di informazioni di identificazione personale che ogni hacker vorrebbe avere e dell'ignoranza generale della popolazione su come utilizzare correttamente le impostazioni di privacy dei social media per migliorare la propria sicurezza online.
- Un altro rischio molto elevato, soprattutto tra gli adolescenti, è quello di fidarsi di altre persone e del tipo di informazioni personali divulgate online.
- Questo può essere combattuto con mezzi tecnologici e con l'applicazione di politiche di sicurezza.
- Dovremmo considerare insicure le informazioni trasmesse attraverso i social media e quindi non trasmettere informazioni sensibili attraverso i social media, pertanto la responsabilità principale di rimanere al sicuro spetta all'UTENTE.

Cattive abitudini sui social media

- I social network sono oggi piattaforme molto utilizzate dagli utenti. Abbiamo a disposizione un'ampia gamma di possibilità.

- Alcune sono più orientate al caricamento di foto o video, altre alle nostre opinioni e in altri casi semplicemente per tenersi in contatto con amici e familiari. In ogni caso, si tratta di piattaforme che hanno molti utenti in tutto il mondo.
- Questo fa sì che anche gli hacker mettano gli occhi qui. Parleremo di queste abitudini che dovrebbero essere cambiate nei social network se vogliamo mantenere la nostra privacy e la nostra sicurezza.
- Sono molti i tipi di piattaforme che possiamo trovare in rete che ci danno la possibilità di inviare messaggi ad amici o familiari, commentare foto, video...
- Questo li rende un ambiente molto popolare sia per gli utenti privati che per le aziende.
- Tuttavia, questo comporta anche qualche rischio per la nostra sicurezza e privacy. Gli hacker possono guardare qui per portare a termine i loro attacchi. In particolare, possono sfruttare le cattive abitudini degli utenti quando utilizzano queste piattaforme.

Abitudini da cambiare

- La privacy e la sicurezza sono fattori molto importanti per gli utenti.
- Tuttavia, non sono sempre presenti.
- Possiamo essere vittime di molti tipi di attacchi che compromettono questi due fattori.
- Anche noi possiamo commettere errori nell'uso dei social media e questo ci condiziona.

Aggiungere qualsiasi tipo di contatto

- Un errore molto comune nei social network è quello di aggiungere qualsiasi tipo di contatto. Questo può accadere su piattaforme come Facebook.
- È possibile che quello che stiamo aggiungendo sia un bot piuttosto che un utente reale.
- È necessario saperli differenziare ed evitare di aggiungere qualsiasi tipo di contatto che il vostro invito riceve.
- A volte i bot sono progettati esclusivamente per raccogliere dati degli utenti. Questo può compromettere la nostra privacy. Dobbiamo avere un vero e proprio filtro sui contatti che aggiungiamo.
- È importante avere tra i nostri amici persone che non rappresentino un problema per la nostra sicurezza e privacy.

Non collegatevi ai social network da nessuna parte

- Spesso si accede attraverso i social network su qualsiasi sito. È molto comodo, ma non è il massimo per la privacy.
- Certamente in molte occasioni troviamo la possibilità di registrarci su una pagina o di collegarci a una piattaforma attraverso Facebook o Twitter. Evitiamo di registrarci su quel sito e di compilare un lungo modulo. Il problema è che forniamo dati personali a quel sito web attraverso Facebook. Questi dati/informazioni che condividiamo possono essere utilizzati da terzi per scopi pubblicitari.

Non fornire più informazioni del necessario

- È sicuramente una delle peggiori abitudini di molti utenti. Inseriscono nei social network molti dati personali, informazioni che non sono realmente necessarie.
- Ad esempio, dati come il nostro numero di telefono, l'indirizzo e-mail, informazioni sul luogo in cui viviamo... Tutto ciò influisce sulla nostra pubblicità e potrebbe essere utilizzato per scopi negativi.
- Non date più informazioni di quelle realmente necessarie. In questo modo miglioreremo la nostra privacy in rete e potremo persino evitare alcuni problemi di sicurezza.

Diffusione di fake news

- Il problema delle fake news è ancora presente oggi. Posso raggiungerli attraverso molti mezzi, ma senza dubbio nei social network sono più che presenti.
- Come sappiamo, si tratta di notizie false che usano come esca e che a volte possono anche distribuire malware.
- È importante evitare di condividere questo tipo di fake news e anche di accedervi quando le vediamo sui social media.
- Questo migliorerà la nostra sicurezza.

Non proteggiamo la nostra privacy

- Un ultimo errore è quello di non proteggere adeguatamente la privacy. Ad esempio, lasciamo i nostri profili aperti a chiunque.
- Forniamo informazioni a chiunque possa raccoglierle per creare un profilo per noi e persino inviare pubblicità mirata o eseguire vari attacchi che riguardano la nostra sicurezza.

L'ingegneria sociale in una prospettiva interdisciplinare

-A causa della tecnica utilizzata dagli hacker, è necessario affrontare una prospettiva interdisciplinare come l'informatica, la psicologia, l'economia e l'etica.

La disciplina della tecnologia dell'informazione

- L'ingegneria sociale dovrebbe essere discussa nel contesto degli attuali sistemi informativi e della loro difesa come forma di mitigazione del rischio.
- L'autenticazione a più fattori è un modo comune e spesso efficace per le organizzazioni di confermare che la persona che accede ai sistemi abbia effettivamente tale accesso.
- Un ulteriore fattore potrebbe essere l'utilizzo di una rete privata virtuale (VPN), ovvero l'autenticazione per convalidare ulteriormente l'utente.

Disciplina psicologica

- È necessario comprendere il concetto e capire i pensieri e i comportamenti dell'aggressore e della vittima.

- I metodi sono importanti per l'ingegneria sociale perché vengono utilizzati per aggirare le protezioni eventualmente presenti, come i firewall e i sistemi utilizzati per identificare gli intrusi.
- Aiuta a comprendere le azioni dei dipendenti che sono una delle cause principali delle violazioni dei dati.

Prospettiva aziendale

- è importante perché l'ingegneria sociale può interessare molti tipi di aziende e avere implicazioni sul modo in cui le organizzazioni sono strutturate e gestite.
- aiuta a determinare i fattori che influenzano gli attacchi di social engineering ed è vantaggioso se considerato in termini più specifici in relazione alle seguenti aree aziendali: formazione e sviluppo, politiche documentate, procedure di audit interno, budget e cultura organizzativa.
- è in grado di rilevare le carenze in tutte le aree che possono contribuire agli attacchi.

Prospettiva etica

- è importante nel contesto dell'ingegneria sociale e della ricerca correlata perché l'idea di manipolare un altro essere umano viola molti principi etici.
- aiuta, nel caso di un evento di ingegneria sociale, a curare le vittime.

È importante considerare:

- ogni disciplina, fornendo informazioni su come comprendere e interpretare l'argomento, proteggersi da diversi tipi di attacchi e comprendere l'impatto dell'ingegneria sociale dal punto di vista umano e organizzativo.
- che l'interpretazione di ogni disciplina è utile solo se vista nel contesto delle altre discipline.

Tecniche di sicurezza

- Inventario delle attrezzature
- Inventario delle applicazioni e dei sistemi operativi
- Controllo delle apparecchiature wireless
- Progettazione della sicurezza di rete
- Limitare e controllare le porte di rete, i protocolli di comunicazione e i servizi.
- Protezione delle aree perimetrali
- Accesso fisico alle sedi
- Uso controllato dei privilegi amministrativi
- Monitoraggio e controllo degli account utente
- Valutazione delle competenze e formazione sulla sicurezza

VPN (Rete privata virtuale)

Una rete privata virtuale è una connessione sicura su una rete non sicura come Internet. Virtuale significa l'esistenza di una rete unica, indipendentemente dalla topologia, ovvero un gruppo di

computer distribuiti geograficamente che comunicano e possono essere amministrati come un'unica rete.

Per rete privata si intende una rete virtuale con controllo degli accessi che garantisce la riservatezza, l'integrità dei messaggi e l'autenticazione tra gli utenti e i computer che partecipano alla comunicazione.

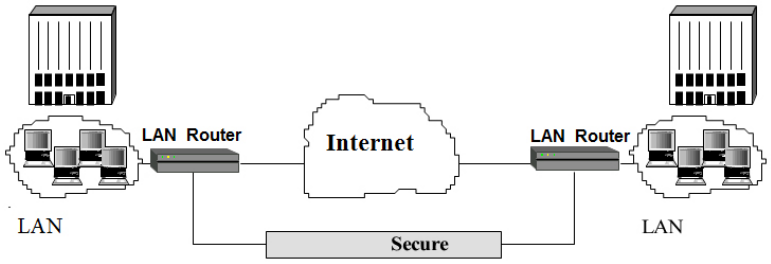

Fig. 2: VPN (rete privata virtuale)

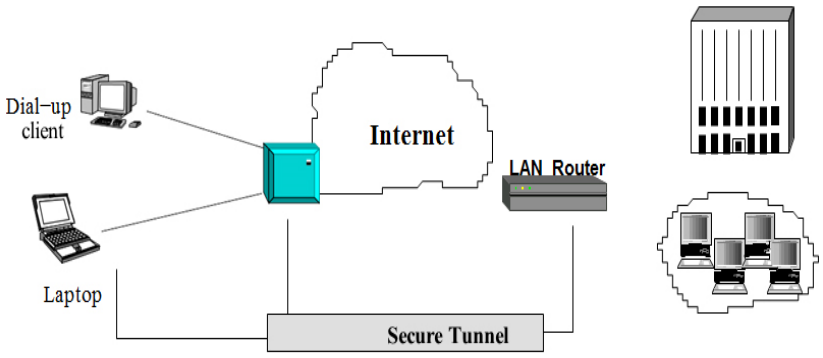

Fig. 3: VPN per l'accesso remoto

Creare un'infrastruttura industriale sicura

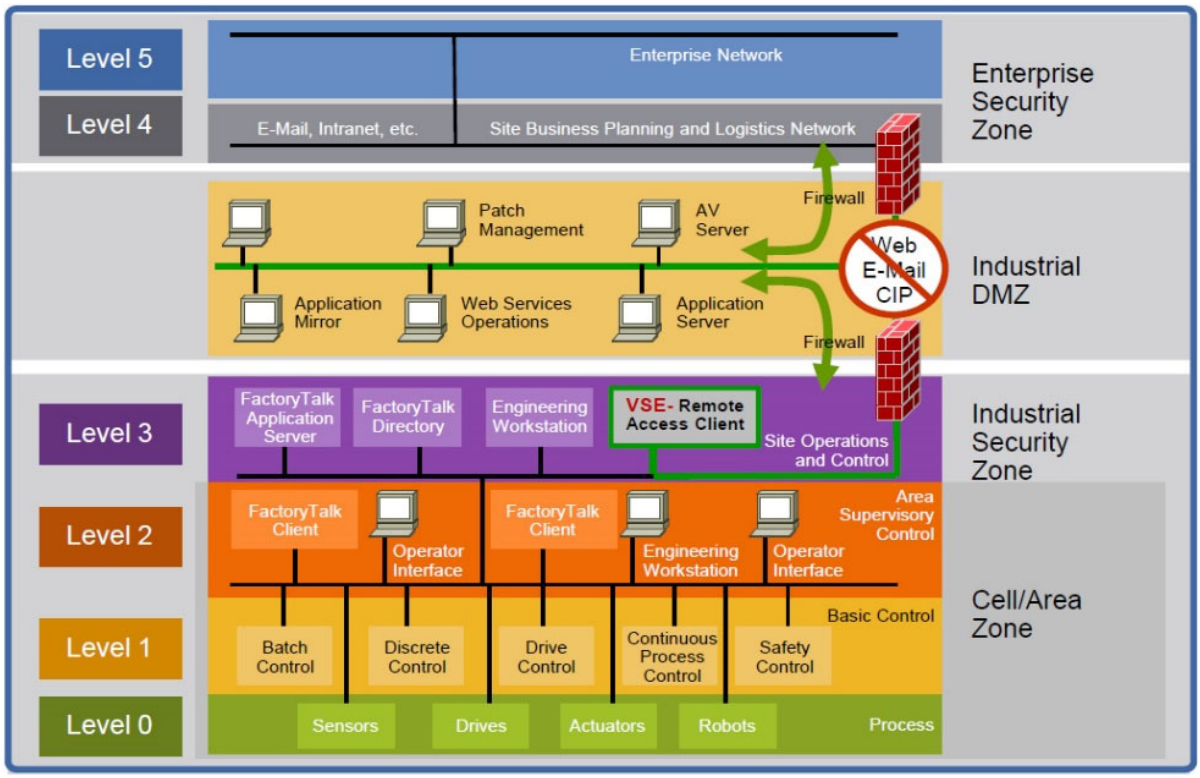

Fig. 4: Modello logico ISA 95 - Sistema di automazione e controllo industriale (IACS)

- La difesa in profondità (DiD) supporta questo approccio. Basandosi sull'idea che un singolo punto di protezione può essere e sarà probabilmente sconfitto, la sicurezza DiD stabilisce più livelli di protezione attraverso una combinazione di salvaguardie fisiche, elettroniche e procedurali.
- Una banca utilizza più misure di sicurezza, come videocamere, una guardia e un caveau, per garantire che le minacce incontrino più di una linea di difesa.
- Un approccio di sicurezza in profondità comprende sei componenti principali:

1. Politiche e procedure
2. Fisico
3. Rete
4. Computer
5. Applicazione
6. Il dispositivo

Creare un'infrastruttura industriale sicura

- La sicurezza fisica deve limitare l'accesso del personale non solo alle aree di una struttura, ma anche ai punti di ingresso nell'infrastruttura fisica di rete, come pannelli di controllo, cablaggi e dispositivi.

- La segmentazione delle aree dell'impianto in reti locali virtuali (VLAN) è una best practice di sicurezza a livello di rete.
- Le VLAN più piccole sono più facili da gestire e mantenere nelle comunicazioni in tempo reale.
- Possono aiutare a isolare i dispositivi da quelli compromessi, mantenendo l'impatto negativo all'interno di una singola VLAN.
- Una delle tecnologie discusse dovrebbe essere una zona industriale smilitarizzata (IDMZ), che crea una barriera protettiva critica tra l'impresa e le aree industriali.
- Un'IDMZ limita il traffico dal passaggio diretto tra le due zone e può aiutare a gestire meglio l'accesso imponendo l'autenticazione o monitorando il traffico alla ricerca di minacce note.

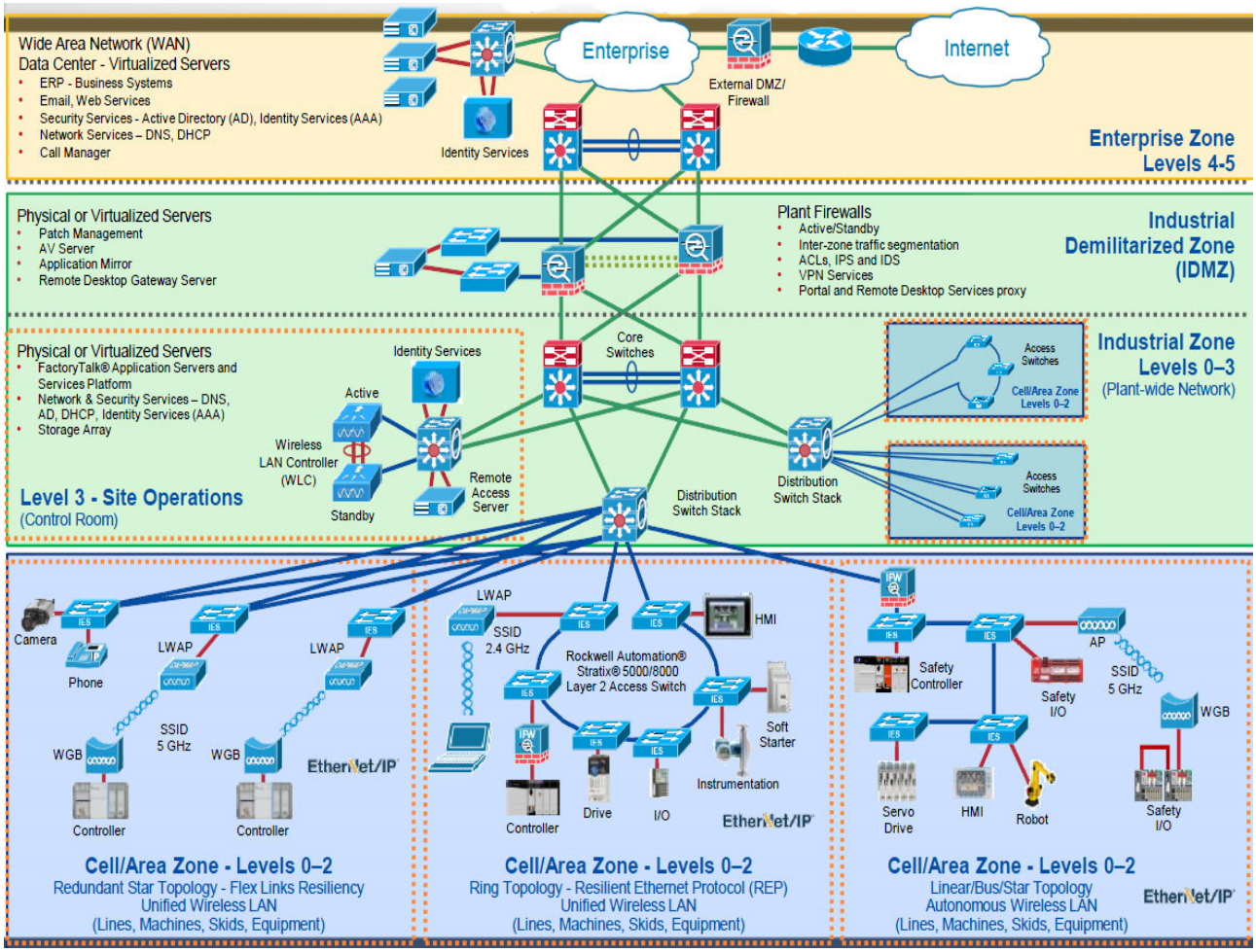

Fig. 5: IDMZ

Domande:

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

- Quali sono i rischi dei social network?
- Misure per la sicurezza e la privacy nei social network
- Quali sono le principali tecniche di sicurezza nei social network?

Domande di autovalutazione.

- I rischi delle reti sociali
- Sicurezza e privacy nelle reti sociali
- Tecniche di sicurezza

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

Vedi allegato

Riferimenti:

Requisiti per l'approvvigionamento
URL: Appalti-requisiti
URL: https://www.ekransystem.com/en/blog/third-party-providers
Determinazione dei requisiti per l'approvvigionamento
URL: https://www.procurementclassroom.com/procurement-requirement-determination/
Sicurezza e privacy nelle reti sociali
URL: https://www.igi-global.com/chapter/security-privacy-social-networks/14073
Sicurezza e privacy nelle reti sociali
URL: https://sefcom.asu.edu/publications/security-privacy-social-ic2011.pdf
Privacy e sicurezza nei social media online
URL: https://www.geeksforgeeks.org/privacy-and-security-in-online-social-media/
Tecniche di sicurezza dei dati e privacy
URL: https://www.educba.com/data-security-techniques/
Cosa sono le tecniche di sicurezza
URL: Concetti di sicurezza-sviluppi-e-tendenze-future
Le tecniche di sicurezza più efficaci
URL: https://dzone.com/articles/most-effective-security-techniques-part-1
URL: https://panorays.com/blog/what-is-a-third-party-vendor/