Valutazione dei rischi

Obettivo:

Adesso dovrai iniziare a ragionare come un vero IT Manager. In questo progetto infatti, avrai l'opportunità di confrontarti con una autentica realtà aziendale, in modo tale da poter creare l'analisi dei rischi informatici (Risk Assessment) dell'azienda!
La tua SFIDA sarà infatti quella di creare un "RISK ASSESSMENT".
Concentriamoci sull'esercizio.

Brief progetto:

Tra le principali responsabilità di chi ricopre ruoli di responsabilità in campo IT, c'è quella di analizzare il rischio che potrebbe portare a danneggiare l'azienda (come ad esempio un malware) al fine di capire come garantire un'adeguata protezione delle infrastrutture hardware e software aziendali, nonché dei dati e delle informazioni.

Stiamo parlando di analizzare il rischio cybersecurity di una vera azienda!

Una delle priorità di un IT Manager è capire quali sono i valori di rischio che potrebbero comportare una perdita di dati personali e strategici dell'azienda e come mitigarli applicando i principi di cybersecurity. Bisogna ragionare con attenzione.

Nello specifico, il RISCHIO viene calcolato tramite il prodotto di due elementi:

- Verosimiglianza : La probabilità che una determinata minaccia possa concretizzarsi.

- Impatto : Il danno che si verificherebbe qualora si concretizzi una determinata minaccia.

Rispetto a queste MINACCE:

- Insider Threat
- Furto di dati
- Intrusione dall'esterno (fisica)
- Malware
- Bug/feature
- Errore umano
- Accesso indebito a sistemi, dati e informazioni dall'interno
- Man-in-the-middle
- Manomissione
- Intrusione dall'esterno (logica)

- Esplosioni
- Phishing
- Incendi
- Denial of Service
- Impersonificazione
- Eventi naturali (geologici, meteorologici)
- Furto di dispositivi

Ecco la situazione in cui ti trovi:

L'azienda ha necessità di capire quali sarebbero i valori di rischio riguardanti alcune minacce informatiche in maniera tale da poter stimare il budget da destinare alla mitigazione dei valori di rischio più alti.
Istruzioni progetto:
Prepara un documento di *RISK ASSESSMENT* che contenga una tabella con questi elementi:

1. Riporta in un documento la lista delle minacce sopra elencate.
2. Fai una ricerca sul significato di quelle minacce, in cosa consistono? Come potrebbero verificarsi?
3. Ricordando cosa ti ha detto il referente dell'azienda su cui fare il Risk Assessment. Conoscere le misure di sicurezza presenti e come è organizzata è fondamentale.
4. Dai un valore da 1 a 5 alla verosimiglianza e all'impatto su ogni minaccia, dove 1 è una verosimiglianza minima e un impatto minimo (per cui quella minaccia sarà molto difficile che si verifichi / il danno sarà molto basso) e 5 una verosimiglianza massima e un impatto massimo (per cui quella minaccia si potrebbe verificare molto facilmente / il danno sarebbe altissimo!).
5. Moltiplica i valori (da 1 a 5) che hai dato su ogni minaccia tra quelle elencate ed otterrai il valore finale di rischio (da 1 a 25) per quella determinata minaccia.

Azienda:

Valutazione dei rischi fatta su un'azienda di call center "Electra S.R.L.".
Il referente mi ha chiesto di fare attenzione soprattutto ai dati dei clienti visto che si tratta di un call center e anche prestare attenzione alla perdita dei dati.

Minacce	Prevenzione e mitigazione minacce	Verosomiglianza	Impatto	Risultato
Insider Threat	Un insider threat è una minaccia dannosa per un'organizzazione che			

	proviene da persone all'interno dell'azienda, come dipendenti, ex dipendenti, appaltatori o soci in affari, che dispongono di informazioni privilegiate relative alle pratiche di sicurezza, ai dati e ai sistemi informatici dell'organizzazione quindi per mitigare la minaccia: ● Identificare i dati sensibili e limitare l'accesso solo ai dipendenti che ne hanno bisogno. ● Monitorare l'attività dei dipendenti e degli utenti per rilevare eventuali comportamenti sospetti. ● Fornire formazione e sensibilizzazione ai dipendenti sulla sicurezza informatica e sui rischi degli insider threat. ● Implementare una politica di sicurezza informatica che includa la gestione dei rischi Insider. ● Utilizzare strumenti di sicurezza informatica come firewall, antivirus e software di rilevamento delle intrusioni.	2	5	10
Furto di dati	Il furto di dati, detto anche furto di informazioni, è l'archiviazione o il trasferimento illegale di informazioni personali, riservate o finanziarie. Tali informazioni possono includere password, codice software o algoritmi, nonché tecnologie o processi proprietari per mitigare la minaccia: ● Utilizzare password ● complesse e cambiarle regolarmente. ● Non condividere mai le password con nessuno. ● Non fornire	3	5	15

	informazioni personali a siti web non affidabili o sconosciuti. ● Utilizzare software antivirus e antispyware aggiornati per proteggere il proprio computer da attacchi informatici. ● Non aprire mai allegati o link sospetti in email o messaggi di testo. ● Utilizzare una connessione Internet sicura e crittografata quando si accede a siti web sensibili come quelli delle banche o dei servizi finanziari.			
Intrusione dall'esterno (fisica)	Un'intrusione informatica dall'esterno si verifica quando un utente non autorizzato accede al tuo computer o alla tua rete da remoto. Ci sono diversi modi per capire se il tuo computer è stato violato: come controllare i programmi, installati sul sistema operativo, controllare le connessioni in uscita, controllare la lista degli utenti e controllare i log degli accessi ● Usare badge personalizzati con i permessi per accedere alle aree più riservate o telecamere.	2	4	8
Malware	Un attacco malware è un'azione dannosa contro un dispositivo o un sistema informatico da parte di un software malevolo chiamato malware e per mitigare la minaccia: ● Mantieni sempre aggiornato il sistema operativo e l'antivirus o anti-malware. ● Non fare clic su link sospetti nelle email. ● Non fare clic sui popup	1	3	3

	che si aprono nel browser. ● Non visitare siti di categorie a rischio (pornografia, pirateria ecc.). ● Non inserire dati personali su siti che non utilizzano il protocollo HTTPS. ● Non scaricare programmi da siti che non conosci.			
Bug/feature	Gli hacker possono sfruttare i bug e feature dei software per accedere a sistemi e dati protetti. Un bug è un errore di programmazione che può causare comportamenti imprevisti o indesiderati in un sistema per mitigare il problema: Per impedire minacce derivate dai bug/feature, è possibile utilizzare un buon antivirus e un buon antimalware per monitorare l'eventuale presenza di minacce come virus e keylogger. Ed è possibile aggiungere un'esclusione a Sicurezza di Windows per escludere file, cartelle, tipi di file o processi.	3	3	9
Errore umano	Gli errori umani possono causare problemi di sicurezza informatica. Un modo per mitigare e ridurre la possibilità di questi avvenimenti bisogna: ● Fornire formazione e istruzione ai dipendenti sui rischi di sicurezza informatica e sulle migliori pratiche. ● Limitare l'accesso ai dati e al software solo alle persone autorizzate. ● Utilizzare software di sicurezza per proteggere i dispositivi da malware e virus.	1	3	3

	● Verificare regolarmente i dati e il software per rilevare eventuali anomalie.			
Accesso indebito a sistemi, dati e informazioni dall'interno	L'accesso indebito a sistemi, dati e informazioni dall'interno può avvenire quando un individuo autorizzato ad accedere a un sistema informatico o telematico protetto utilizza le proprie credenziali per accedere a informazioni o dati per scopi non autorizzati o estranei ai compiti d'ufficio Per evitare l'accesso indebito a sistemi, dati e informazioni dall'interno, è possibile limitare i danni causati dalle minacce interne con una serie di misure di sicurezza come la crittografia dei dati, la gestione degli accessi e delle autorizzazioni.	4	5	20
Man-in-the-middle	Il Man-in-the-middle è un attacco informatico in cui un attaccante intercetta la comunicazione tra due parti e si inserisce al posto di una di esse per intercettare e manipolare i dati scambiati. Per difendersi da questo tipo di attacco, è possibile utilizzare una serie di misure di sicurezza come l'utilizzo di una connessione sicura HTTPS, l'utilizzo di una VPN e l'utilizzo di un buon antivirus e antimalware.	2	3	6
Manomissione	La manomissione è un tipo di attacco informatico in cui un aggressore modifica o altera i dati o il software di un sistema informatico. Ecco alcuni consigli per proteggersi dalla manomissione: ● Utilizzare software di sicurezza per proteggere i dispositivi da malware e virus.	3	4	12

	● Utilizzare password complesse e cambiarle regolarmente. ● Verificare regolarmente i dati e il software per rilevare eventuali anomalie. ● Limitare l'accesso ai dati e al software solo alle persone autorizzate.			
Intrusione dall'esterno (logica)	L'intrusione logica dall'esterno si riferisce all'accesso non autorizzato a un sistema informatico Per impedire l'intrusione dall'esterno (logica), è possibile utilizzare una serie di misure di sicurezza come l'utilizzo di un firewall, l'aggiornamento costante del software e dei sistemi operativi, la crittografia dei dati e l'utilizzo di reti Wi-Fi sicure.	2	4	8
Esplosioni	Per prevenire le esplosioni, è possibile adottare una serie di misure tecniche e organizzative. Ad esempio, è possibile sostituire i liquidi facilmente infiammabili o i gas e le polveri infiammabili con sostanze che non possono formare un'atmosfera esplosiva. Inoltre, è possibile utilizzare sistemi chiusi per impedire che si crei un'atmosfera esplosiva all'esterno delle apparecchiature e adottare misure di ventilazione per prevenire la formazione di atmosfere esplosive o limitarle Per salvare i dati in un'azienda in caso di esplosioni, è importante avere un piano di backup dei dati. Identificare i dati critici che devono essere salvati. Scegliere un metodo di backup appropriato, ad esempio un disco rigido esterno o un	1	5	5

	servizio di cloud storage. Creare una pianificazione regolare per il backup dei dati. Testare regolarmente il piano di backup per assicurarsi che funzioni correttamente.			
Phishing	Il phishing è un attacco informatico in cui un attaccante cerca di ottenere informazioni sensibili come username, password e dati bancari fingendosi un'entità affidabile in una comunicazione e-mail o messaggio istantaneo. Invece per difendersi dal spear phishing di attacco, è possibile utilizzare una serie di misure di sicurezza come l'utilizzo di un buon antivirus e antimalware, l'utilizzo di una connessione sicura HTTPS e l'utilizzo di un filtro antispam.Creare protocolli di sicurezza in azienda e farli rispettare. Creare canali di comunicazione interna sicuri e limitarsi a essi. Non cliccare su link sconosciuti e non aprire file inattesi. Verificare il mittente nel protocollo di invio. Evitare l'HTML e il download di immagini. Non aprire gli allegati.	4	4	16
Incendi	Per prevenire gli incendi, è possibile adottare una serie di misure e regole di comportamento. Ad esempio, è possibile disporre l'arredamento distante da sorgenti di calore e evitare il rischio di fughe di gas e cortocircuiti che possono provocare incendi Per salvare i dati in un'azienda in caso d'incendi, è importante avere un piano di backup dei dati. Identificare i dati critici che devono essere salvati.	1	5	5

	Scegliere un metodo di backup appropriato, ad esempio un disco rigido esterno o un servizio di cloud storage. Creare una pianificazione regolare per il backup dei dati. Testare regolarmente il piano di backup per assicurarsi che funzioni correttamente.			
Denial of Service	Un attacco DoS (Denial of Service) è un tipo di attacco informatico che mira a rendere un sistema o una risorsa di rete irraggiungibile per gli utenti autorizzati. Questo può avvenire attraverso l'inondazione del sistema o della risorsa con un traffico di rete eccessivo, causando il sovraccarico e il blocco del sistema. Per proteggersi dagli attacchi DoS: ● Utilizzare un firewall per bloccare il traffico di rete indesiderato. ● Utilizzare un sistema di rilevamento delle intrusioni (IDS) per monitorare il traffico di rete e rilevare eventuali attacchi. ● Utilizzare un sistema di prevenzione delle intrusioni (IPS) per bloccare gli attacchi DoS in tempo reale. ● Configurare i server in modo da limitare il numero di connessioni simultanee e le richieste da parte di un singolo indirizzo IP. ● Utilizzare servizi di mitigazione degli attacchi DoS forniti da fornitori terzi .	1	5	5
Impersonificazione	L'impersonificazione è un tipo di attacco informatico in cui un aggressore si finge di essere un'altra persona o			

	un’organizzazione per ottenere informazioni personali o finanziarie. Come agire: ● Non fornire mai informazioni personali o finanziarie a persone o organizzazioni sconosciute. ● Verificare sempre l’identità delle persone o delle organizzazioni che richiedono informazioni. ● Utilizzare software di sicurezza per proteggere i dispositivi da malware e virus. ● Utilizzare password complesse e cambiarle regolarmente.	5	5	25
Eventi naturali (geologici, meteorologici)	Per salvare i dati in un’azienda in caso di emergenza, è importante: ● Avere un piano di backup dei dati. ● Identificare i dati critici che devono essere salvati. ● Scegliere un metodo di backup appropriato, ad esempio un disco rigido esterno o un servizio di cloud storage. ● Creare una pianificazione regolare per il backup dei dati. ● Testare regolarmente il piano di backup per assicurarsi che funzioni correttamente.	1	5	5
Furto di dispositivi	Il furto di dispositivi è un problema comune che può causare la perdita di dati sensibili e l’accesso non autorizzato alle informazioni personali. Ecco alcuni consigli per proteggersi dal furto di dispositivi: ● Utilizzare password complesse per proteggere i dispositivi. ● Non lasciare i	1	5	5

	dispositivi incustoditi in luoghi pubblici. ● Utilizzare software di crittografia per proteggere i dati sensibili. ● Configurare i dispositivi in modo da richiedere l'autenticazione dell'utente per accedere ai dati.			

Motivazione:

La motivazione della mia valutazione è principalmente incentrata sulla protezione dei dati aziendali, inclusi i dati dei clienti e le informazioni sensibili trattate dal call center. Data la natura del nostro settore, è essenziale concentrarsi sulla mitigazione dei rischi più probabili, come violazioni della sicurezza informatica, perdita di dati e accessi non autorizzati. Garantire la sicurezza delle informazioni sensibili è fondamentale per mantenere la fiducia dei clienti e assicurare la continuità operativa dell'azienda.