Salve a tutti. Benvenuti a questo modulo sulla gestione del rischio. La gestione del rischio è un compito centrale di ogni attività imprenditoriale e, poiché sempre più aziende dipendono dalla funzionalità dei servizi informatici e dei sistemi di informazione, la gestione del rischio per la sicurezza delle informazioni diventa sempre più importante.

Iniziamo quindi con alcune basi.

Qual è la motivazione della gestione del rischio o perché abbiamo bisogno della gestione del rischio? Quando si protegge un'organizzazione, è essenziale implementare misure di sicurezza che siano specificamente appropriate per l'organizzazione. La gestione del rischio supporta questo sforzo valutando il rischio in relazione agli asset dell'organizzazione e al panorama delle minacce. In questo modo si gettano le basi di un sistema di controllo interno che aiuta a prevenire le frodi e garantisce la sicurezza dei prodotti, dei servizi e delle attività aziendali. La gestione del rischio è spesso richiesta anche dalla legge, quindi è un requisito legale. Ma questa non è l'unica motivazione. La gestione del rischio può anche apportare un valore commerciale significativo per l'organizzazione, facilitando le decisioni. Spesso le organizzazioni devono rispondere alla domanda su quanto denaro spendere per la sicurezza e la gestione del rischio fornisce informazioni che aiutano a rispondere a questa domanda. Inoltre, aiuta a gestire l'incertezza.

Quindi, la gestione del rischio è sempre strettamente legata all'incertezza, il che significa che si tratta di fare ipotesi sul futuro, su cose che non sono ancora note. Pertanto, necessita di un approccio sistematico, che tratteremo più avanti in questo video. Gli esiti dei rischi possono essere negativi o positivi. Se sono positivi, si parla spesso di gestione delle opportunità, mentre spesso la gestione del rischio si concentra maggiormente sugli eventi negativi.

Prima di iniziare ad approfondire l'argomento, vorrei definire alcuni termini fondamentali e iniziare con il termine minaccia. La minaccia è una potenziale fonte di danno o un evento negativo. Può trattarsi di un evento doloso, di un evento esistenziale, di un disastro naturale e così via. Un esempio potrebbe essere una violazione dei dati. Il termine successivo che vorrei definire è la probabilità. La probabilità è la probabilità che la minaccia o il rischio si concretizzino. Al posto della probabilità si usa spesso anche la frequenza, ovvero la frequenza con cui in un certo periodo di tempo potrebbe verificarsi una minaccia, a seconda dell'approccio al rischio che si sta utilizzando. L'ultimo termine fondamentale che vorrei sottolineare è l'impatto, che riflette le conseguenze che si verificano quando un asset viene colpito da una determinata minaccia. Gli impatti possono essere misurati sia in termini qualitativi sia in termini quantitativi e in base a diversi tipi di categorie di perdita: finanziaria, reputazionale, ambientale e così via.

Diamo un'occhiata più da vicino ai rischi per la sicurezza delle informazioni.

I rischi per la sicurezza delle informazioni sono quelli che mettono a repentaglio gli obiettivi di sicurezza delle informazioni: riservatezza, integrità e disponibilità. Gli attacchi che possono compromettere questi obiettivi di protezione includono attacchi contro i sistemi informativi, ma anche rischi come errori umani o disastri naturali. È inoltre importante sottolineare che i rischi per la sicurezza delle informazioni non riguardano solo le operazioni informatiche, ma l'intera organizzazione, poiché oggi la maggior parte delle organizzazioni dipende fortemente dalle operazioni informatiche. E naturalmente le conseguenze possono essere di vasta portata, dalle sanzioni finanziarie alla perdita di reputazione o di clienti.

Le minacce comuni alla sicurezza delle informazioni includono attacchi alla rete, minacce interne, social engineering, malware e ransomware, phishing, attacchi denial of service, attacchi alla supply chain e così via. Esistono diversi elenchi di minacce che possono essere utilizzati come base per identificare le minacce. Ne ho elencate tre che sono un'ottima scelta, ad esempio le minacce elementari del BSI dell'IT-Grundschutz-Compendium, l'allegato C della ISO 27005 e gli scenari di rischio COBID.

Esistono molti approcci alla gestione del rischio, quindi cosa deve avere un buon approccio alla gestione del rischio?

La prima cosa da fare è avere un approccio sistematico per identificare, valutare e valutare i rischi. Cosa intendo con questo? È importante che ci sia un modo sistematico di valutare i rischi e che i risultati siano comparabili nel tempo. Quindi, è necessario trovare criteri che permettano che, anche se due persone valutano i rischi in due anni diversi, i risultati rimangano comunque comparabili. Inoltre, una buona gestione del rischio deve essere adattata alle esigenze dell'organizzazione e al panorama delle minacce. Cosa intendo dire con questo? Dipende molto, sia che siate una piccola o media impresa o una grande azienda, quale approccio di gestione del rischio potrebbe essere appropriato per voi. Inoltre, dipende dalla probabilità di subire un attacco, quale gestione del rischio e quale frequenza di valutazione potrebbero essere adatte a voi. Per avere successo con l'approccio alla gestione del rischio, è anche importante che l'importanza della gestione del rischio sia promossa all'interno dell'organizzazione dal top management. Quindi, per implementare la gestione del rischio è necessario il consenso del management. Nelle prossime diapositive, quindi, approfondiremo le principali attività di gestione del rischio.

Una fase molto importante in ogni approccio alla gestione del rischio è l'identificazione del rischio, perché si possono valutare solo i rischi che si sono identificati. Si tratta quindi di un aspetto cruciale nella gestione del rischio e per questo spesso si utilizzano liste di controllo, come ho già introdotto nella sezione precedente, come il catalogo delle minacce elementari o gli scenari di rischio COBIT. Ha anche senso fare delle interviste per raccogliere l'esperienza dei dipendenti. Forse ci sono nuovi errori del passato che potrebbero essere potenziali rischi che potrebbero presentarsi in futuro.

La cosa successiva è che ogni rischio viene analizzato. Cosa intendo con questo? È importante descrivere qual è la probabilità che si verifichi e quali potrebbero essere i pericoli o le conseguenze se un rischio si concretizza.

L'ultimo passo consiste nell'elaborare un elenco di priorità dei rischi, in modo da sapere quali sono i primi da affrontare e quali potrebbero essere trascurati o affrontati in un secondo momento.

L'ultimo passo consiste nel far fronte ai rischi, quindi nell'implementare misure di salvaguardia o di mitigazione che riducano i rischi a un livello accettabile per l'organizzazione.

Come ho già detto, esistono diversi tipi di framework per la gestione del rischio, tutti validi, e dovete trovare quello più adatto a voi. Noi esamineremo OCTAVE Allegro, che è un approccio semplice con molto materiale di supporto che aiuta a rendere il processo buono e sistematico nella vostra organizzazione. Ma potrebbe essere una buona scelta anche esaminare altri approcci, se pensate che siano più adatti a voi.

Diamo quindi un'occhiata più da vicino a OCTAVE Allegro.

OCTAVE Allegro è un approccio basato sugli asset informativi. Quindi, si concentra principalmente sugli asset informativi ed è molto adatto alle piccole aziende, in quanto fornisce molti materiali, fogli di lavoro ed è pensato per essere facile da usare e comunque comparabile e un approccio molto strutturato per valutare i rischi.

Come si può vedere, OCTAVE Allegro è suddiviso in 4 fasi: stabilire i driver per la gestione del rischio, individuare gli asset informativi, identificare gli asset informativi, individuare le minacce. E, naturalmente, l'ultima fase consiste nell'identificare le misure di mitigazione per quei rischi che non sono accettabili.

Dopo aver definito i criteri di gestione del rischio, il passo successivo è l'identificazione delle risorse informative. Un asset informativo è costituito da tutti i dati o le informazioni di valore per l'organizzazione, indipendentemente dalla loro forma. Quindi, possono essere archiviati elettronicamente o fisicamente.

Le domande tipiche di queste fasi sono: quali sono le informazioni di maggior valore per l'organizzazione o quali informazioni sono necessarie per eseguire i principali processi aziendali. L'obiettivo di questa fase è identificare e documentare tutti gli asset informativi essenziali. È importante sottolineare che l'attenzione deve essere focalizzata sugli asset più critici, poiché non sarebbe possibile valutare i rischi per tutti gli asset informativi e OCTAVE Allegro vi supporta fornendo modelli per i cosiddetti Information Asset Profile nei suoi fogli di lavoro. Un altro compito essenziale è quello di assegnare i proprietari agli asset critici, che possono anche fornire maggiori informazioni sulla criticità degli asset e sui possibili impatti.

Diamo un'occhiata al profilo di un asset informativo così critico. Come potete vedere, OCTAVE Allegro fornisce anche fogli di lavoro con esempi. Qui si possono vedere anche le domande fondamentali che dovrebbero essere poste, ad esempio, quando si identificano gli asset critici, qual è l'asset informativo critico? Perché avete selezionato questi asset? Perché sono importanti? La descrizione? Che ne dite di ottenere maggiori informazioni sull'asset e sulla proprietà?

E infine, ma non meno importante, quali sono i requisiti di sicurezza per lo specifico asset informativo?

Nella terza fase di OCTAVE Allegro, si determinano i contenitori delle risorse informative, e per contenitore delle risorse informative si intende tutto ciò che viene immagazzinato, trasportato o elaborato. Quindi, questo include software, hardware, rete, ma anche persone. I contenitori delle risorse informative possono quindi essere classificati in contenitori tecnici come hardware e software, contenitori fisici come gli schedari o le persone. È anche importante documentare il proprietario di un contenitore di risorse informative, perché spesso i proprietari si assumono la responsabilità di proteggere il contenitore e aiutano a identificare le misure di mitigazione del rischio più avanti nel processo. È inoltre importante sottolineare che i contenitori delle risorse informative possono essere punti di vulnerabilità, quindi punti in cui i rischi e le minacce possono mettere in pericolo una specifica risorsa informativa.

OCTAVE Allegro fornisce anche un foglio di lavoro per acquisire le informazioni sui contenitori delle risorse, come si può vedere. È sufficiente una piccola descrizione del contenitore e il proprietario.

Il passo successivo è l'identificazione delle aree di interesse.

Un'area di preoccupazione è una dichiarazione su un evento che potrebbe verificarsi e che ha un impatto su una delle risorse informative identificate. Quindi, in questa fase vengono identificate e documentate le possibili minacce, ma non solo quelle, bensì anche le conseguenze. Quindi, considerate i requisiti di sicurezza che avete specificato quando avete identificato i requisiti di riservatezza, integrità e disponibilità delle risorse informative, ad esempio, e come le potenziali minacce potrebbero avere un impatto su di essi e quali sarebbero le conseguenze. Le aree di criticità sono la base per le fasi successive, quindi prendetevi il tempo necessario per individuare le aree di criticità. L'obiettivo di questa fase non è quello di individuare tutti i possibili scenari di minaccia per uno specifico asset informativo, ma quelli che vi vengono subito in mente e che potrebbero colpire gli asset informativi.

Come potrebbe essere un esempio? La guida di OCTAVE Allegro fornisce informazioni anche su questo. Quindi, si tratta di una semplice dichiarazione come quella mostrata nella diapositiva.

Nella fase successiva vengono identificati gli scenari di minaccia.

Quindi, le aree di preoccupazione vengono perfezionate in scenari di minaccia. Per dettagliare ulteriormente le proprietà di una minaccia. Come si può vedere sul lato destro, OCTAVE Allegro utilizzava i cosiddetti alberi delle minacce che, da un lato, si concentrano su un determinato asset e, dall'altro, si affinano all'attore, ossia all'agente di minaccia che potrebbe violare i requisiti di protezione della sicurezza, come la riservatezza, l'integrità e la disponibilità di un asset, in questo caso un agente di minaccia interno o esterno. Poi il motivo per cui si tratta di un attacco deliberato o di un attacco esistenziale. Il motivo si applica ovviamente solo agli attori umani. E poi il risultato. Qual è il risultato? È una violazione della riservatezza, come la divulgazione? È una violazione dell'integrità, come la modifica? Oppure è una violazione della disponibilità, come l'interruzione o l'interruzione e la perdita? Avendo a disposizione questi alberi delle minacce, è possibile fornire maggiori informazioni su queste aree di preoccupazione. OCTAVE Allegro suggerisce di creare questi alberi delle minacce in quattro categorie. Una è quella degli attori umani che utilizzano mezzi tecnici, l'altra quella degli attori umani che utilizzano l'accesso fisico e poi i problemi tecnici come i crash del software, i difetti dell'hardware, il codice maligno e così via. Oppure tutti gli altri tipi di problemi, come i disastri naturali, l'interruzione della fornitura di energia elettrica o le interruzioni da parte di terzi.

Nella fase 6 - Identificazione dei rischi - le conseguenze sono derivate dagli scenari di minaccia delle fasi precedenti.

L'obiettivo è quindi quello di creare dichiarazioni d'impatto dettagliate, come mostrato a destra, per documentare le conseguenze di determinati scenari di minaccia.

Nella fase successiva, i rischi vengono ulteriormente analizzati. Quindi, si determina qualitativamente in che misura l'organizzazione è impattata da una minaccia, calcolando un rischio relativo o per tutti i rischi identificati per tutte le risorse informative.

Quindi, come ho detto, la valutazione dei rischi viene effettuata in termini qualitativi e in base all'impatto e alla probabilità e, partendo dagli Scenari di minaccia e dalle Conseguenze della fase precedente, viene assegnato un valore di impatto per ogni area di impatto e il punteggio di rischio successivo aiuta a dare priorità alle ultime fasi. Lo si può vedere nella

sezione di destra. Inoltre, da un lato ci sono le aree di impatto che sono classificate in base alla loro importanza e dall'altro le aree di rischio che sono state classificate in base alla loro importanza.

Il valore d'impatto è associato al punteggio e si può vedere l'importanza relativa del valore d'impatto rispetto al punteggio di rischio.

Una volta fatto questo, si ottiene un buon profilo di rischio delle risorse informative per ogni risorsa, come nell'esempio. Si dispone di un determinato asset informativo, di un'area di criticità identificata e di una descrizione dettagliata della minaccia. Chi è l'attore della minaccia? Con quali mezzi potrebbe essere attaccato l'asset informativo? Quale potrebbe essere il movente? Quali risultati ci si aspetta? Quali proprietà di sicurezza potrebbero essere violate e quali sono i requisiti di sicurezza dell'asset? Qual è la probabilità che la minaccia si verifichi? E quali sarebbero le conseguenze? Come si può vedere, si ottiene un punteggio di rischio relativo che può essere utilizzato come fonte per pianificare ulteriori opzioni di mitigazione o trattamento del rischio.

L'ultima fase di OCTAVE Allegro consiste nel selezionare l'approccio di mitigazione.

Quando si sceglie l'approccio di mitigazione, si possono applicare 4 diversi tipi di strategie di rischio. Si può accettare il rischio, quindi documentarlo e monitorarlo nel tempo, si può rinviare il rischio a un momento successivo, si può mitigare il rischio o trasferirlo. L'opzione più frequentemente scelta è quella di mitigare, quindi di determinare i controlli interni che stanno minimizzando o riducendo il rischio attuale a un livello accettabile. E, naturalmente, alla fine si deve verificare se il rischio residuo è ancora accettabile e appropriato per l'organizzazione.

OCTAVE Allegro fornisce anche un foglio di lavoro per la mitigazione di ciascun profilo di rischio, che è piuttosto semplice. Qui si può vedere, a livello superiore, se si accetta, si attenua o si trasferisce il rischio e poi, più in dettaglio, che tipo di controlli aggiungere ai diversi tipi di contenitori.

Con questo vorrei ringraziarvi per la vostra attenzione. Spero che abbiate imparato molto sulla gestione del rischio.

E naturalmente, se avete altre domande, potete sempre contattarmi e sarò felice di rispondere alle vostre domande.