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

[redacted]ulo di formazione InCyT

Sicurezza delle informazioni per manager Unità (Modulo) 4, Settimana 7 e 8 Nome dell'unità (modulo): Rischio informatico e resilienza	
Attività di apprendimento	❑ **Webinar**❑ **Esercitazioni**❑ **Workshop**❑ **Presentazione**❑ **Altro**
Apprendimento responsabile	• Simon Tjoa • Peter Kieseberg
Obiettivi dell'attività di apprendimento	1. I partecipanti conoscono i fondamenti della gestione del rischio e della resilienza 2. I partecipanti sono in grado di eseguire l'analisi dell'impatto (BIA) sul business e l'analisi dei rischi (RIA). 3. I partecipanti possono ricavare contromisure e decisioni di sicurezza dai risultati delle analisi.
Competenze da acquisire	• IS 1, IS 3 • SM 1
Durata dell'attività di apprendimento	2 settimane • Settimana 7 (2 ore) • Settimana 8 (2 ore)
Apprendimento requisiti	***Cosa serve?*** • Competenze gestionali di base • Competenze informatiche di base • Competenze di base in materia di sicurezza

Brevi informazioni sul modulo

Descrizione
Una sicurezza perfetta non è possibile. Sapendo questo, è fondamentale prendere decisioni informate su come spendere i soldi per le giuste misure di sicurezza. La gestione del rischio informatico e della resilienza fornisce una serie di strumenti e tecniche essenziali per valutare lo stato attuale della sicurezza di un'organizzazione e pianificare i controlli per mantenere il rischio di sicurezza delle informazioni a un livello accettabile.

Contenuto del materiale didattico

Senza correre rischi è impossibile fare affari. Pertanto, la gestione del rischio e gli strumenti e le tecniche corrispondenti forniscono un modo sistematico per affrontare il rischio. Domande come quanta sicurezza sia sufficiente o quale contromisura debba essere implementata per prima trovano risposta nella gestione del rischio. La gestione del rischio è quindi un'attività importante per consentire decisioni informate. Tra gli standard e le best practice più importanti che affrontano questo tema essenziale vi sono ISO 27005, ISO 31000 o BSI 200-3.

Prima di esaminare più da vicino il processo di gestione del rischio, è fondamentale definire i termini essenziali:

- **Vulnerabilità:** "Debolezza in un sistema informativo, nelle procedure di sicurezza del sistema, nei controlli interni o nell'implementazione che potrebbe essere sfruttata o innescata da una fonte di minaccia". [1]
- **Controllo:** "Una salvaguardia o una contromisura prescritta per un sistema informativo o un'organizzazione, progettata per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e per soddisfare una serie di requisiti di sicurezza definiti".[2]
- **Minaccia:** "Qualsiasi circostanza o evento con il potenziale di avere un impatto negativo sulle operazioni dell'organizzazione (comprese la missione, le funzioni, l'immagine o la reputazione), sui beni dell'organizzazione, sugli individui, su altre organizzazioni o sulla nazione attraverso un sistema informativo mediante accesso non autorizzato, distruzione,

[1] https://csrc.nist.gov/glossary/term/vulnerability
[2] https://csrc.nist.gov/glossary/term/security_control

divulgazione, modifica delle informazioni e/o negazione del servizio".[3]

- **Rischio**: "misura della misura in cui un'entità è minacciata da una circostanza o da un evento potenziale, e tipicamente è una funzione di: (i) l'impatto negativo, o l'entità del danno, che si verificherebbe se la circostanza o l'evento si verificasse; e (ii) la probabilità che si verifichi".[4]
  "effetto dell'incertezza sugli obiettivi".[5]

Dalla definizione della ISO 31000 ("effetto dell'incertezza"), possiamo dedurre che i rischi possono avere impatti positivi e negativi. Spesso, se i rischi hanno impatti positivi, vengono definiti opportunità.

Il processo generale di **gestione del rischio** inizia con l'ambito, il contesto e i criteri. Poiché non è possibile analizzare tutti i rischi per tutte le attività, è importante stabilire le priorità e decidere quali servizi, processi e unità organizzative devono essere inclusi nella valutazione. Avere un ambito adeguato è fondamentale per garantire risultati validi da un lato e uno sforzo ragionevole dall'altro. Il contesto è l'ambiente interno ed esterno. La determinazione dei criteri di rischio è importante per garantire un processo ripetibile, che porti a risultati comparabili. I criteri devono essere definiti in modo tale che persone diverse siano in grado di valutare i rischi in modo comune.

Esempi di criteri sono i criteri di impatto (ad esempio, basso, medio, alto) per varie dimensioni, come quella finanziaria, della reputazione o della salute.

Di seguito viene presentato un esempio di OCTAVE Allegro relativo all'impatto sulla reputazione e sui clienti:

[3] https://csrc.nist.gov/glossary/term/threat
[4] https://csrc.nist.gov/glossary/term/risk
[5] https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

Allegro Worksheet 1	RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE		
Impact Area	Low	Moderate	High
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Customer Loss	Less than _____% reduction in customers due to loss of confidence	_____to _____% reduction in customers due to loss of confidence	More than _____% reduction in customers due to loss of confidence
Other:			

Figura 1: Criteri di misurazione della reputazione[6]

Dopo la definizione dei criteri di rischio e dell'ambito, il primo passo è l'**identificazione dei rischi**. L'identificazione dei rischi è fondamentale, in quanto è possibile valutare solo i rischi che sono stati identificati. È quindi opportuno confrontare le minacce identificate con gli elenchi di minacce di ISO 27005, MEHARI o altre best practice o standard.

Esistono varie tecniche[7] per identificare i rischi, come il brainstorming, la tecnica Delphi, l'analisi dei modi e degli effetti dei guasti (FMEA) o gli studi di pericolosità e operatività (HAZOP).

Nella fase successiva dell'**analisi dei rischi (RIA – Risk Impact Analysis)**, si ottiene una migliore comprensione dei rischi identificati. Si determinano quindi la probabilità/frequenza di accadimento e l'impatto/conseguenze. Per determinare le conseguenze, è importante definire un modo sistematico per valutare gli impatti. Spesso una misura qualitativa (ad esempio, bassa, media, alta) è più facile da usare rispetto alle misure quantitative.

I rischi sono spesso visualizzati in una cosiddetta matrice di rischio, che evidenzia il rischio utilizzando come assi la probabilità e l'impatto.

[6] https://resources.sei.cmu.edu/asset_files/technicalreport/2007_005_001_14885.pdf
[7] Cmp. https://www.iso.org/standard/72140.html

Probability	Harm severity			
	Minor	Marginal	Critical	Catastrophic
Certain	High	High	Very high	Very high
Likely	Medium	High	High	Very high
Possible	Low	Medium	High	Very high
Unlikely	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium
Eliminated	Eliminated			

Figura 2: Matrice di rischio [Fonte Wikipedia].[8]

Nella fase successiva, i rischi vengono valutati. Ciò significa che i risultati della fase precedente vengono presi in considerazione per decidere se è necessario intraprendere azioni. Inoltre, si procede alla definizione delle priorità dei rischi.

Successivamente viene determinata una delle quattro strategie principali per affrontare i rischi:

- Accettazione del rischio: documentare e monitorare il rischio se rientra nella propensione al rischio dell'organizzazione.
- Trasferimento del rischio: condividere i rischi (ad esempio, assicurazione, joint venture).
- Evitare il rischio: rimuovere la fonte di rischio (ad es., intercapedine d'aria).
- Riduzione del rischio: ridurre l'impatto o la probabilità di accadimento (ad esempio, controllo degli accessi).

Dopo la determinazione delle misure, si valuta se il rischio residuo è accettabile o se devono essere adottate ulteriori misure.

Come attività di supporto al processo principale di valutazione del rischio, si svolgono la comunicazione del rischio (cioè la comunicazione con le parti interessate), il monitoraggio del rischio e il reporting del rischio.

Poiché non tutti i rischi possono essere presi in considerazione, a differenza della gestione del rischio, la **continuità operativa** e la **resilienza** si concentrano sulle attività critiche anziché sui singoli rischi. In questo modo è possibile prepararsi a rischi sconosciuti e a bassa probabilità/alto impatto.

Per garantire un programma di continuità operativa efficace, il supporto del top management è fondamentale. Un importante artefatto che evidenzia l'importanza della gestione della continuità

[8] https://en.wikipedia.org/wiki/Risk_matrix

operativa è la politica di continuità operativa. In questo documento viene espresso formalmente il consenso del management. Inoltre, il documento evidenzia l'ambito e gli obiettivi delle attività di continuità operativa, i ruoli e le responsabilità importanti (ad esempio, il responsabile della continuità operativa) e il quadro operativo utilizzato per l'esecuzione del programma. Va sottolineato che l'ambito non deve essere troppo ampio per garantire che la complessità dell'analisi e l'impegno non diventino troppo elevati.

Per comprendere gli effetti delle interruzioni dei servizi sull'azienda e per avere una buona base per pianificare le misure di recupero, vengono effettuate le analisi di impatto sul business. È lo strumento centrale del processo di continuità operativa e cattura la rilevanza/significatività dei prodotti/servizi. Oltre alla criticità dei prodotti/servizi, vengono determinate e valutate le loro dipendenze.

I dati chiave importanti, che vengono utilizzati quando si esegue un'**analisi dell'impatto sul business (Business Impact Analysis – BIA)**, sono i seguenti:

- **MAO (maximum acceptable outage):** "tempo necessario affinché gli impatti negativi [...], che possono derivare dalla mancata fornitura di un prodotto/servizio o dall'esecuzione di un'attività [...], diventino inaccettabili".[9]
- **RTO (recovery time objective):** "periodo di tempo successivo a un incidente [...] entro il quale un prodotto e un servizio [...] o un'attività [...] vengono ripresi o le risorse [...] vengono recuperate".[10]
- **RPO (recovery point objective):** "punto in cui le informazioni [...] utilizzate da un'attività [...] vengono ripristinate per consentire all'attività di operare alla ripresa".[11]

Nella prima fase vengono identificati i prodotti e i servizi più critici o essenziali. Dopo l'identificazione, si valuta quale danno si verificherebbe nel tempo se un determinato prodotto o servizio venisse interrotto.

La figura 3 mostra come l'impatto nel tempo potrebbe essere descritto in un foglio di calcolo.

[9] MAO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en
[10] RTO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en
[11] RPO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en

Assessment Period / Damage Category	1 Hour(s)	2 Hour(s)	4 Hour(s)	8 Hour(s)	24 Hour(s)	48 Hour(s)	96 Hour(s)	168 Hour(s)	240 Hour(s)	720 Hour(s)
Financial	0	0	0	0	0	0	2	3	4	4
Health & Safety	0	0	0	0	0	0	0	3	4	4
Legal, Regulatory & Contractual	0	0	0	0	1	1	1	2	2	2
Brand and Reputation	0	0	0	1	1	1	2	4	4	4
Environmental	0	0	0	0	0	0	0	0	0	0
Rational for the assessment (Description) Verbal Description of Implications										

Figura 3: Impatto nel tempo dell'interruzione di un servizio.[12]

Inoltre, l'analisi dell'impatto aziendale rileva da quali processi, attività e risorse dipendono i servizi rilevanti. In questo modo è possibile determinare cifre chiave importanti, come l'obiettivo del tempo di ripristino, l'obiettivo del punto di ripristino e l'interruzione massima accettabile.

Una volta conosciuta la criticità dei processi, dei servizi e delle risorse, si elaborano le strategie di continuità operativa. Le strategie includono, tra l'altro, la diversificazione (ad esempio, attività in luoghi geograficamente separati), la replica (ad esempio, copiando i dati per recuperarli in un altro sito) o il subappalto (ad esempio, utilizzando servizi di terzi).

Sulla base delle strategie vengono redatti piani di continuità operativa che aiutano le organizzazioni a reagire in modo efficiente dopo un incidente. Per essere utilizzabili in situazioni di alta pressione, è fondamentale che i piani siano scritti di conseguenza. Ciò significa che i piani devono contenere solo le informazioni rilevanti per la gestione di un incidente. Inoltre, le informazioni devono essere di rapida comprensione. Pertanto, è necessario utilizzare liste di controllo chiare e orientate all'azione.

I tipici piani di continuità operativa contengono informazioni su scopo, ambito, struttura di gestione degli incidenti, ruoli e responsabilità, attivazione del piano, modalità di ripristino e dettagli di contatto.

Per provare e verificare l'adeguatezza dei piani, si utilizzano diversi tipi di esercitazioni. Si può trattare di esercitazioni basate sulla discussione, come i desk check o le esercitazioni su tavolo, oppure di esercitazioni tecniche, come la verifica del ripristino di alcuni sistemi.

Domande:

Vedere i documenti Word

[12] https://en.wikipedia.org/wiki/Risk_matrix

Allegati:

Vedere i file Powerpoint e Video

Riferimenti:

- ISO 22301:2019, Sicurezza e resilienza - Sistemi di gestione della continuità operativa - Requisiti
- ISO 22313:2020, Sicurezza e resilienza - Sistemi di gestione della continuità operativa - Guida all'uso della ISO 22301
- ISO/TS 22317:2021, Sicurezza e resilienza - Sistemi di gestione della continuità operativa - Linee guida per l'analisi dell'impatto sul business
- ISO/TS 22331:2018, Sicurezza e resilienza - Sistemi di gestione della continuità aziendale - Linee guida per la strategia di continuità aziendale
- ISO/TS 22332:2021, Sicurezza e resilienza - Sistemi di gestione della continuità operativa - Linee guida per lo sviluppo di piani e procedure di continuità operativa
- ISO 31000:2018, Gestione del rischio - Linee guida, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
- IEC 31010:2019, Gestione del rischio - Tecniche di valutazione del rischio