

impatto di tali modifiche sulla sicurezza del sistema è un'attività essenziale per assicurare un monitoraggio continuo e prevenire l'abbassamento del livello di sicurezza del sistema.

6.2.1 Tool per l'analisi del rischio

6.2.1.1 AGID Cyber Risk Management

Cyber Risk Management¹⁶ di AgID è lo strumento nazionale per la valutazione e il trattamento del rischio cyber. Per la protezione dei dati in formato digitale, a garanzia della loro riservatezza, integrità e disponibilità, il tool AgID di Cyber Risk Management identifica le situazioni e i vari ambiti nei quali le informazioni possono venirsi a trovare, consentendo di valutare i rischi per la loro sicurezza.

Lo strumento è stato realizzato per consentire alle pubbliche amministrazioni di analizzare l'esposizione al rischio dei servizi erogati dalle amministrazioni stesse ed in caso predisporre i "Piani di Trattamento del Rischio". AgID, dal canto suo, fornisce supporto alle amministrazioni che ne hanno necessità sia in fase di analisi che nella fase d'implementazione di tali piani, pianificati e realizzati in base ai risultati forniti attraverso la fase di Risk Treatment.

La Pubblica Amministrazione ha la peculiarità di erogare servizi verso i cittadini, verso i propri dipendenti, verso le imprese e verso altre amministrazioni.

L'analisi del rischio può essere svolta sulle singole entità (cioè sulla pubblica amministrazione come entità unica) ed anche su parti di esse, ad esempio sui dipartimenti ritenuti più critici. A essere esaminati sono i servizi erogati dalla pubblica amministrazione in correlazione con i servizi trasversali, cioè quelli utilizzati dalle pubbliche amministrazioni ma forniti da terzi, siano essi appartenenti a una PA oppure no.

Il quadro normativo sul quale AgID ha costruito il processo di Risk Management si basa sulle linee guida e sui principi dettati dallo standard ISO 31000 [DR-3] e sull'Information Risk Assessment Methodology 2 (IRAM2) dell'Information Security Forum (ISF).

La metodologia adottata è di tipo "Gray Box", poiché l'analisi parte da una situazione nota solo in parte. I servizi, ad esempio, non devono necessariamente essere esaminati in dettaglio: le informazioni fornite formano una matrice di correlazione che viene analizzata con un algoritmo sviluppato ad hoc e che fornisce come risultato l'elenco delle minacce con i relativi dettagli. Parte del report può essere visto nell'immagine seguente:

Report dei rischi per categoria di minaccia

Attacchi Logici e/o Fisici								
● Attacchi al sistema di autenticazione								
Minaccia	Impatto R-I-D	Vulnerabilità	Esposizione alla minaccia	Probabilità di accadimento	Rischio attuale	Propensione al rischio	Opzioni di trattamento	Rischio derivato
Accesso non autorizzato a credenziali di autenticazione valide	ALTO	ALTO	ALTO	ALTO	ALTO	MEDIO	MITIGARE	ALTO
Session hijacking	ALTO	ALTO	CRITICO	CRITICO	CRITICO	MEDIO	MITIGARE	CRITICO
Sfruttare vulnerabilità nei meccanismi di autenticazione	ALTO	ALTO	CRITICO	CRITICO	CRITICO	MEDIO	MITIGARE	CRITICO
● Attacchi al sistema di comunicazione								
● Attacchi fisici								
Minaccia	Impatto R-I-D	Vulnerabilità	Esposizione alla minaccia	Probabilità di accadimento	Rischio attuale	Propensione al rischio	Opzioni di trattamento	Rischio derivato
Attacchi all'infrastruttura fisica dell'organizzazione	ALTO	ALTO	MEDIO	BASSO	BASSO	MEDIO	ACCETTARE	BASSO
Furto o perdita di sistemi informativi	ALTO	ALTO	MEDIO	BASSO	BASSO	MEDIO	ACCETTARE	BASSO
● Azioni non autorizzate								
● Compromissione dei sistemi informatici di Terze Parti								
● Denial of service								
● Errori di configurazione								
● Exploit del software								
● Information Gathering								
● Information leakage								
● Malware								
● Social engineering								

Figura 12 - Cyber Risk Management di AgID – Report dei rischi per categoria di minaccia