CAPITOLO 8. Sicurezza informatica

In un momento storico nel quale la minaccia cibernetica cresce continuamente in quantità e qualità e i servizi informatici e telematici erogati dalla Pubblica Amministrazione diventano sempre più cruciali per il funzionamento del sistema Paese, la sicurezza informatica riveste un ruolo fondamentale in quanto garantisce non solo la disponibilità, l'integrità e la riservatezza delle informazioni proprie del Sistema informativo della Pubblica Amministrazione, ma anche la resilienza della complessa macchina amministrativa. Essa è inoltre direttamente collegata ai principi di *privacy* previsti dall'ordinamento giuridico.

Le norme vigenti[11] conferiscono ad AGID un mandato importante nell'attuazione di iniziative tecniche ed organizzative volte sia a migliorare la consapevolezza della Pubblica Amministrazione nei riguardi della minaccia, sia ad aumentarne le capacità di prevenzione, protezione e risposta agli incidenti. In particolare, la recente edizione 2017 del Piano Nazionale riassume questo ampio mandato attribuendo ad AGID il compito di *"dettare indirizzi, regole tecniche e linee guida in materia di sicurezza informatica e di omogeneità degli standard, di assicurare la qualità tecnica e la sicurezza dei sistemi informativi pubblici e della loro rete di interconnessione e di monitorare i piani ICT delle amministrazioni pubbliche"*. AGID persegue questo mandato sia direttamente sia mediante il CERT-PA, struttura attiva dal 2013 la quale è stata oggetto, durante il 2017, di uno specifico rafforzamento in termini sia di personale che di strumenti tecnici.

Il Piano Triennale, tenendo conto delle indicazioni contenute nel Quadro Strategico e nel Piano Nazionale, ha individuato la razionalizzazione delle risorse ICT descritta nel capitolo 3 "Infrastrutture" come uno dei principali approcci per aumentare il livello di sicurezza complessivo dell'amministrazione attraverso la riduzione della "superficie" esposta agli attacchi informatici. Questo è, infatti, uno degli aspetti tecnici maggiormente critici tra quelli individuati nel Rapporto "*Italian Cyber Security Report 2014*". Altro aspetto di fondamentale criticità emerso dal medesimo rapporto è la mancanza nelle pubbliche amministrazioni della consapevolezza sulla minaccia e l'assenza di strutture organizzative locali in grado di operare efficacemente un'attività di preparazione e risposta agli incidenti. Su questo fronte AGID opera sia mediante l'azione di *awareness* condotta dal CERT-PA ma anche attraverso la

[11] In particolare: il Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico e il relativo Piano Nazionale per la protezione cibernetica e la sicurezza informatica del 2013, nonché la Direttiva 1° agosto 2015 del Presidente del Consiglio.

pubblicazione di documenti di indirizzo ed operativi (linee guida, regole tecniche) finalizzati ad accrescere la consapevolezza e la capacità di difesa delle Amministrazioni interessate.

Le attività gestite da AGID sono raggruppate nelle seguenti aree:

- *CERT-PA*, in cui ricadono le attività svolte dal CERT-PA (*Computer Emergency Readiness/Response Team*, ovvero "squadra per la risposta ad emergenze informatiche" a supporto dei sistemi informatici della Pubblica Amministrazione) che opera all'interno dell'AGID e che supporta le pubbliche amministrazioni nella prevenzione e nella risposta agli incidenti di sicurezza informatica del dominio costituito dalle pubbliche amministrazioni;
- regolazione e regolamentazione, in cui ricadono le attività di emanazione di normative, regole tecniche, linee guida e documenti di riferimento sugli aspetti di sicurezza informatica (ad es. le Misure minime di sicurezza ICT per le pubbliche amministrazioni).

8.1 Scenario

Presso AGID è operativo dal 2013 il CERT-PA, che offre alle pubbliche amministrazioni accreditate:

- servizi di analisi e di indirizzo, finalizzati a supportare la definizione dei processi di gestione della sicurezza, lo sviluppo di metodologie, il disegno di processi e di metriche valutative per il governo della sicurezza cibernetica;
- servizi proattivi, aventi come scopo la raccolta e l'elaborazione di dati significativi ai fini della sicurezza cibernetica, l'analisi della minaccia, l'emissione di bollettini e segnalazioni di sicurezza, l'implementazione e la gestione di basi di dati informative;
- servizi reattivi, aventi come scopo la gestione degli allarmi di sicurezza, il supporto ai processi di gestione e la risoluzione degli incidenti di sicurezza all'interno del dominio delle PA;
- servizi di formazione e comunicazione, per promuovere la cultura della sicurezza cibernetica, favorendo il grado di consapevolezza e competenza all'interno delle pubbliche amministrazioni, attraverso la condivisione di informazioni relative a specifici eventi in corso, nuovi scenari di rischio o specifiche tematiche di sicurezza delle informazioni.

In attesa dell'emanazione da parte del Dipartimento della Funzione Pubblica delle Regole tecniche per la sicurezza ICT delle pubbliche amministrazioni proposte da AGID, tenuto conto dell'urgenza conseguente all'evoluzione delle minacce cibernetiche sul panorama internazionale, ed in particolare nei riguardi della Pubblica Amministrazione, AGID ha

sviluppato il documento delle Misure minime per la sicurezza ICT delle Pubbliche amministrazioni che fornisce indicazioni puntuali su come raggiungere livelli di sicurezza prefissati a partire da quello minimo, obbligatorio per tutti. Tale documento è stato emesso con Circolare n. 2 del 18 aprile 2017, pubblicata in Gazzetta Ufficiale (serie generale) n. 103 del 5 maggio 2017 ed è divenuto quindi obbligatorio riferimento normativo per tutte le amministrazioni, che avrebbero dovuto garantire la propria conformità entro il 31/12/2017.

Nel corso del 2017 AGID, tramite il CERT-PA, ha attivato un progetto per la sperimentazione delle modalità di scambio automatico di informazioni operative (indicatori di compromissione) tra strutture di sicurezza mediante protocolli STIX e TAXII tramite piattaforme per la raccolta, l'archiviazione, la distribuzione e la condivisione di indicatori di sicurezza informatica e minacce relative all'analisi degli incidenti di sicurezza informatica. Tale sperimentazione, che comprende due Gruppi di lavoro dedicati rispettivamente agli aspetti tecnici ed alla definizione di una tassonomia ad hoc, ha lo scopo di produrre le specifiche tecniche ed organizzative che verranno emanate come standard per la realizzazione di un sistema nazionale di interscambio automatico di indicatori di compromissione qualificati tra operatori accreditati.

Nel corso del 2017 AGID, tramite il CERT-PA, ha provveduto a sviluppare ulteriormente il *National Vulnerability Database* gestito tramite la piattaforma Infosec. Quest'ultima è stata potenziata ed arricchita di funzionalità nonché messa sperimentalmente a disposizione di tutte le amministrazioni in sola consultazione. Le statistiche di accesso hanno mostrato come Infosec sia rapidamente diventato una piattaforma tecnica di riferimento da parte della comunità nazionale ed internazionale di analisti, evidenziando un numero significativo e sempre crescente di accessi dall'estero (il monitoraggio sulla gestione della sicurezza informatica nella PA è disponibile nella sezione Avanzamento trasformazione digitale del sito AGID).

8.2 Obiettivi

- Definire i profili di sicurezza dei componenti ICT della Pubblica Amministrazione e, a valle di una specifica analisi del rischio, fornire i riferimenti tecnici e normativi che le pubbliche amministrazioni dovranno adottare. La mancata attuazione dei profili di sicurezza potrebbe comportare, proporzionalmente al tipo di inadempimento, anche la necessità di interrompere l'erogazione dei servizi connessi;
- offrire alle pubbliche amministrazioni supporto alla prevenzione e al trattamento degli incidenti di sicurezza informatica;

- provvedere a effettuare *assessment* e verifiche di sicurezza onde accertare l'applicazione delle regole di sicurezza informatica individuate da parte delle pubbliche amministrazioni;
- elaborare e pubblicare un modello organizzativo standard per la realizzazione di "CERT di prossimità", ossia CERT di secondo livello sia "orizzontali" (territoriali) che "verticali" (tematici o di settore), il quale costituirà il riferimento normativo per la eventuale costituzione di tali strutture aventi funzione di snodo tra il CERT-PA e le amministrazioni locali;
- elaborare e pubblicare lo standard nazionale per l'interscambio automatizzato tra operatori accreditati (CERT, strutture di sicurezza) di informazioni di sicurezza e indicatori di compromissione qualificati mediante protocolli STIX e TAXII, utilizzando piattaforme per la raccolta, l'archiviazione, la distribuzione e la condivisione di indicatori di sicurezza informatica e minacce relative all'analisi degli incidenti di sicurezza informatica e all'analisi del *malware*, e adottando la tassonomia specificamente definita;
- potenziare ulteriormente il *National Vulnerability Database* e i relativi strumenti informativi a supporto, mettendo a disposizione delle amministrazioni e dei ricercatori funzionalità più estese per il supporto all'analisi ed alle ricerche.

Al fine di raggiungere gli obiettivi del Piano, AGID ed il CERT-PA provvederanno a:

- emanare linee guida finalizzate ad accrescere il livello di consapevolezza e di protezione della Pubblica Amministrazione;
- emanare standard e norme tecniche di riferimento che le amministrazioni dovranno seguire per innalzare il proprio livello di *preparedness* e di risposta agli incidenti cibernetici e rafforzare altresì la cooperazione globale tra le strutture volte alla protezione dello spazio cibernetico nazionale. Tra questi:
    - lo standard tecnico per l'interscambio automatico tra operatori accreditati di indicatori di compromissione qualificati, utilizzando i protocolli STIX e TAXII, e le tassonomie sviluppate *ad hoc*;
    - il modello organizzativo standard per la realizzazione dei "CERT di prossimità" (territoriali o tematici) da parte delle pubbliche amministrazioni interessate.
- monitorare il livello di applicazione delle Misure minime di sicurezza ICT da parte delle pubbliche amministrazioni, continuando a fornire alle amministrazioni supporto interpretativo e guida all'applicazione, e valutando l'opportunità di provvedere ad un loro eventuale aggiornamento in funzione delle evoluzioni del settore;
- incrementare ulteriormente la capacità operativa del CERT-PA, in termini sia di personale che di infrastrutture tecniche e risorse elaborative, anche in vista degli

adempimenti che si renderanno necessari a seguito del recepimento da parte dell'Italia della Direttiva NIS[12];

- sviluppare ulteriormente la *Cyber Security Knowledge Base* nella quale sono raccolte le informazioni sugli eventi di sicurezza occorsi nel tempo all'interno delle PA;
- sviluppare ulteriormente il *National Vulnerability Database* (NVD), catalogo delle vulnerabilità informatiche che integra i cataloghi disponibili a livello internazionale (ad es. MITRE) con le vulnerabilità riscontrate sui sistemi sviluppati in ambito nazionale;
- continuare a rendere prontamente disponibili strumenti e informazioni utili per prevenire e rispondere ad eventuali attacchi informatici;
- continuare a fornire supporto alle amministrazioni nella predisposizione di risposte agli incidenti;
- continuare a fornire supporto alle amministrazioni e approfondire la funzione di monitoraggio dello spazio cibernetico delle pubbliche amministrazioni anche attivando ulteriori collaborazioni con le comunità di riferimento nazionali ed internazionali oltre quelle già in corso;
- continuare a fornire supporto alle amministrazioni nella gestione degli incidenti e nel successivo ripristino.

8.3 Linee di azione

LA55 - CERT-PA - Ampliamento capacità operativa

Tempi In corso

Attori AGID

Descrizione CERT-PA, operante dal 2013, aumenterà progressivamente la sua capacità operativa, rafforzando l'infrastruttura ICT di erogazione dei servizi di base e potenziando il primo sistema informativo sulle minacce cibernetiche (*Cyber Security Knowledge Base*), anche attraverso l'implementazione delle soluzioni Infosharing CERT-PA e *National Vulnerability Database*(NVD).

[12] A livello europeo, è opportuno citare la proposta di regolamento "*Cybersecurity Act*" riguardante ENISA, l'Agenzia di Cibersicurezza UE, e la creazione di un quadro europeo di certificazione per i prodotti di sicurezza ICT (COM (2017) 477), ancora in fase di negoziato.

Risultati Ampliamento della propria *constituency,* gestione della piattaforma di *infosharing* in modalità autonoma da parte delle amministrazioni accreditate. Costituzione del NVD tramite la piattaforma Infosec.

Aree di intervento Nel breve periodo, impatto sulle PA.

LA56 - CERT-PA - Piattaforma Infosec

Tempi Giugno 2019

Attori AGID

Descrizione CERT-PA ridisegna e rende disponibile la piattaforma Infosec al fine di offrire un supporto altamente tecnico per gli analisti di sicurezza. La piattaforma sarà punto di riferimento tecnico operativo e informativo per tutte le PA.

Risultati Rilascio della piattaforma (luglio 2019).

Aree di intervento Nel breve periodo, impatto sulle PA.

LA57 - Adeguamento delle PA agli standard Trasmissione automatizzata IoC

Tempi In corso

Attori AGID, PA

Descrizione Definizione degli standard per la trasmissione automatizzata degli indicatori di compromissione (IoC), emanazione delle linee guida del modello architetturale per la trasmissione automatizzata degli IoC.

Le PA, al fine di aderire all'architettura per la trasmissione automatizzata degli IoC, adottano gli standard emanati e predispongono un piano di adeguamento e realizzano i servizi nel rispetto delle Linee guida.

Risultati Emanazione standard e Linee guida del modello architetturale di gestione della trasmissione automatizzata degli IoC (settembre 2019).

Piano di adeguamento delle amministrazioni (dicembre 2019).

Aree di intervento Nel breve periodo, impatto sulle PA.

LA58 - Realizzazione piattaforma nazionale della PA per la trasmissione automatizzata degli IoC

Tempi In corso

Attori AGID, PA

Descrizione AGID realizza, in via sperimentale, per le pubbliche amministrazioni, una piattaforma nazionale di trasmissione automatizzata degli IoC.

Risultati Al fine di poter utilizzare tale piattaforma, le PA adottano gli standard emanati e predispongono le proprie infrastrutture all'utilizzo della piattaforma secondo gli standard e le Linee guida emanate da AGID (luglio 2019).

Aree di intervento Nel breve periodo, impatto sulle PA.

LA59 - Segnalazioni incidenti Informatici al CERT-PA

Tempi In corso

Attori PA

Descrizione Tutte le pubbliche amministrazioni sono tenute a monitorare e segnalare prontamente al CERT-PA gli incidenti informatici e ogni situazione di potenziale rischio, utilizzando i canali di comunicazione riportati nella sezione dedicata del sito AGID. Per tutti i soggetti accreditati su *Infosharing* CERT-PA è disponibile un'apposita funzionalità di segnalazione.

Risultati Attività ricorrente.

Aree di intervento Nel breve periodo, impatto sulle PA.

LA60 - Emanazione Linee Guida di sicurezza cibernetica per le PA

Tempi In corso

Attori AGID, PA

Descrizione A supporto e complemento delle Misure minime di sicurezza ICT, documento di natura prescrittiva che indirizza adempimenti tecnici puntuali, AGID emana documenti che indirizzano i temi strategici, organizzativi ed operativi necessari alle PA per innalzare il proprio livello di sensibilità, conoscenza, preparazione e capacità di risposta relativamente alla crescente minaccia cibernetica.

Risultati Emanazione delle Linee guida di sicurezza cibernetica per le PA (entro dicembre 2019).

Aree di intervento Nel breve periodo, impatto sulle PA.