La sicurezza informatica del Paese, tra nuova governance nazionale e Agenda digitale

Il ruolo della PA, il progetto digital security e la componente Sicurezza del piano triennale

Francesco Tortorelli – responsabile direzione Pubblica amministrazione e vigilanza

FORUM PA 15 Maggio 2019

AgID: ruoli e attività

- **Indirizzo e coordinamento delle PA**
- **Avvio di progetti di innovazione**
- **Regolatorio**
- **Vigilanza e controllo**
- **Supporto e assistenza alle PA**
- **Gestione di infrastrutture di uso comune**

AgID: principali attività relative alla sicurezza ICT

	Ambito PA	Ambito generale
AgID		**Emanazione di Linee Guida**
	Definizione di azioni nel piano triennale per l'informatica delle PA	
	Supporta Consip nella **definizione dei requisiti di sicurezza** per le gare strategiche (Cloud, S-RIPA, servizi di Sicurezza)	
		Vigilanza sui Trusted Services (Qtsp eIDAS, PEC, SPID, Conservatori)
	Servizi sussidiari per la gestione della sicurezza	
AgID CERT -PA	**Servizi proattivi** di allertamento	
	Supporto alla gestione e risposta agli incidenti di sicurezza	
		Early warning tramite avvisi e bollettini di sicurezza
		Infosec Fornisce statistiche e dati analitici su Pattern di attacco, Vulnerabilità e IoC
	Vulnerability assessment	

Gli obiettivi di sicurezza del piano triennale (cap. 8)

AgID è impegnata nel rafforzamento della propria capacità operativa e nel miglioramento degli strumenti a disposizione, nonché nell'emanazione di linee guida

13.6 Indicazioni relative alla sicurezza

2019

- Le PA devono garantire la propria conformità alle "Misure minime per la sicurezza ICT delle Pubbliche amministrazioni" di AGID.
- Le PA, al fine di aderire all'architettura per la trasmissione automatizzata degli IoC (indicatori di compromissione), adottano gli standard emanati da AGID e predispongono un piano di adeguamento realizzando i servizi nel rispetto delle linee guida.
- Le PA monitorano e segnalano al CERT-PA gli incidenti informatici e ogni situazione di potenziale rischio, utilizzando i canali di comunicazione sul sito AGID.

2020

- Le PA seguono le indicazioni contenute nelle linee guida di sicurezza cibernetica adottate da AGID

Il CERT-PA

Creato nel 2013 (sulla base dell'esperienza del precedente CERT-SPC), inizio operatività dal 2015, avvio del primo nucleo di servizi nel 2016

Constituency

- Pubbliche Amministrazioni Centrali, Regioni, Città Metropolitane (**68 Amministrazioni accreditate**)

- Monitoraggio di tutti i domini .gov.it **~22.000 Amministrazioni**

Attività

- Analisi OSINT/CLOSINT su fonti qualificate aperte/semiaperte
- Segnalazioni Gestite **~3600**
- IoC(Indicatori di Compromissione) acquisiti ed elaborati **~7.400.000**
- IoC qualificati emessi **~64.900 IoC** qualificati (~**19.600** IP, ~**45.300** URL)
- Malware analizzati **~27.000**

OLTRE 5 INCIDENTI SEGNALATI AL CERT-PA DI MEDIA AL GIORNO

4,4 FILE DI DATI SOTTRATTI RECUPERATI AL GIORNO DI MEDIA

OLTRE 50 MALWARE ANALIZZATI DI MEDIA AL GIORNO

Linee Guida CERT Regionali (dal 14.5.19 in consultazione pubblica)

Il documento descrive gli aspetti significativi da considerare per poter avviare e gestire un CERT e che potranno essere presi a riferimento per la costituzione di CERT regionali.

Normative Applicabili

Struttura Amministrativa Organizzativa

Risorse Necessarie

Linee Guida CERT - Regionali

Catalogo Servizi da Erogare

Modalità di Analisi e Valutazione Risultati

Requisiti di Sicurezza Logica e Fisica da implementare

Piano di Attuazione

Linee Guida Sicurezza nel Procurement

(dal 14.5.19 in consultazione pubblica)

Il documento, **realizzato su mandato del DIS-NSC e con la collaborazione delle amministrazioni NSC e di Consip**, illustra in maniera semplice e fruibile la problematica della sicurezza nel Procurement ICT, presentando buone prassi e soluzioni già in uso, per verificare il livello di sicurezza degli attuali processi al fine di innalzarne il livello senza aumentare in modo eccessivo la complessità dei processi.

Le Azioni sono state numerate come pure i requisiti di sicurezza eleggibili per le gare.

Alcune matrici di correlazione e applicabilità rendono più semplice l'applicazione delle linee guida e la loro pertinenza con il contesto di applicazione.

Linee Guida Sicurezza nel Procurement /2

1.1: **Indicazioni per le amministrazioni**

Azioni da compiere nelle varie fasi del processo di acquisizione, requisiti da capitolato, suggerimenti da declinare per le varie tipologie di acquisizione

- **Azioni da svolgere prima della fase di procurement**
  (es. classificazione di sistemi/servizi per criticità, definizione metodologie generali, piani di contingenza, formazione, politiche per il personale, sensibilizzazione decisori, ecc.)
- **Azioni da svolgere in fase di procurement**
  (scrittura documentazione di gara, formazione commissioni, scelta criteri per l'ammissione e l'assegnazione dei punteggi, ecc.)
- **Azioni da svolgere dopo la stipula del contratto**
  (aspetti di cui tener conto in operatività o a posteriori, dopo la chiusura del contratto)

1.2 Indicazioni per AgID

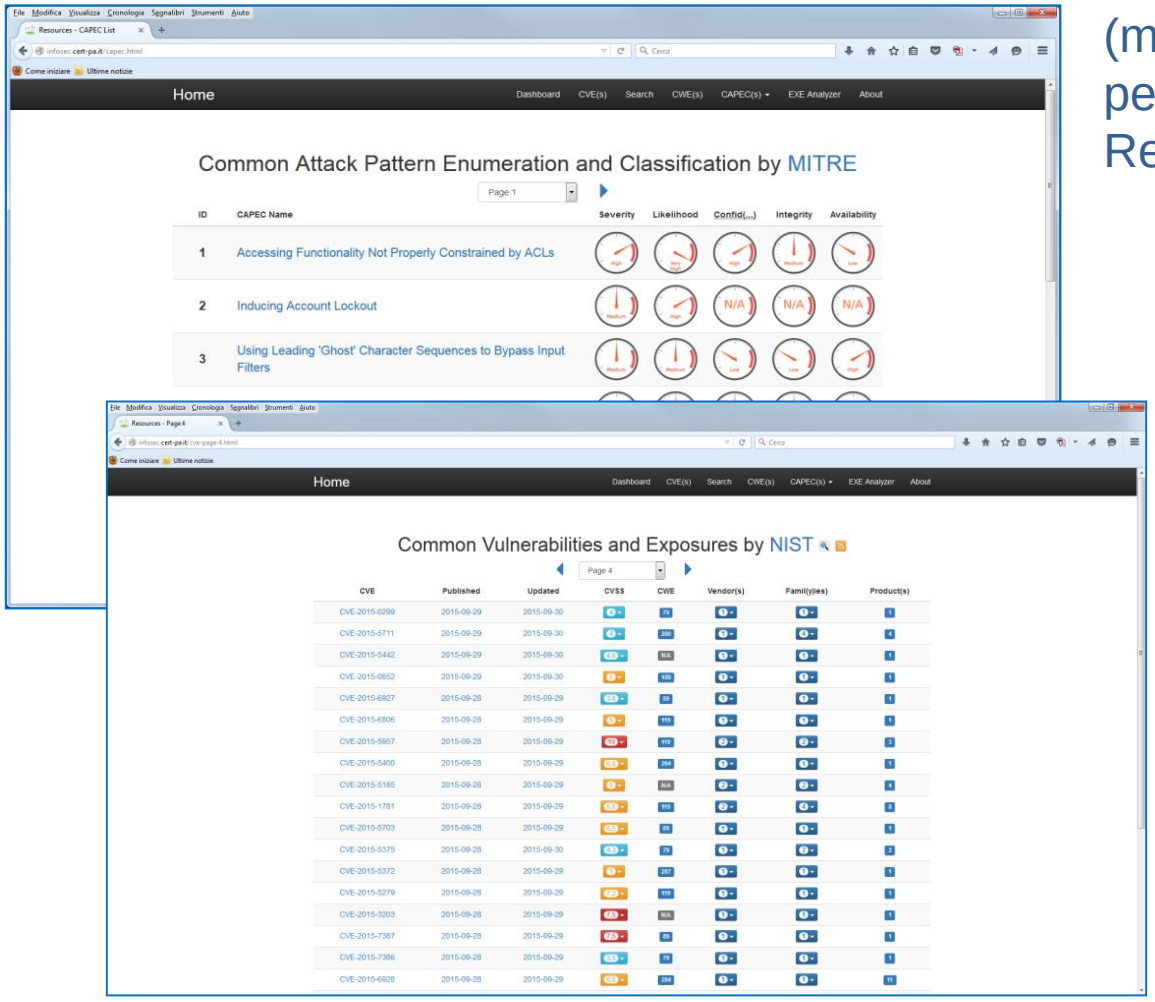
Di cosa l'Agenzia può farsi carico a normativa vigente (Pareri e monitoraggio)

1.3 Indicazioni per le centrali di committenza

Ciò che Consip e le altre c.d.c. possono svolgere per rendere più sicuro il procurement ICT

Tool a disposizione di tutti: Infosec (*)

(*) **è stato inserito** dai ricercatori della comunity internazionale di ricerca Cyber Security (Awesome Malware Analysis) **nella lista dei migliori sistemi di analisi di malware.** In particolare al quarto posto dei Malware Corpora,



(miglior repository di samples per analisi) e al nono posto per Related Awesome Lists

Elemento centrale per il National Italian Vulnerability Database

Fornisce statistiche e dati analitici su Pattern di attacco, Vulnerabilità e IoC (Indicatori di compromissione)

Disponibile a tutti (in consultazione) su infosec.cert-pa.it

Metodologia di Cybersecurity Risk Management

Messa a disposizione delle PA da AgID

1 Metodologia di Cyber Risk Management personalizzata per la PA italiana

La metodologia è stata sviluppata a partire dalla IRAM2 dell'ISF e dai principi della ISO31000, e contestualizzata per l'ecosistema della PA italiana.

2 Knowledge base nazionale per la valutazione del Rischio Derivato

Il tool consente anche di calcolare e valutare il rischio derivante dall'utilizzo di servizi trasversali nazionali e locali.

3 Integrazione con servizi nazionali

Il tool è integrato con i servizi nazionali quali ad esempio SpID, il database di servizi della PA denominato «servizi.gov.it», etc….

4 Azioni di trattamento integrate con convenzioni nazionali attive

Il tool fornisce in output un report delle azioni di trattamento necessarie a fronte dei rischi individuati, con indicazione delle relative convenzioni pubbliche attive.

5 Gestione avanzata di utenti e ruoli (ABAC)

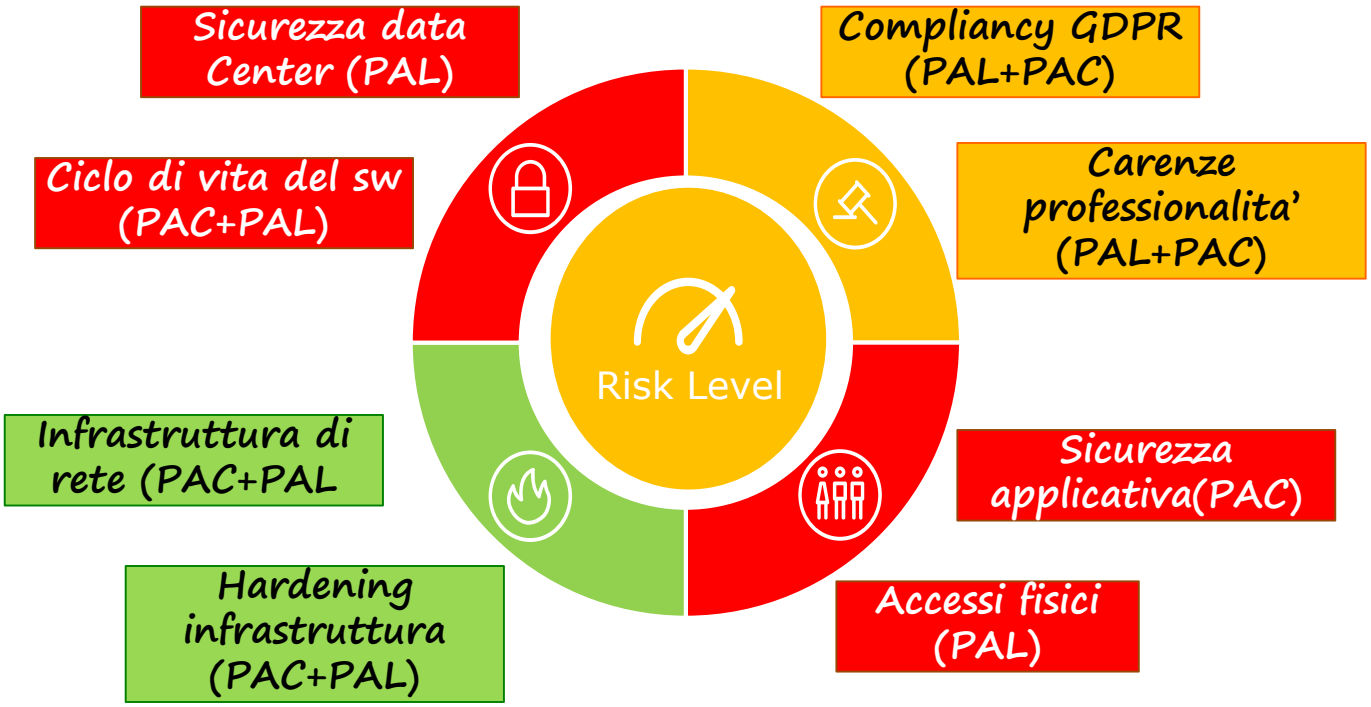
Il tool consente di gestire gli accessi degli utenti alle varie funzionalità, in base agli attributi assegnati.

6 Statistiche e Trend

Sui dati inseriti è possibile effettuare analisi e statistiche a livello puntuale e generale (e.g. trend annuale dei rischi della PA).

Tool Risk Assessment

Livelli di rischio riscontrati per tipologia di PA



44 PA analizzate: 11 PAC, 11 Regioni, 3 città metropolitane e 19 PAL
e altri 10 enti in corso di attivazione

Gestione automatizzata degli IoC

- **A Luglio pv** AgID rilascerà, ad un primo nucleo della propria Constituency, una **piattaforma per la trasmissione e la gestione automatizzata di IoC** (Indicatori di Compromissione) validati e certificati dal CERT-PA.
- Basata sugli **standard STIX e TAXII** la piattaforma permetterà di ricevere gli **IoC**, elaborati dal sistema di analisi malware Infosec (realizzato da AgID), garantendo la possibilità acquisire automaticamente e in **real time** informazioni utili al contrasto delle minacce cyber nel contesto italiano e del dominio PA.
- Nei circa tre mesi di erogazione in test del servizio, la piattaforma ha raccolto 28.000 IoC validati e accessibili ad un GdL pilota composto da 5 organizzazioni tra PA e Aziende Private.

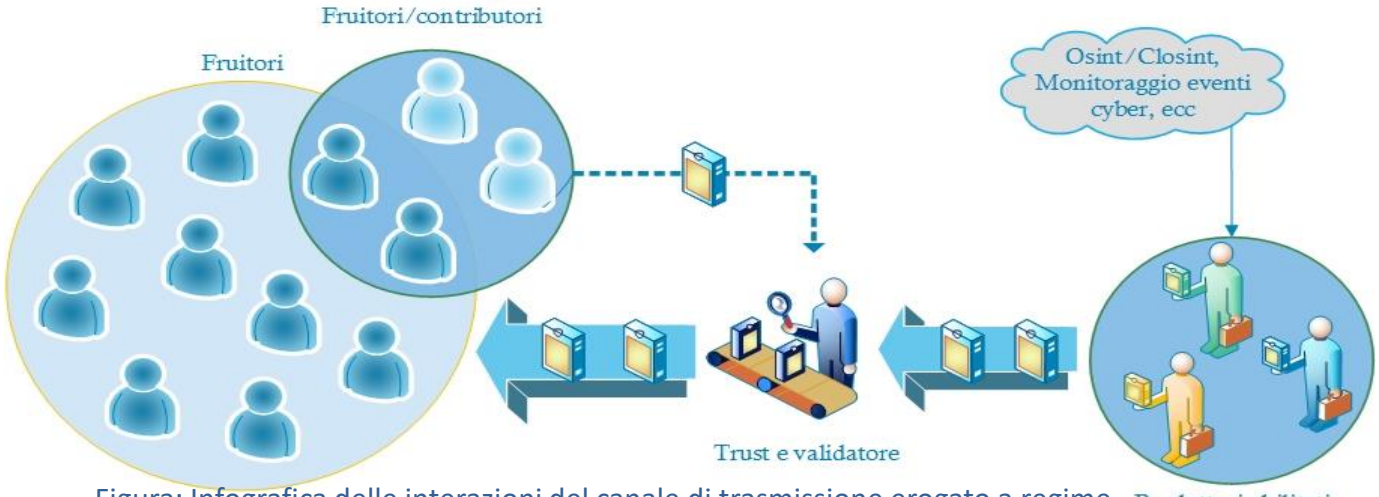


Figura: Infografica delle interazioni del canale di trasmissione erogato a regime.

AGID | Agenzia per l'Italia Digitale

Il Paese che cambia passa da qui.

agid.gov.it

Link

Linee guida in consultazione :

- Procurement: https://docs.italia.it/AgID/documenti-in-consultazione/lg-procurement-ict/it/bozza/
- Cert locali: https://docs.italia.it/AgID/documenti-in-consultazione/lg-cert-regionali/it/bozza/

Sito pubblico CERT-PA : https://www.cert-pa.it/

Infosec : https://infosec.cert-pa.it/

Dati sicurezza : https://avanzamentodigitale.italia.it/it/progetto/digital-security-cert-pa/

Piano triennale : https://www.agid.gov.it/it/agenzia/piano-triennale