Audizione informale

in relazione all'esame del disegno di legge C. 2100 Governo recante conversione in legge del decreto legge n. 105 del 2019 recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica

Teresa Alvaro

Direttore Generale

10 Ottobre 2019

AGID

Agenzia per l'Italia Digitale

Il ruolo di AgID per la cyber security

Secondo il **Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico** e il relativo **Piano Nazionale** (a cura del DIS), AgID svolge un ruolo nell'attuazione di iniziative tecniche ed organizzative volte sia a migliorare la consapevolezza della Pubblica Amministrazione nei riguardi della minaccia informatica, sia ad aumentarne le capacità di prevenzione, protezione e risposta agli incidenti di sicurezza informatici.

- **Il Piano Nazionale 2017 attribuisce ad AgID il compito di:**
  - ✓ *dettare indirizzi;*
  - ✓ *emanare regole tecniche e linee guida in materia di sicurezza informatica e di omogeneità degli standard;*
  - ✓ *assicurare la qualità tecnica e la sicurezza dei sistemi informativi pubblici e della loro rete di interconnessione;*
  - ✓ *monitorare i piani ICT delle amministrazioni pubbliche.*

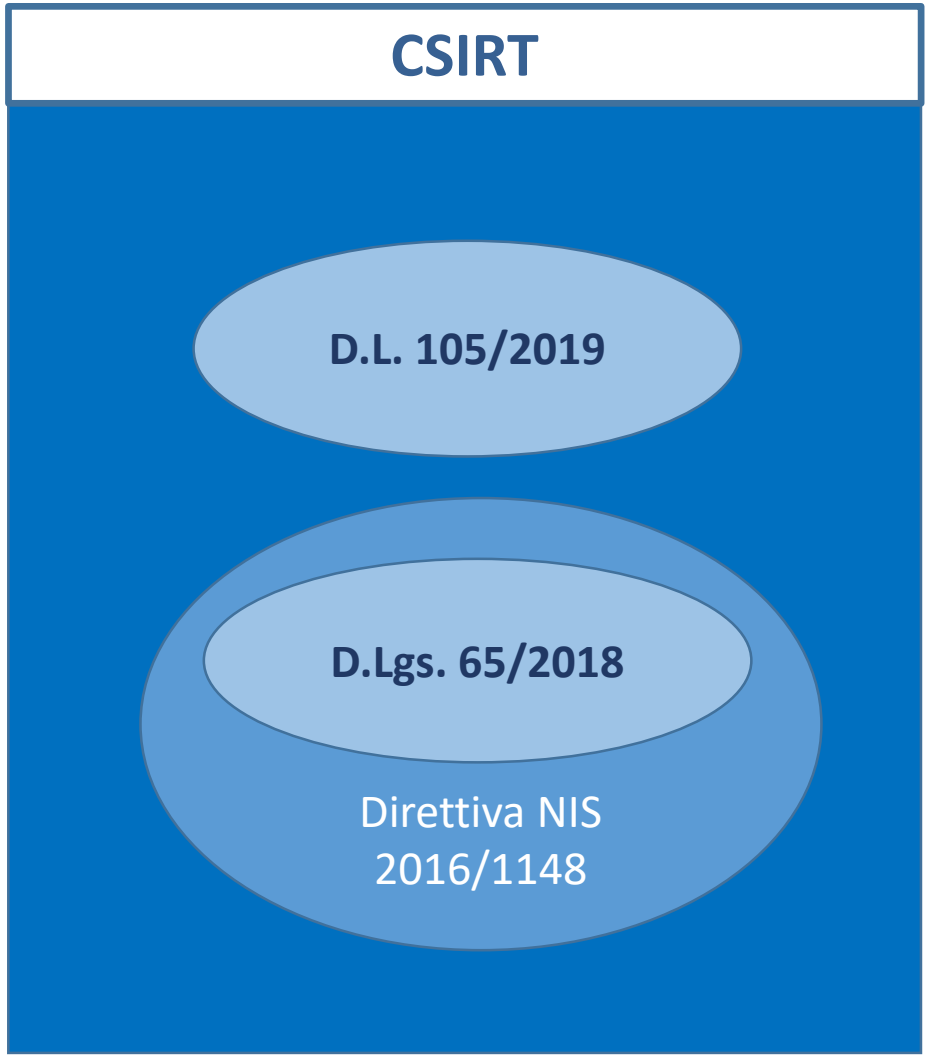
- **Il Codice dell' Amministrazione Digitale (CAD) attribuisce ad AgID**, tra l'altro, il compito di emanare linee attuative riguardo aspetti di sicurezza e continuità operativa dei sistemi.

- **Il Piano Triennale 2019-2021 per l'informatica nella PA al cap. 8 prevede che AgID:**
  - ✓ aggiorni le Misure Minime di sicurezza ICT in funzione delle evoluzioni del settore
  - ✓ emani le Linee Guida Sicurezza nel Procurement ICT
  - ✓ realizzi il National Vulnerability Database
  - ✓ realizzi la Piattaforma per la condivisione indicatori compromissione ed eventi cyber

D.L. 105/2019: aspetti qualificanti

- ✓ L'impianto normativo del D.L. 105/2019, in correlazione con la Direttiva NIS 2016/1148 e il relativo D.Lgs. 65/2018 di attuazione, **individua un perimetro di sicurezza cibernetica anche in capo alle amministrazioni, agli enti e agli operatori nazionali pubblici.**

- ✓ **L'individuazione di un unico soggetto (CSIRT)** per la **ricezione delle notifiche degli incidenti di sicurezza all'interno del perimetro**, così come già previsto dal D.Lgs. 65/2018 per le notifiche da parte degli operatori di servizi essenziali e i fornitori di servizi digitali, sebbene con alcune differenze.



D.L. 105/2019: punti di attenzione

- ✓ L'art. 12, comma 5 del D.Lgs. 65/2018 stabilisce che gli operatori dei servizi essenziali sono tenuti a **notificare allo CSIRT** gli **incidenti** di sicurezza aventi un **impatto rilevante sulla continuità dei servizi essenziali forniti**; in base all'esperienza maturata dal CERT-PA, si richiama l'attenzione sull'opportunità che il D.L. 105/2019 preveda che gli **operatori del perimetro segnalino ogni incidente** sia per disporre di una maggiore base informativa a disposizione del perimetro, sia per evitare valutazioni «incerte/soggettive» sulla portata dell'impatto

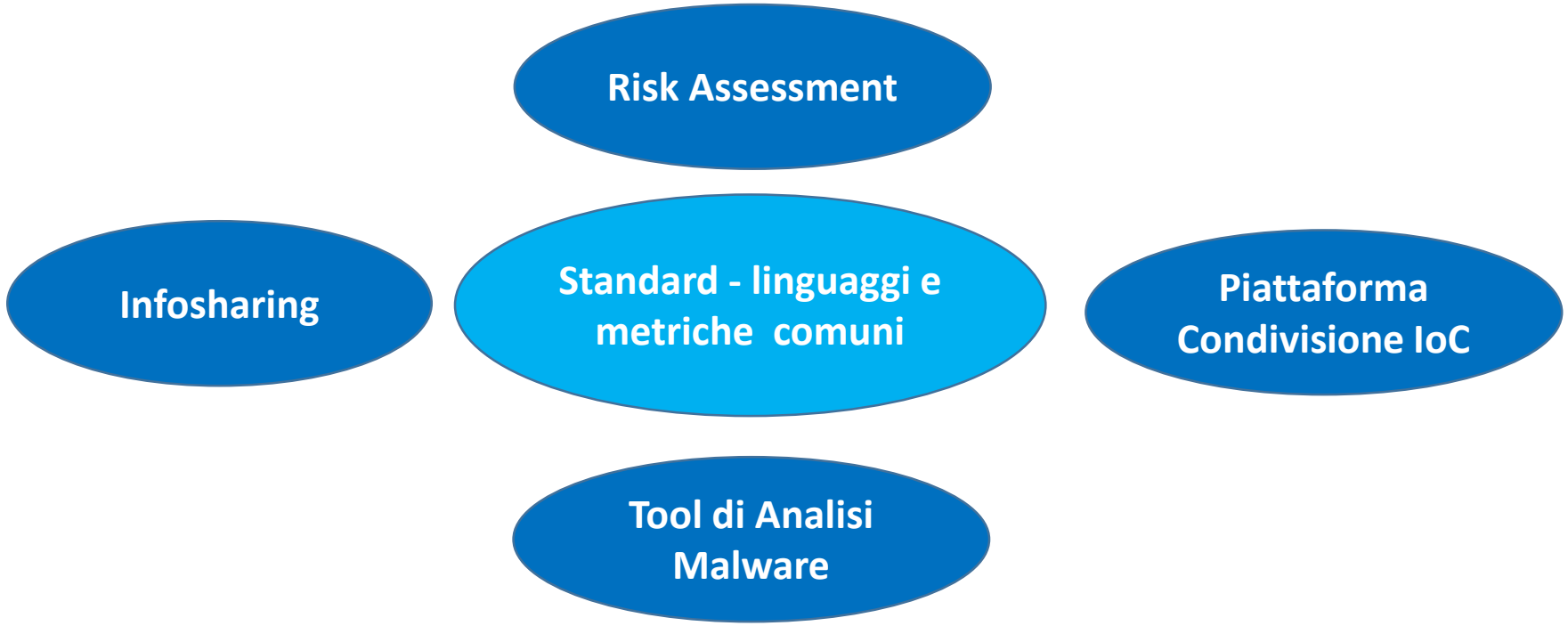
- ✓ **L'art.1, comma 12 del D.L.** individua la Presidenza del Consiglio dei Ministri quale autorità competente per l'accertamento delle violazioni e per l'irrogazione delle sanzioni nei confronti di:
  a) soggetti pubblici;
  b) soggetti di cui all'articolo 29 del D. Lgs. 82/2005 (CAD), ovvero:
     - fornitori servizi fiduciari qualificati ai sensi del regolamento EIDAS (firme, sigilli, marche temporali…)
     - Gestori di identità digitali e PEC
     - Conservatori di documenti informatici

  Si evidenzia la **sovrapposizione delle attività (vigilanza e sanzioni**) nei riguardi delle categorie di **soggetti al punto b) con quelle già esercitata da AgID ai sensi e per gli effetti dell'art. 32-bis CAD (vigilanza e sanzioni)**

- ✓ **l'art.1 comma 16 del D.L**. prevede che *"La Presidenza del Consiglio dei Ministri, per lo svolgimento delle funzioni di cui al presente decreto può avvalersi dell'Agenzia per l'Italia Digitale (AgID) sulla base di apposite convenzioni, nell'ambito delle risorse finanziarie e umane disponibili a legislazione vigente, senza nuovi o maggiori oneri per la finanza pubblica…"*; **non definendo i limiti dell'avvalimento, tale dispositivo può risultare impraticabile**.

D.L. 105/2019: proposte

- ✓ Dall'esperienza maturata dal CERT-PA di AgID, per prevenire i rischi di sicurezza e contrastare le minacce informatiche, rivestono un ruolo di fondamentale importanza anche Strumenti e Tool dedicati
- ✓ Il decreto in oggetto dovrebbe prevedere risorse per dotarsi di tali strumenti e richiedere che le entità del perimetro condividano le informazioni di sicurezza attraverso l'uso di tali strumenti



D. L. 105/2019

PREVEDE

- ✓ Linee Guida
- ✓ Notifica Incidenti
- ✓ Vigilanza

Cosa è stato fatto: linee guida La sicurezza nel Procurement ICT

Le **Linee guida «La sicurezza nel procurement ICT»** sono il prodotto finale delle attività di un gruppo di lavoro promosso dal Nucleo per la Sicurezza Cibernetica (NSC) e **coordinato da AgID** al quale hanno partecipato i rappresentanti delle amministrazioni facenti parte del CISR e Consip.

Le linee guide saranno emanate ai sensi del CAD secondo l'iter previsto (già effettuata la consultazione pubblica):

- ✓ **forniscono** indicazioni operative su come affrontare la sicurezza nel ciclo del procurement ICT;
- ✓ **stabiliscono una semantica comune** delle definizioni e dei concetti relativi alla sicurezza nel procurement ICT, rendendoli coerenti con la normativa e con il contesto della pubblica amministrazione;
- ✓ **mettono a disposizione** buone prassi**,** strumenti operativi, esempi pratici, riferimenti puntuali, per verificare il livello di sicurezza dei processi di acquisizione e per elevare tale livello.

Cosa è stato fatto: Metodologia di Cybersecurity Risk Management e Tool

Sviluppati da AgID e disponibili per tutte le PA

Il tool e la metodologia, opportunamente configurato/adattata, potrebbero essere **riusati dalle entità del perimetro** per **valutare con standard/metodologie/criteri comuni il rischio cyber**

Ad oggi utilizzati da	
20 amministrazioni centrali	48 Comuni
15 Regioni	4 ASL e Ospedali
5 Città metropolitane	6 Scuole & Università
3 Consorzi di comuni	6 Province

1 **Metodologia di Cyber Risk Management personalizzata**
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 (SPID, il database di servizi della PA «servizi.gov.it»,…)

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 **Statistiche e trend**
I dati disponibili sono anche utilizzati per analisi e statistiche a livello puntuale e generale (e.g. trend annuale dei rischi della PA).

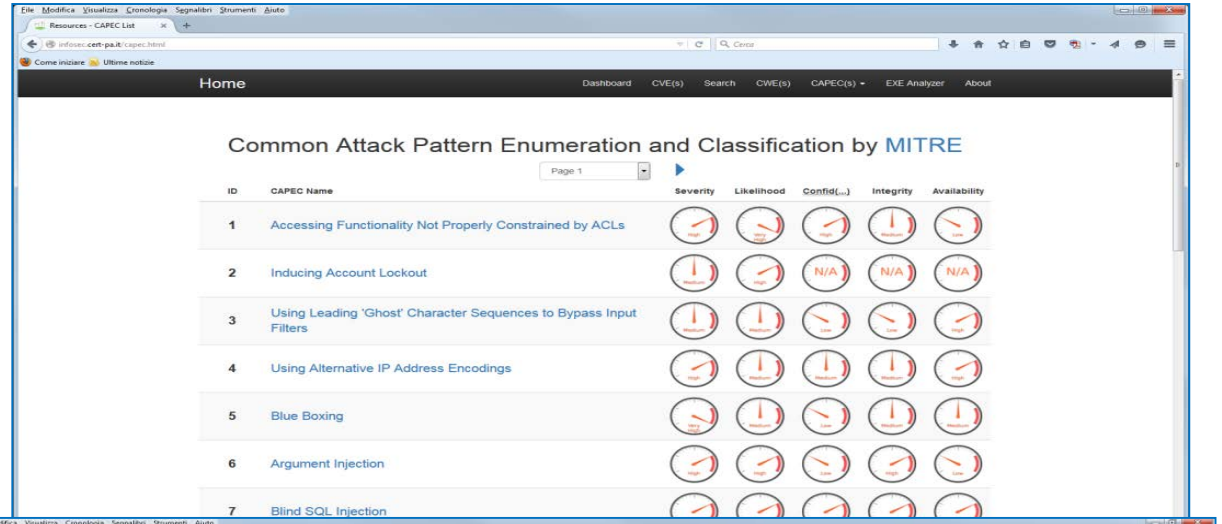
Cosa è stato fatto: servizi e strumenti di contrasto alle minacce Cyber

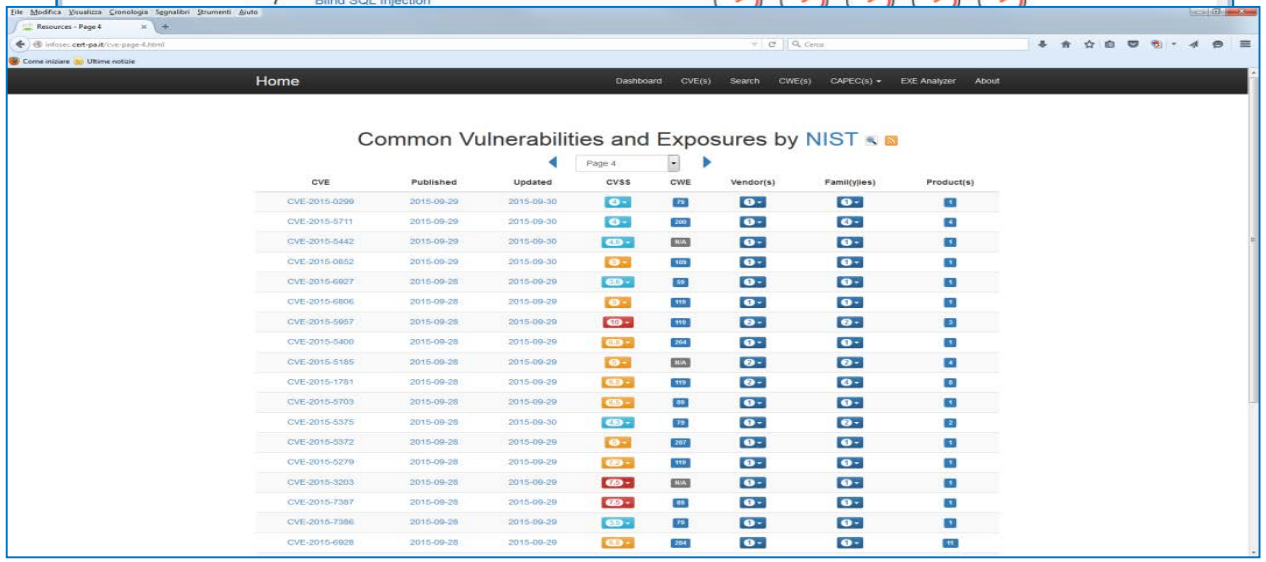
National Vulnerability Database è stato implementato tramite la piattaforma **Infosec realizzata da AgID**

La Piattaforma Infosec

- ✓ **Acquisisce, processa, correla** e produce report statistici e dati analitici su Pattern di Attacco, Vulnerabilità e IoC
- ✓ **70% degli accessi in consultazione dall'estero**
- ✓ è stata censita nella lista di strumenti e risorse "Awesome Malware Analysis" tra i migliori repository di analisi di malware (Malware Corpora) e tra i siti più affidabili da cui ricevere le liste di distribuzione per gli IoC

Infosec potrebbe essere utilizzata dalle entità individuate nel perimetro di sicurezza



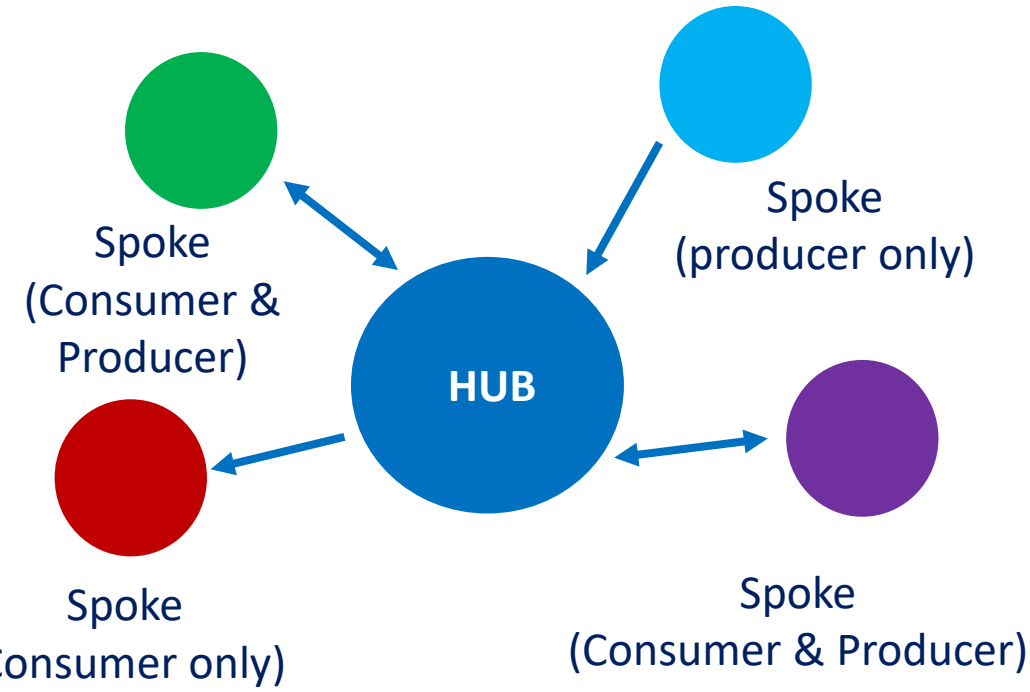


Cosa è stato fatto: Piattaforma per la Condivisione IoC ed Eventi Cyber

La Piattaforma **raccoglie**, **archivia**, e **condivide gli indicatori di compromissione** e gli **eventi cyber emersi dall'analisi degli incidenti di sicurezza informatica.**

La piattaforma opera in tempo reale in modalità «machine to machine» per reagire in maniera dinamica alle minacce.

Ad oggi la piattaforma ha già veicolato circa 10.000 tra IoC e eventi cyber.



Risultato di uno sviluppo sperimentale condotto da un gruppo ristretto di aziende private e pubbliche amministrazioni guidato da CERT-PA nel 2018-19.
Entro il 2019 si concluderà la fase preliminare di utilizzo a cui hanno partecipato 10 soggetti pubblici e 2 privati.
Dal 2020 sarà disponibile per tutte le Pubbliche Amministrazioni e soggetti qualificati (CERT Regionali, società in house).

L'estensione della piattaforma alle entità del perimetro permetterebbe di raggiungere un **elevato livello di automazione e dinamicità** nella gestione degli eventi Cyber, per una **protezione in tempo reale**.