Architettura Nazionale Cyber Security

Indice

- Le basi normative
- Il Decreto Gentiloni
- Il recepimento della Direttiva NIS
- La nascita del CSIRT
- Perimetro di sicurezza nazionale cibernetica
- Overview
- Ecosistema cyber italiano

Le basi normative

- **DPCM 17 febbraio 2017 (Decreto Gentiloni)**
- **Dlgs. 65/2018 (Recepimento della Direttiva NIS)**
- **Decreto del Presidente del Consiglio dei Ministri 8 agosto 2019**
- **Perimetro di sicurezza nazionale cibernetica, legge di conversione 18 novembre 2019, n. 133**

Il Decreto Gentiloni

- **DPCM 17 febbraio 2017 (Decreto Gentiloni)**

Centralità del Presidente del Consiglio dei ministri (art. 2) quale vertice del Sistema di informazione per la Sicurezza della Repubblica

- convoca il CISR in situazioni di crisi che coinvolgono la sicurezza nazionale
- adotta su proposta del CISR il quadro strategico nazionale per la sicurezza dello spazio cibernetico
- Adotta su deliberazione del CISR, il Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionale
- Impartisce, sentito il CISR, le direttive al DIS.

Il Decreto Gentiloni

- **CISR (art. 4)**
  - Partecipa in caso di crisi cibernetica alle determinazioni del Presidente con funzioni di consulenza e di proposta
  - Esprime parere sulle direttive del Presidente
  - approva linee di indirizzo per favorire l'efficace collaborazione tra i soggetti istituzionali e gli operatori privati interessati alla sicurezza cibernetica
  - promuove l'adozione delle iniziative necessarie per assicurare, in forma coordinata, la piena partecipazione dell'Italia ai diversi consessi di cooperazione internazionale
  - formula le proposte di intervento normativo ed organizzativo ritenute necessarie al fine del potenziamento delle misure di prevenzione e di risposta alla minaccia cibernetica e quelle per la gestione delle crisi.

Il Decreto Gentiloni

- **CISR Tecnico (art. 5)**
  - svolge attività preparatorie delle riunioni del CISR
  - Coordina la formulazione delle identificazioni necessarie allo svolgimento delle attività di individuazione delle minacce alla sicurezza dello spazio cibernetico, al riconoscimento delle vulnerabilità, nonché per l'adozione di best practices e misure di sicurezza.

Il Decreto Gentiloni

- **NSC (artt. 8-9)**
  - presieduto da un Vice Direttore generale del DIS, ed è composto dal Consigliere militare e da un rappresentante del DIS, dell'AISE, dell'AISI, del Ministero degli affari esteri, dell'interno, della Difesa, della Giustizia, del MISE, del MEF, del Dipartimento della protezione civile e dell'Agid e, se necessario, rappresentanti di altre amministrazioni o operatori
  - Si riunisce almeno una volta al mese
  - Riferisce al Direttore Generale del DIS
  - promuove la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati interessati e l'elaborazione delle necessarie procedure di coordinamento interministeriale

Il Decreto Gentiloni

- **NSC (artt. 8-9)**
  - mantiene attiva, 24 ore su 24, 7 giorni su 7, l'unità per l'allertamento e la risposta a situazioni di crisi cibernetica
  - valuta e promuove procedure di condivisione delle informazioni alla fine della diffusione di allarmi relativi ad eventi cibernetici e per la gestione delle crisi
  - acquisisce le comunicazioni circa i casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità significativi ai fini del corretto funzionamento delle reti e dei servizi dal MISE, dagli organismi di informazione per la sicurezza, dalle Forze di polizia e, in particolare, dal CNAIPIC, dalle strutture del Ministero della difesa e dai CERT

Il Decreto Gentiloni

- **NSC (artt. 8-9)**
  - promuove e coordina, in raccordo con il MISE e con l'AgID i profili di rispettiva competenza, lo svolgimento di esercitazioni (interministeriali e internazionali)
  - costituisce punto di riferimento nazionale per i rapporti con l'ONU, la NATO, l'UE, altre organizzazioni internazionali ed altri Stati
  - In situazioni di crisi cibernetica: (a) riceve le segnalazioni anche dall'estero e dirama allarmi; (b) valuta se l'evento assumente dimensioni, intensità e natura tali da essere fronteggiato dalle amministrazioni in maniera ordinaria; (c) informa il Presidente del Consiglio dei Ministri (per il tramite del Direttore generale del DIS).

Recepimento della Direttiva NIS

- **Dlgs. 65/2018 (Recepimento della Direttiva NIS)**

Sono designate come Autorità nazionali competenti (art. 7):

- MISE per il settore dell'energia, sottosettori energia elettrica, gas e petrolio e per il settore infrastrutture digitali, sottosettori IXP, DNS, TLD, nonché per i servizi digitali
- MEF per il settore bancario e per il settore infrastrutture dei mercati finanziari, in collaborazione con Banca d'Italia e Consob
- Ministero della Salute, Regioni e le Province autonome di Trento e di Bolzano per il settore sanitario
- Ministero dell'ambiente e della tutela del territorio e del mare e le Regioni e le Province autonome di Trento e Bolzano per il settore di fornitura e distruzione di acqua potabile

Recepimento della Direttiva NIS

- **Dlgs. 65/2018 (Recepimento della Direttiva NIS)**

Il DIS è designato quale punto di contatto unico.

È prevista l'istituzione presso la Presidenza del Consiglio dei Ministri il CSIRT (art. 8) che tra le altre cose:

- Assicura la conformità dei requisiti previsti dalla NIS
- Definisce le procedure di prevenzione e gestione degli incidenti

- **Decreto del Presidente del Consiglio dei Ministri 8 agosto 2019**: istituzione del CSIRT presso il Dipartimento delle Informazioni per la Sicurezza (DIS) della Presidenza del Consiglio dei Ministri.

Il perimetro di sicurezza nazionale cibernetica

- **Legge di conversione 18 novembre 2019, n. 133**

Il Presidente del Consiglio dei ministri, su proposta del CISR

- Entro 4 mesi (art. 1, comma 2):

- adotta un decreto per l'individuazione delle amministrazioni pubbliche, gli enti e gli operatori pubblici e privati aventi una sede nel territorio nazionale, inclusi nel perimetro di sicurezza nazionale cibernetica sulla base dei seguenti criteri: (a) il soggetto esercita una funzione essenziale per lo Stato, per il mantenimento di attività civili, sociali o economiche; (b) esercizio di tale funzione o la prestazione del servizio dipende da reti, sistemi informativi e servizi informatici; (c) del criterio di gradualità, tenendo conto dell'entità del pregiudizio per la sicurezza nazionale di un malfunzionamento.

Il perimetro di sicurezza nazionale cibernetica

- **Legge di conversione 18 novembre 2019, n. 133**

Il Presidente del Consiglio dei ministri, su proposta del CISR

- Entro 10 mesi (art. 1, comma 3):

- Adotta un decreto: (a) per la definizione delle procedure per la notifica degli incidenti al CSIRT, che le inoltra al DIS e al NSC. Il DIS assicura la trasmissione al CNAIPIC, al PdC (se proveniente da soggetto pubblico) e al MISE (se proveniente da soggetto privato); (b) per le misure per garantire elevati livelli di sicurezza tenendo conto degli standard definiti a livello internazionale e dell'Unione europea.

Il perimetro di sicurezza nazionale cibernetica

- **Legge di conversione 18 novembre 2019, n. 133**

All’elaborazione delle misure provvedono, secondo gli ambiti di competenza delineati dal presente decreto, il Ministero dello sviluppo economico e la Presidenza del Consiglio dei ministri, d’intesa con il Ministero della difesa, il Ministero dell’interno, il Ministero dell’economia e delle finanze e il Dipartimento delle informazioni per la sicurezza (art. 1, comma 4).

CVCN istituito nel MISE (art.1, comma 6):

Assicura la sicurezza e l’assenza di vulnerabilità dei prodotti, hardware e software, impiegati su reti, sistemi informativi e servizi informatici degli attori rientranti nel perimetro

elabora e adotta, previo conforme avviso dell’organismo tecnico di supporto al CISR, schemi di certificazione cibernetica, tenendo conto degli standard definiti a livello internazionale e dell’Unione europea

Il perimetro di sicurezza nazionale cibernetica

- **Legge di conversione 18 novembre 2019, n. 133**

Il Ministero dell'Intero e della Difesa utilizzano propri CEVA utilizzando le metodologie di verifica e di test definite dal CVCN.

La Presidenza del Consiglio dei ministri in caso di crisi di natura cibernetica (art. 5): in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici, su deliberazione del CISR (informando il COPASIR delle misure disposte entro 30 giorni), può disporre per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione, secondo un criterio di proporzionalità, la disattivazione di uno o più apparati o prodotti impiegati per l'espletamento dei servizi interessati.

Il perimetro di sicurezza nazionale cibernetica

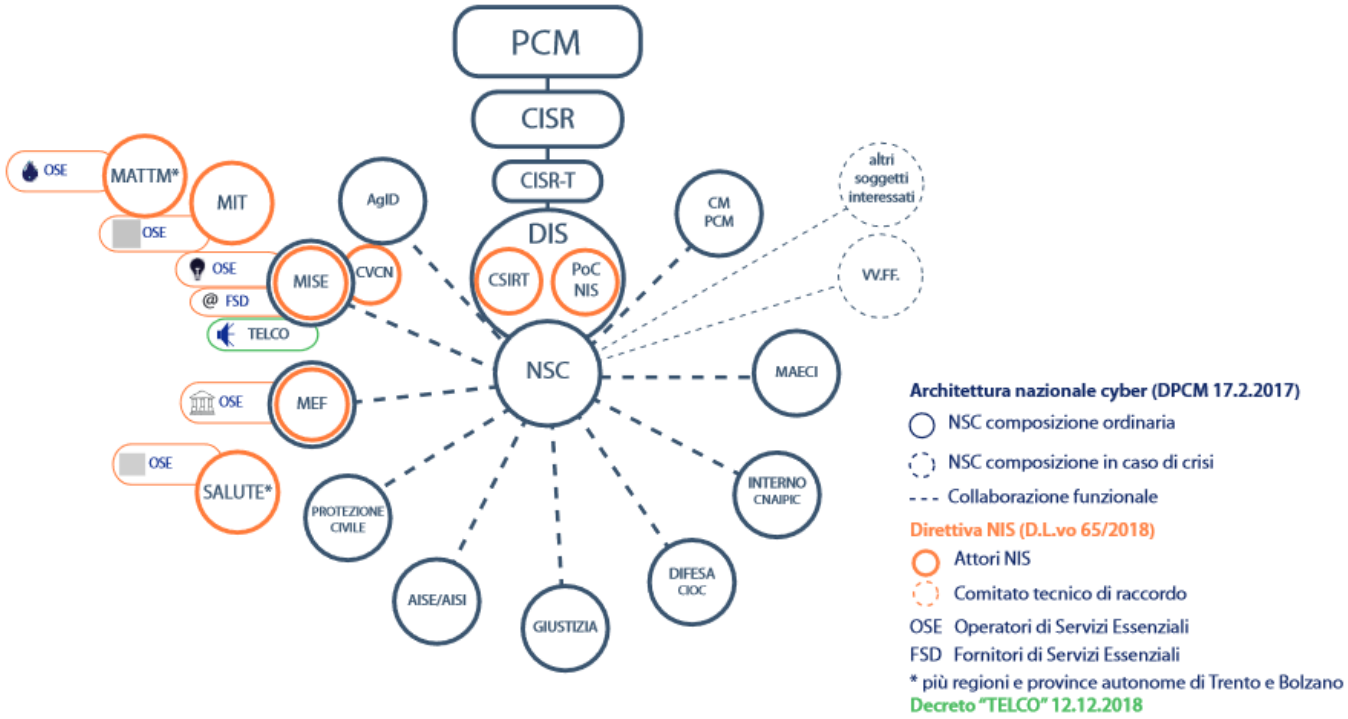
IL "PERIMETRO" IN PILLOLE	
A chi si applica	Soggetti nazionali pubblici e privati che – impiegando reti, sistemi informativi e servizi informatici – esercitano una funzione essenziale dello Stato ovvero assicurano un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato
A cosa si applica	Reti, sistemi informativi e servizi informatici dei soggetti inclusi nel "perimetro" dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale
Cosa prevede	• Notifica degli incidenti, così da assicurare un immediato flusso di informazioni a favore delle strutture deputate alla prevenzione, preparazione e gestione degli eventi cyber (in particolare CSIRT e Nucleo per la Sicurezza Cibernetica, entrambi incardinati nel DIS) • Misure di sicurezza relative a organizzazione, processi e procedure, anche in relazione al procurement ICT • Screening tecnologico degli approvvigionamenti ICT appartenenti a categorie specifiche, destinati agli asset inclusi nel "perimetro". La procedura prevede che il soggetto che intenda procedere a tali acquisizioni ne dia comunicazione al Centro di Valutazione e Certificazione Nazionale (CVCN), che, entro un massimo di 60 giorni, può effettuare verifiche preliminari ed imporre condizioni e test di hardware e software • Attività ispettiva e sanzionatoria a cura di Presidenza del Consiglio dei Ministri e MiSE, rispettivamente per i soggetti pubblici e per quelli privati "perimetrati" • Norme di coordinamento con il Decreto Legislativo n. 65/2018, di recepimento della Direttiva NIS, e con il Codice delle Comunicazioni Elettroniche per i soggetti sottoposti contestualmente ad una di queste discipline e alla legge sul "perimetro"
Poteri d'emergenza	In presenza di un rischio grave ed imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici, il Presidente del Consiglio – ove indispensabile e per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione – può disporre, previa deliberazione del CISR, la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati

Overview dell’architettura italiana di cyber security

Centralità di:

- Presidenza del Consiglio dei Ministri;
- DIS come “punto di contatto unico nazionale NIS” per la gestione operativa di incidenti transfrontalieri;
- NSC per la gestione operativa di incidenti che hanno un impatto sulla sicurezza nazionale, e le attivazioni che deriveranno dal cosiddetto “Perimetro di sicurezza nazionale cibernetica”;
- CSIRT per la notifica degli incidenti dei soggetti rientranti nella NIS e nel perimetro.

Ecosistema Cyber Italiano



Approfondimento

Libri di testo, risorse web e altri materiali di approfondimento

- Camera dei Deputati, Documentazione e Ricerche, “Dominio cibernetico, nuove tecnologie e politiche di sicurezza e difesa cyber”, 24 settembre 2019
- Laboratorio Nazionale di Cybersecurity, CINI - Consorzio Interuniversitario Nazionale per l’Informatica, “Libro Bianco sulla cybersecurity. ll Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici Progetti e Azioni per difendere al meglio il Paese dagli attacchi informatici”, 2018 https://cybersecnatlab.it
- Legge di conversione 18 novembre 2019, n. 133 (in questa stessa Gazzetta Ufficiale - alla pag. 29), recante: «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica»