La Direttiva europea NIS, Network and Information Security: soggetti attuatori, competenze, obblighi e prospettive nel processo di recepimento e a regime

Webinar, 26 ottobre 2017

Elisabetta Zuanelli

Coordinatore del Piano di formazione nazionale in cybersecurity, cyberthreat, privacy

Partenariato PP Università degli Studi di Roma “Tor Vergata”, Poste Italiane, Clariter Texi, Pragmema, Profice, Supercom, Istituto per il governo societario (www.cybersecurityprivacy.it)

Responsabile scientifico del Master di 2° livello dell’Università degli Studi di Roma «Tor Vergata» in Competenze digitali per la protezione dei dati, la cybersecurity e la privacy

Lo scenario quantitativo degli attacchi cyber

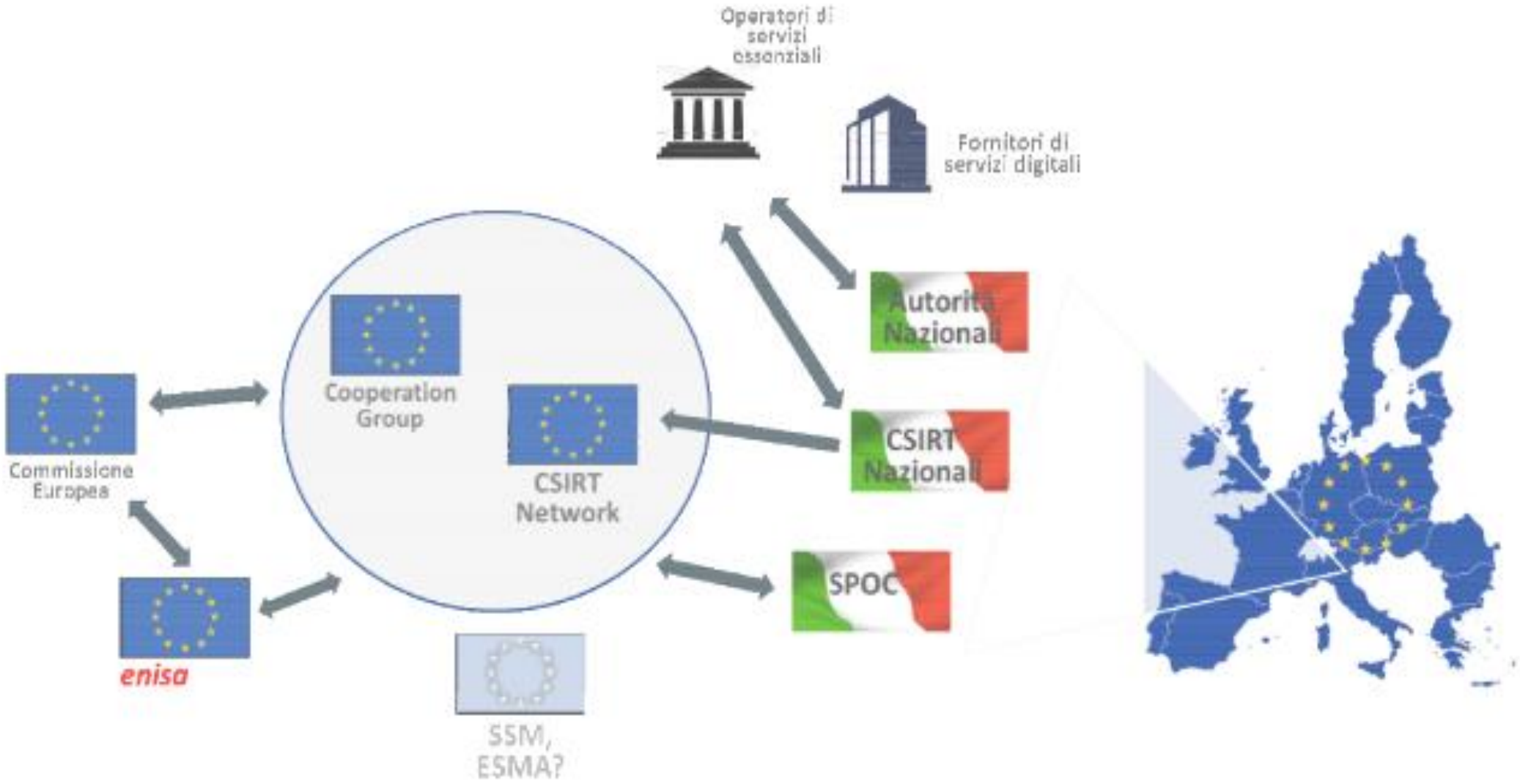
- L’80% delle aziende europee ha subito almeno un incidente cybersecurity nel 2015

- Il numero di incidenti di sicurezza per tutte le industrie nel mondo è cresciuto del 38%nel 2015

La Direttiva UE 2016/1148 del 6 luglio 2016 NIS (Sicurezza delle reti e dei sistemi informativi)

- scadenze
- soggetti attuatori
- competenze
- operatori di servizi essenziali
- fornitori di servizi digitali

L’architettura NIS



Scadenze

- La Direttiva NIS : in vigore da agosto 2016
- Gli stati membri: 21 mesi per adottare le necessarie misure di implementazione a livello di legislazione nazionale
- 6 mesi supplementari per identificare gli operatori delle infrastrutture critiche nazionali
- Il recepimento: 9 maggio 2018
- La transizione:

❑gruppo di cooperazione e rete CSIRT: operativo dal 9 febbraio 2017

❑gruppo di cooperazione assiste gli stati membri per l'identificazione degli operatori dei servizi essenziali e gli effetti negativi: da 9 febbraio 2017 a 9 novembre 2018


Agosto 2016
Entrata in vigore
6 mesi
Febbraio 2017
Inizio dei lavori del Gruppo di Cooperazione
Agosto 2017
Adozione dei requisiti di sicurezza e notifica per i fornitori di servizi digitali
12 mesi
18 mesi
Febbraio 2018
Il Gruppo di Cooperazione stabilisce il programma di lavoro
Maggio 2018
Recepimento nella legislazione nazionale
21 mesi
27 mesi
Novembre 2018
Gli Stati membri identificano gli operatori dei servizi essenziali
Maggio 2019
Prima relazione della Commissione Europea per valutare il lavoro degli Stati membri nell'identificazione degli operatori di servizi essenziali
33 mesi
Maggio 2021
La Commissione Europea valuta l'implementazione della Direttiva con particolare attenzione alla cooperazione strategica e operativa, e alle relazioni con i gestori dei servizi essenziali e con i fornitori di servizi digitali
57 mesi

Riesame

- Due anni dopo l'entrata in vigore della direttiva NIS e ogni 18 mesi successivi, la Rete CSIRTs produrrà una relazione per valutare l'esperienza acquisita con la cooperazione operativa, ivi comprese le conclusioni e le raccomandazioni emerse. La relazione sarà inviata alla Commissione.
- Riesame del funzionamento della direttiva (art. 23): entro il 9 maggio 2018 la Commissione presenta al Parlamento europeo e al Consiglio una relazione sulla coerenza nell'identificazione degli operatori dei servizi essenziali
- Riesame periodico

Il rapporto con le norme di contesto

- il GDPR e la Direttiva 95/46
- le norme settoriali UE
- le norme locali nazionali
- le norme internazionali

Il quadro strategico nazionale

Decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017
Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali

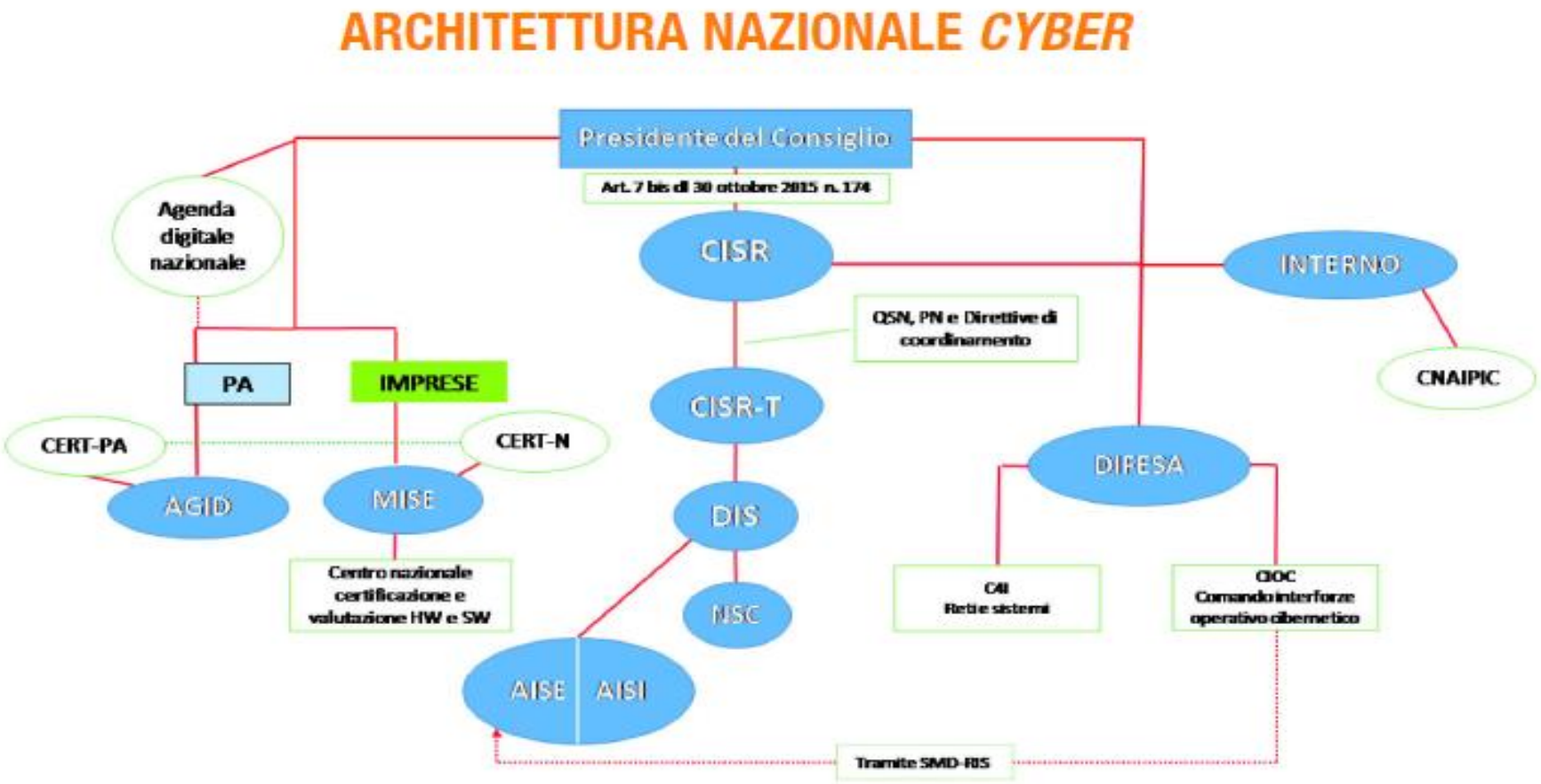
(Gazzetta Ufficiale n. 87 del 13 aprile 2017)

QUADRO STRATEGICO NAZIONALE (QSN)

INDIRIZZI STRATEGICI

1. Potenziamento delle capacità di difesa delle Infrastrutture Critiche nazionali e degli attori di rilevanza strategica per il sistema-Paese
2. Miglioramento, secondo un approccio integrato, delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati
3. Incentivazione della cooperazione tra istituzioni ed imprese nazionali
4. Promozione e diffusione della cultura della sicurezza cibernetica
5. Rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica
6. Rafforzamento delle capacità di contrasto alle attività e contenuti illegali *on-line*

Il Quadro strategico nazionale: struttura e competenze



Il piano nazionale

PIANO NAZIONALE (PN)

INDIRIZZI OPERATIVI

1. Potenziamento capacità di *intelligence*, di polizia e di difesa civile e militare
2. Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati
3. Promozione e diffusione della cultura della sicurezza informatica. Formazione ed addestramento
4. Cooperazione internazionale ed esercitazioni
5. Operatività delle strutture nazionali di *incident prevention*, *response* e *remediation*
6. Interventi legislativi e *compliance* con obblighi internazionali
7. *Compliance* a *standard* e protocolli di sicurezza
8. Supporto allo sviluppo industriale e tecnologico
9. Comunicazione strategica e operativa
10. Risorse
11. Implementazione di un sistema di *cyber risk management* nazionale

La gestione delle crisi

l soggetti attuatori

- La Commissione
- La *governance* degli Stati membri
- La/e Autorità
- Il gruppo di cooperazione
- Il CSIRT nazionale
- La rete di CSIRT
- Enisa
- Il punto di contatto unico

Le aziende: obblighi e sanzioni

Gli operatori di servizi essenziali (scad. 9 novembre 2018)

- Elenco
- Obblighi: *risk assessment* e *risk evaluation*
- La *compliance*: Ue e internazionali (framework NIST, COBIT, ISO, ISA, ecc.)
- Le notifiche
- Le sanzioni
- L'impatto: criteri di valutazione
- Giurisdizione e territorialità

Identificazione degli operatori di servizi essenziali

1.Entro il 9 novembre 2018, gli Stati membri identificano, per ciascun settore e sottosettore gli operatori di servizi essenziali con una sede nel loro territorio.

2.I criteri per l'identificazione degli operatori di servizi essenziali sono i seguenti:

a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali;

b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi;

c) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

3. Ciascuno Stato membro istituisce un elenco dei servizi

Tipologia degli operatori di servizi essenziali

Gli operatori di servizi essenziali sono aziende private o enti pubblici con un ruolo importante per la società e l'economia nei seguenti settori:

- Energia: elettricità, petrolio e gas.
- Trasporto: aereo, ferroviario, marittimo e stradale.
- Bancario: gli istituti di credito.
- Infrastrutture dei mercati finanziari: le sedi di negoziazione e le controparti centrali.
- Salute: ambienti sanitari.
- Acqua: fornitura di acqua potabile e distribuzione.
- Infrastruttura digitale: specificamente gli Internet Exchange point, i fornitori di servizi DNS (Domain Name System) e i registri TLD (Top Level Domain).

La Internet exchange map

Effetti negativi rilevanti

fattori intersettoriali:

a) il numero di utenti che dipendono dal servizio fornito dal soggetto interessato;
b) la dipendenza di altri settori di cui all'allegato II dal servizio fornito da tale soggetto;
c) l'impatto che gli incidenti potrebbero avere, in termini di entità e di durata, sulle attività economiche e sociali o sulla pubblica sicurezza;
d) la quota di mercato di detto soggetto;
e) la diffusione geografica relativamente all'area che potrebbe essere interessata da un incidente;
f) l'importanza del soggetto per il mantenimento di un livello sufficiente del servizio, tenendo conto della disponibilità di strumenti alternativi per la fornitura di tale servizio.

fattori settoriali: ove opportuno

Obblighi in materia di sicurezza e notifica degli incidenti

- **misure tecniche e organizzative** adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi che usano nelle loro operazioni
- tenuto conto delle conoscenze più aggiornate in materia, dette misure **assicurano un livello di sicurezza della rete e dei sistemi informativi** adeguato al rischio esistente
- misure adeguate per **prevenire e minimizzare l'impatto di incidenti** a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di **assicurare la continuità di tali servizi.**
- **notifiche** senza indebito ritardo all'autorità competente o al CSIRT gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati.

Obblighi di attuazione

Fornire all’Autorità

a) le **informazioni necessarie per valutare la sicurezza rete e dei sistemi informativi**, compresi i documenti relativi alle politiche di sicurezza;

b) la prova dell'effettiva attuazione delle politiche di sicurezza, come i **risultati di un audit sulla sicurezza svolto dall'autorità competente o da un revisore abilitato** e, in quest'ultimo caso, metterne a disposizione dell'autorità competente i risultati, inclusi gli elementi di prova.

Impatto dell’incidente

a) il **numero di utenti** interessati dalla perturbazione del servizio essenziale;

b) la **durata** dell'incidente;

c) la **diffusione geografica** relativamente all'area interessata dall'incidente.

I fornitori di servizi digitali

- I fornitori: identità
- Obblighi
- Giurisdizione e territorialità

Le tipologie dei fornitori di servizi digitali

1. Mercato online
2. Motore di ricerca online
3. Servizi nella nuvola (cloud computing)

Obblighi in materia di sicurezza e notifica degli incidenti (Art. 16)

- I fornitori di servizi digitali devono **identificare e adottare misure tecniche e organizzative** adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi
- Elementi da considerare:

a) la sicurezza dei sistemi e degli impianti;
b) trattamento degli incidenti;
c) gestione della continuità operativa;
d) monitoraggio, audit e test;
e) conformità con le norme internazionali.

Obblighi

- Misure preventive
- Riduzione dell’impatto
- Notifica all’Autorità competente o al CSIRT

Valutazione d’impatto

a) il **numero di utenti** interessati dall'incidente, in particolare gli utenti che dipendono dal servizio per la fornitura dei propri servizi;

b) la **durata** dell'incidente;

c) la **diffusione geografica** relativamente all'area interessata dall'incidente;

d) la **portata della perturbazione del funzionamento del servizio**;

e) la **portata dell'impatto sulle attività economiche e sociali.**

NB

L'obbligo di notificare un incidente si applica soltanto qualora il fornitore di servizi digitali abbia accesso alle informazioni necessarie per valutare l'impatto di un incidente nei confronti dei parametri di cui al primo comma.

Giurisdizione e territorialità

1. Un fornitore di servizi digitali è considerato soggetto alla **giurisdizione dello Stato membro in cui ha lo stabilimento principale.**

2. Un fornitore di servizi digitali che non è stabilito nell'Unione, ma offre servizi di cui all'allegato III all'interno dell'Unione, designa un **rappresentante** nell'Unione.

3. La designazione di un rappresentante da parte di un fornitore di servizi digitali fa salve le **azioni legali che potrebbero essere avviate nei confronti del fornitore stesso di servizi digitali**.

Sanzioni

- Gli Stati membri stabiliscono le **norme relative alle sanzioni** da irrogare in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva e adottano tutti i provvedimenti necessari per la loro applicazione.

- Le sanzioni previste sono **effettive, proporzionate e dissuasive**.

- Gli Stati membri notificano tali **norme e provvedimenti alla Commissione entro il 9 maggio 2018** e provvedono a darle immediata notifica di ogni successiva modifica.

Problematicità 1

- Correlazione NIS con GDPR (cessazione delle norme pregresse e *eprivacy*)

Il Garante europeo della protezione dei dati è stato consultato conformemente all'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 e ha espresso un parere il 14 giugno 2013 (4).

Il trattamento di dati personali ai sensi della presente direttiva è effettuato ai sensi della direttiva 95/46/CE. 2.Il trattamento di dati personali da parte di istituzioni e organismi dell'Unione ai sensi della presente direttiva è effettuato a norma del regolamento (CE) n. 45/2001.

Problematicità 2
Correlazione con le norme intersettoriali e settoriali, operatori vari, recepimento nazionale, coordinamento attività

- Trasporto via acqua
- Settore bancario
- Sorveglianza dell'Eurosistema sui sistemi di pagamento e di regolamento
- Sistemi di intermediazione online
- Accordi paralleli (es. *privacy shield* e DSM)

- Disomogeneità possibile nell'identificazione degli operatori di servizi essenziali e gli operatori di servizi digitali (liste di servizi e di operatori)
- Sanzioni: diverse per stato membro e da armonizzare
- Notifiche (parametri, referenti (Autorità e/o CSIRT)
- Riferimento a standard internazionali (europei e non): concorrenza vendor
- Compliance vs sicurezza
- Giurisdizione: localizzazione della sede e/o del rappresentante
- Interazione tra Commissione, gruppo di cooperazione, Autorità, rete dei CSIRT, Enisa, punti unici di contatto, ecc.

Grazie

Q&A