II CONFERENZA NAZIONALE

La Direttiva NIS e il GDPR: compliance istituzionali, strutture e coordinamento

2° edizione del Master in

«Competenze digitali per la Protezione dei Dati, la Cybersecurity e la Privacy»

6 NOVEMBRE 2018 ROMA

NIS e GDPR: compliance istituzionali, competenze, risorse

Elisabetta Zuanelli

Presidente CReSEC/Università degli Studi di Roma "Tor Vergata"

Coordinatore del Partenariato per il 'Piano nazionale di formazione in Cybersecurity, Cyberthreat e Privacy'

Una premessa

 Il Partenariato 'Tor Vergata', il Master, alta formazione, competenze digitali, progettualità

Trasformazione digitale: nuove tecnologie(cloud, lot, mobile, platforms, AI, ecc.), mercati, competenze istituzionali e abracadabra digitali

 L'adeguatezza del sistema e il 'rumore' dell'informazione: chiacchiere e distintivo o rincorsa istituzionale pubblica e privata

Security Types:

- Network security
- Endpoint security
- Application security
- Content security
- Wireless security
- Cloud security

By Service:

- Consulting
- Design and integration
- Risk and threat assessment
- Managed security services
- Training and education

By Vertical:

- Aerospace, defenseand intelligence
- Government (excluding defense) and public utilities
- Banking, Financial Services, and Insurance (BFSI)
- Telecommunication
- Healthcare
- Retail
- Manufacturing

Stakeholders and cyber security market size

The global Cyber Security market size was estimated to grow from \$106.32 Billion in 2015 to \$170.21 Billion by 2020, at a Compound Annual Growth Rate (CAGR) of 9.8%

Stakeholders:

- Cyber security vendors
- Networking solution providers
- Independent Software Vendors (ISVs)
- Software vendors
- System integrators
- Value-added resellers
- Service providers and distributors
- Research organizations
- IT security agencies
- Suppliers, distributors, and contractors
- Consulting companies
- Cloud Business Intelligence (BI) platform vendors/cloud infrastructure providers
- Investors and venture capitalists

NIS,GDPR e altro: i temi della compliance

► Le scadenze prossime:

CSIRT unico, elenchi fornitori di servizi essenziali e servizi digitali, Autorità, coordinamento nazionale ed europeo

I nuovi pacchetti normativi: cyberact (framework standard), il rapporto GDPR/Codice privacy, ecc.

Awareness, standard professionali e certificazioni?



Il paradosso dell'osservatore

Dentro o fuori del sistema?



Problemi da affrontare

- la prosecuzione della macchina avviata: Piano strategico nazionale della cybersecurity e piano operativo (e con la protezione dei dati?)
 - la coerenza formale e operativa delle Autorità
- elenchi delle aziende di servizi essenziali e digitali (e i vendor di tecnologie digitali ???)

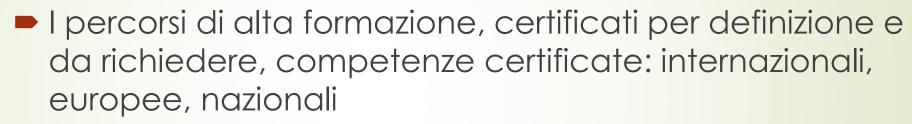
i casi telecomunicazioni, sanità, ambiente, infrastrutture e trasporti, sviluppo economico, banche

Standard e certificazioni

- Il framework europeo ENISA e le scelte nazionali in materia di standard tecnologici di servizi cyber e prodotti e servizi digitali
- Come avverrà l'integrazione a livello europeo?
- Qualche problema: multinazionali digitali e della sicurezza e PMI del mercato

Territorialità degli standard???

Le competenze: tra alta formazione e corsi certificati



Framework di alta formazione di base e permanente

Il ruolo degli operatori di sistema



Gli stakeholder e lo scambio europeo e internazionale delle visioni di competenze digitali e di sicurezza

- Attenzione alla restrizione e chiusura delle competenze: non solo ICT
- Investimenti in formazione per il mercato: chi paga???
- Investimenti in R&D: progettualità finalizzata alla competitività del sistema (come?)

Il dibattito odierno: tavole rotonde e workshop



...dai problemi alle soluzioni...