Audizioni su sicurezza nazionale cibernetica

Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica,

Rome

08 October, 2019

Pierluigi PAGANINI

Scenario corrente

Perimetro di sicurezza nazionale cibernetica

- Cyberspazio è un contesto privo di frontiere, con implicazioni nature tecnologica, investigativa, diplomatica ed organizzativa.

- Perimetro include soggetti pubblici e privati che assicurano attraverso reti e sistemi informatici l'erogazione di servizi essenziali per il Sistema Paese.

- Protezione del 'Perimetro di sicurezza nazionale cibernetica' non può prescindere dalla collaborazione con altri paese e quindi dalla definizione delle 'interfacce' per lo scambio delle informazioni relative alle minacce.

- Perimetro di sicurezza cibernetica nazionale è progetto di sistema paese (R. Baldoni).

Scenario corrente

Perimetro di sicurezza nazionale cibernetica

- Il numero di attacchi informatici è in costante e rapido aumento. Attacchi sempre più sofisicati.
- IoT, mobile, Cloud stanno ampliando la nostra superficie di attacco.
- Cruciali aspetti di protezione delle infrastrutture critiche.
- Financial cybercrime allarme sistemico che minaccia economia del Paese. Oltre 79 percento di attacchi informatici sono ‘financially-motivated’
- +37 percento Incremento attacchi ‘gravi’ nel biennio
- Attacchi nation-state sempre piu’ complessi e di difficile attribuzione.
- La maggior parte degli attacchi non è denunciata o peggio non ci si accorge degli stessi. Norme per emersione degli incidenti per attore nel perimetro.

Il Perimetro

Perimetro di sicurezza nazionale cibernetica

- Corretto approccio sistematico alla definizione del perimetro di sicurezza nazionale cibernetica.
  - Definizione Governance
  - Perimetro di applicazione
  - Ruoli e responsabilità soggetti coinvolti
  - Criteri valutazione

- Per la natura stessa dei fenomeni in analisi è necessario definire in maniera chiara e non ambigua i criteri di valutazione.

- Valutazione impatto attuazione misure su soggetti obbligati. Necessità di partire dalla compliance a standard internazionali già applicate al nostro contesto.

Il Perimetro

Perimetro di sicurezza nazionale cibernetica

- Periodo adeguamento delle misure di sicurezza richieste per garantire attuazione degli adeguamenti necessari all'innalzamento del livello di sicurezza delle entità appartenenti al perimetro.
- Piani di addestramento nazionali per personale che opera nell'ambito del perimetro.
- Processi di certificazione delle strutture di approvvigionamento (Supply Chain). Incremento attacchi alla Supply Chain.
- Sicurezza delle organizzazioni interne al perimetro è funzionale al livello di sicurezza dei loro fornitori di servizio.

Criticità

Perimetro di sicurezza nazionale cibernetica

- Indeterminatezza delle specializzazione degli attori coinvolti, configura un rischio di sovrapposizione di responsabilità tra diversi ruoli coinvolti.
- Incrementare capacità interne al governo attraverso programmi specifici di formazione.
- Maggiore trasparenza in relazione alla deroga concessa ai sistemi informatici dedicati alla prevenzione, accertamento e repressione dei reati (ovvero esclusi sistema valutazione CVCN).
- Necessità di una struttura CERT in seno al Ministero dell'Interno, cui potrebbero essere assegnare funzioni di valutazione di sistemi interni al perimetro.

Criticità

Perimetro di sicurezza nazionale cibernetica

- Livello di sicurezza dei sistemi governativi da incrementare rapidamente. Attualmente richieste solo misure minime di sicurezza AGID.

- Necessità di investimenti economici per la messa in sicurezza dei sistemi suddetti. Stessa cosa vale per i programmi di formazione. Prendere ad esempio modello UK con investimenti strutturali governativi.

- Necessari investimenti in ambito ricerca. Nuove tecnologie offrono nuove opportunità, ma espongono le nostre strutture a nuovi rischi. Necessità di una adeguata pianificazione finanziaria in materia ricerca su tecnologie emergenti.

- Qualifica tecnologica degli approvvigionamenti ICT è elemento critico soprattutto per fornitori di entità operanti nel perimetro.

- Forte ritardo rispetto ad altri paesi europei (e.g. Francia, Germania). Parliamo di 20 anni rispetto a strutture di certificazione come il BSI tedesco e circa 15 nel caso ANSSI francese.

Criticità

Perimetro di sicurezza nazionale cibernetica

- Valorizzazione industria nazionale in ambito cyber.
- Criticità ruolo Centro di Valutazione e Certificazione Nazionale (CVCN) nell'assicurazione del rispetto dei requisiti di sicurezza e dell'assenza di vulnerabilità di prodotti, hardware e software destinati ad attori operanti nel perimento di sicurezza cibernetica.
- EU Cyber Security Act introduce per la prima volta un quadro di certificazione in materia sicurezza cibernetica a livello UE per prodotti, servizi e processi ICT.
- Necessità collaborazione soggetti pubblici e privati.

To Do

Perimetro di sicurezza nazionale cibernetica

- Hardware Security/Hardware Qualification con riferimento specifico ad ambienti critici.
- Creazione di competenza specifiche attraverso contributo pubblico/privato
- Sviluppo architetture nazionali tolleranti le vulnerabilità a garanzia di livelli sicurezza predefiniti anche in presenza di hardware vulnerabili (Libro Bianco).
- Definizione metodiche/processi di certificazione di hardware e software
- Costituzione di centri di competenza per le certificazioni

To Do

Perimetro di sicurezza nazionale cibernetica

- Controllo ciclo di vita della tecnologia, dal progetto alla manutenzione
- Trusted supply chain
- Percorsi formativi scolastici
- Educazione di base di fondamenti di cyber security a partire dalle scuole medie
- Corsi accademici specializzati
- Alta formazione (corsi di laurea e post-laurea/master), dottorati.
- Formazione professionale multidisciplinare che deve includere fondamenti cyber security (i.e. Programma CyberFirst UK)


Thank you

About me

About Pierluigi Paganini:

Pierluigi Paganini is Chief Technology Officer at Cybaze SpA.
Pierluigi Paganini is a member of the ENISA (European Union Agency for Network and Information Security))Threat Landscape Stakeholder Group, member of Cyber G7 Workgroup of the Italian Ministry of Foreign Affairs and International Cooperation, Director of the Master in Cyber Security at the Link Campus University.
He is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing, and a strong belief that security is founded on the information sharing lead Pierluigi to launch the security blog "Security Affairs" recently awarded as the Best European Personal Security Blog.
Author of the Books "The Deep Dark Web“ “Digital Virtual Currency and Bitcoin” and “Digging the Deep Web: Exploring the dark side of the web”,

Ing. Pierluigi Paganini

Chief Technology Officer & Founder Cybaze SpA.

Founder Security Affairs

http://securityaffairs.co/wordpress

pierluigi.paganini@securityaffairs.co

Pierluigi.paganini@cybaze.it