MERIDIAN
GROUP

Proposte *Meridian Group*

Camera dei Deputati, IV Commissione Permanente (DIFESA);

audizione per *"Indagine conoscitiva sulla difesa cibernetica: nuovi profili e criticità"*

In un'epoca di crescente digitalizzazione e continua evoluzione delle tecnologie informatiche, la sicurezza cibernetica diviene una priorità fondamentale per proteggere integrità e privacy dei dati, conseguentemente alla sicurezza delle nazioni e dei cittadini.

Risulta essenziale oggi comprendere come l'aumento delle tensioni internazionali e dei conflitti possa inevitabilmente comportare un incremento degli attacchi informatici contro infrastrutture critiche e sistemi di una nazione. Tuttavia, riteniamo sia altrettanto necessario evitare di concentrarsi esclusivamente su questo aspetto; una parte significativa dei crimini informatici è motivata ancora da interessi economici, con criminali che sfruttano le vulnerabilità delle infrastrutture meno protette al fine di estorcere denaro da soggetti disposti a pagare riscatti e ingannare utenti poco informati sui rischi della sicurezza informatica.

Di fronte a una tale complessità delle minacce, può essere rilevante sviluppare un approccio globale alla sicurezza informatica e alla difesa cibernetica, in grado di superare la semplice reazione agli eventi contingenti contribuendo a creare una strategia solida, proattiva e duratura.

Come Meridian Group, proponiamo quindi quattro iniziative che riteniamo possano arricchire e ampliare l'attuale situazione.

MERIDIAN SRL
info@meridian-group.eu | www.meridian-group.eu | +39 06 54 278 301 | +39 06 54 278 338
Viale Erminio Spalla, 9 - 00142 Roma (RM) IT | P.IVA/C.F. 13693001003 | REA-RM-1465989

1. Supporto Economico alla Formazione

Riteniamo possa essere estremamente utile dedicare risorse finanziarie mirate a programmi di formazione professionale per i lavoratori, unitamente ad iniziative di sensibilizzazione pubblica, con l'intento di aumentare la *consapevolezza collettiva* sulle buone pratiche di sicurezza online e sui rischi delle minacce emergenti nel cyber spazio.

Per raggiungere questo ambizioso obiettivo, si potrebbero contemplare o rafforzare:

• **Finanziamenti diretti e incentivi fiscali**: destinare fondi specifici e introdurre incentivi fiscali per sostenere programmi formativi e iniziative di sensibilizzazione sulla sicurezza informatica, sia per enti pubblici che privati. Questo supporto finanziario faciliterebbe lo sviluppo e l'implementazione di programmi educativi approfonditi rivolti a vari segmenti della popolazione.

• **Accesso a risorse e strumenti dedicati alla Sicurezza Informatica**: assicurare alle amministrazioni pubbliche e alle piccole e medie imprese (PMI) l'accesso a strumenti e risorse per la sicurezza informatica a condizioni favorevoli. Questo comprenderebbe software di protezione, piattaforme di formazione e consulenze specializzate, rendendo i processi in grado di garantire la sicurezza informatica più accessibili e governabili.

• **Campagne informativo-educative**: promuovere e finanziare campagne informative e iniziative educative che contribuiscano ad aumentare la consapevolezza generale sui rischi cibernetici e consentano di identificare più consapevolmente le opportune strategie di mitigazione degli stessi.

Queste iniziative dovrebbero mirare a raggiungere il più vasto pubblico possibile, sfruttando diversi mezzi di comunicazione per massimizzarne l'impatto.

2. Protocolli di risposta agli attacchi e programma nazionale "Bug Bounty"

Nella gestione degli incidenti informatici, risulta cruciale definire con precisione e in conformità alla legge le operazioni di contenimento e prevenzione degli attacchi, evitando qualsiasi azione che possa violarne i confini legali.

Questa particolare necessità evidenzia l'urgenza di sviluppare protocolli chiari e solidamente ancorati al quadro giuridico, regolamentando le azioni difensive indispensabili per individuare e mitigare gli attacchi, garantendo al contempo che tali misure non siano interpretate erroneamente come violazioni normative.

Particolare riferimento alle piattaforme di *Cyber Intelligence* e all'accesso a fonti dati *CLOSINT*, che rappresentano strumenti ed azioni indispensabili per acquisire informazioni sulle violazioni di sicurezza in ambienti riservati ai criminali informatici.

Queste informazioni possono rappresentare un vantaggio per gli operatori di sicurezza, ma il loro utilizzo deve essere gestito e normato in modo tale che non incorrano in reati. Tra un evento di sicurezza e un incidente di sicurezza intercorre un tempo cruciale che, se sfruttato adeguatamente, può ridurre in modo sensibile le capacità d'attacco dei criminali e le pericolose conseguenze di un attacco informatico.

In parallelo, proponiamo l'istituzione di un programma nazionale *bug bounty*, che incoraggi ricercatori di sicurezza ed *ethical hackers* a collaborare nella scoperta e segnalazione delle vulnerabilità all'interno delle infrastrutture digitali rientranti nel perimetro della sicurezza nazionale, e non solo. Con regole chiare per la segnalazione, garanzia di tutela legale per i partecipanti che agiscono in buona fede e ricompense adeguate all'importanza delle vulnerabilità individuate, il programma potrebbe potenziare in modo significativo la sicurezza delle infrastrutture nazionali.

3. Integrazione di figure specializzate nella prevenzione e risposta agli incidenti di cybersicurezza comparate alle Forze dell'Ordine

Riteniamo fondamentale evidenziare la necessità di creare ruoli specializzati ispirati ai modelli formativi militari, che non solo abbiano una profonda conoscenza di tecnologie e metodologie di settore, ma siano anche esperti nelle normative legali ed etiche relative alla cybersicurezza.

La formazione di queste figure potrebbe prevedere lo sviluppo di percorsi educativi e professionali specifici, in grado di integrare e far convergere competenze tecniche avanzate con una solida comprensione delle implicazioni legali ed etiche, sempre più necessarie oggi per la gestione degli eventi di sicurezza cibernetica.

Un tale approccio garantirebbe ai professionisti di operare sempre nel pieno rispetto dei principi di legalità, proporzionalità e tutela dei diritti civili.

Attraverso:

- la definizione chiara dei requisiti professionali e formativi per le figure dedicate;
- l'erogazione di programmi formativi che integrino conoscenze tecniche e consapevolezza legale ed etica;
- lo sviluppo di partnership tra istituzioni nazionali, accademiche e del settore privato;

si potrebbero gettare le basi per un "sistema nazionale di difesa cibernetica" che sia, non solo tecnologicamente robusto, ma anche solido e aderente alle normative e ai valori fondamentali della nostra società.

4. Gruppi di lavoro nazionali sulla sicurezza informatica con la partecipazione attiva di piccole e medie imprese

L'istituzione di gruppi di lavoro nazionali focalizzati sulla sicurezza informatica e la difesa cibernetica, potrebbero riunire una vasta gamma di attori provenienti sia dal settore pubblico che da quello privato, favorendo in particolar modo la partecipazione delle piccole e medie imprese italiane (PMI).

L'obiettivo principale di questa iniziativa sarebbe quello di:

• **Promuovere la collaborazione interdisciplinare**, ad esempio, sfruttando piattaforme dedicate per lo scambio di conoscenze, esperienze e risorse tra enti governativi, grandi aziende, PMI, istituti accademici e organizzazioni di ricerca. Questo approccio, realizzabile idealmente attraverso la definizione di un ambiente nazionale condiviso e dedicato, aiuterebbe a far circolare liberamente il bagaglio di conoscenze specifico di ognuno, migliorando al contempo le pratiche, così da poter essere adottate rapidamente da tutti i portatori d'interesse.

• **Sviluppare strategie coordinate;** attraverso una collaborazione sinergica, i gruppi di lavoro aiuterebbero ad elaborare e attuare strategie di sicurezza informatica in grado di tenere conto delle particolarità e delle esigenze di tutti i settori coinvolti. Un approccio coordinato consentirebbe di ottimizzare l'utilizzo delle risorse a disposizione e rispondere in modo ancora più efficace alle minacce cibernetiche.

Teniamo infine a sottolineare come la **collaborazione tra tutti gli stakeholder**, anche a livello internazionale, risulti oggi essenziale nel contrasto delle minacce informatiche moderne, che non conoscono confini e richiedono al contempo risposte rapide e coordinate.