MERIDIAN
GROUP

Proposte *Meridian Group*

***Camera dei Deputati**: Audizione sul disegno di legge "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" (A.C.1717)*

Nell'attuale contesto, caratterizzato da una sempre maggiore digitalizzazione delle società e dall'evoluzione costante delle tecnologie informatiche, la sicurezza informatica emerge come una priorità innegabile per garantire l'integrità, la privacy e la sicurezza delle nazioni. Il progetto di legge sulla sicurezza informatica nazionale si inserisce in questo scenario con l'obiettivo di rafforzare le difese dell'Italia contro una vasta gamma di minacce informatiche, consapevole della posizione geopolitica del paese e delle possibili vulnerabilità a cui può essere esposto.

È essenziale riconoscere che l'aumento delle tensioni internazionali e dei conflitti potrebbe certamente portare a un aumento degli attacchi informatici diretti contro le infrastrutture critiche e i sistemi vitali di una nazione. Tuttavia, non bisogna concentrarsi esclusivamente su questa dimensione del problema.

La verità è che una parte significativa dei crimini informatici è motivata da interessi economici, con criminali che cercano di sfruttare le vulnerabilità delle infrastrutture meno protette per estorcere denaro dalle entità disposte a pagare il riscatto e per ingannare utenti poco informati sui rischi legati alla sicurezza informatica.

Di fronte a questa complessità di minacce, il progetto di legge mira a implementare un approccio globale alla sicurezza informatica che vada oltre la mera reazione agli eventi contingenti per sviluppare una strategia duratura e resistente.

In questo contesto, emergono quattro proposte fondamentali che possono arricchire e ampliare il campo di applicazione del progetto di legge:

MERIDIAN SRL
info@meridian-group.eu | www.meridian-group.eu | +39 06 54 278 301 | +39 06 54 278 338
Viale dell'Oceano Atlantico, 182 - 00144 Roma (RM) IT | P.IVA/C.F. 13693001003 | REA-RM-1465989

1. Proposta per il Supporto Economico alla Formazione

Questa proposta sottolinea l'importanza di investire risorse finanziarie in programmi di formazione professionale per i lavoratori, insieme a iniziative di sensibilizzazione pubblica che mirano a aumentare la consapevolezza collettiva sulle buone pratiche di sicurezza online e sui rischi delle minacce emergenti nel cyber spazio. Per raggiungere questo obiettivo, il disegno di legge dovrebbe contemplare:

• Finanziamenti Diretti e Incentivi Fiscali: Assegnare 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 agevolerebbe lo sviluppo e l'attuazione di programmi educativi approfonditi rivolti a diversi segmenti della popolazione.

• Accesso a Risorse e Strumenti per la Sicurezza Informatica: Garantire alle amministrazioni pubbliche e alle piccole e medie imprese (PMI) l'accesso a strumenti e risorse per la sicurezza informatica a condizioni vantaggiose. Ciò includerebbe software protettivi, piattaforme formative online e consulenze specializzate, rendendo la sicurezza informatica più accessibile e gestibile.

• Campagne Informativo-Educative: Promuovere e finanziare campagne informative pubbliche e iniziative educative volte a migliorare la comprensione generale dei rischi cibernetici e delle strategie di mitigazione.

Queste iniziative dovrebbero mirare a raggiungere un vasto pubblico, sfruttando diversi mezzi di comunicazione per massimizzare l'impatto.

ESEMPIO: Cyber Essentials è un'iniziativa governativa britannica che fornisce alle aziende una certificazione per le basi della sicurezza informatica. Il programma, volto a proteggere le organizzazioni dalle minacce cyber più comuni, offre anche sussidi per le piccole e medie imprese PMI per aiutarle a raggiungere e mantenere gli standard richiesti. Attraverso linee guida chiare, workshop e supporto finanziario, Cyber Essentials ha migliorato significativamente la consapevolezza e la resilienza delle PMI britanniche, servendo come esempio di come gli incentivi economici possano promuovere pratiche di sicurezza informatica efficaci.

2. Proposta per Potenziare la Sicurezza Informatica Nazionale tramite Protocolli di Risposta agli Attacchi e il Programma Nazionale Bug Bounty – modifica art.11

All'interno del progetto di legge sulla sicurezza informatica nazionale, si sottolinea l'importanza cruciale di definire in modo preciso e conforme alla legge le operazioni di contenimento degli attacchi informatici, evitando qualsiasi azione che potrebbe violare i confini legali.

Questa necessità mette in evidenza l'urgenza di sviluppare protocolli chiari e saldamente ancorati al quadro giuridico, regolamentando le azioni difensive per individuare e mitigare gli attacchi, garantendo nel contempo che tali misure non siano soggette a interpretazioni erronee come violazioni normative. In questo caso parliamo dell'utilizzo di piattaforme di Cyber Intelligence e dell'accesso a fonti CLOSINT, ad esempio, che riescono ad acquisire informazioni sulle violazioni di sicurezza in ambienti riservati ai criminali informatici.

Queste informazioni possono essere un vantaggio per gli operatori di cyber sicurezza e l'utilizzo di queste informazioni deve essere gestito in modo tale che non si incappi in reati penali.

Non dimentichiamoci che tra l'evento di sicurezza e l'incidente di sicurezza intercorre un tempo fondamentale che, se utilizzato a proprio favore, può ridurre notevolmente le capacità d'attacco dei criminali e le conseguenze derivanti da un attacco.

In parallelo, proponiamo l'istituzione di un programma nazionale bug bounty sotto la supervisione diretta dell'Agenzia per la CyberSicurezza Nazionale (ACN). Questo programma mira a incoraggiare 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. Con l'implementazione di regole chiare per la segnalazione, la garanzia di tutela legale per i partecipanti che agiscono in buona fede e l'offerta di ricompense adeguate all'importanza delle vulnerabilità individuate, il programma mira a potenziare in modo significativo la sicurezza delle infrastrutture critiche nazionali. La combinazione tra lo sviluppo di protocolli per contrastare gli attacchi nel rispetto delle normative esistenti e l'attivazione di un programma nazionale di bug bounty rappresenta una strategia bilaterale volta alla prevenzione e all'innovazione.

ESEMPIO: Il "Hack the Pentagon" è stato il primo programma di bug bounty avviato dal Dipartimento della Difesa degli Stati Uniti. Lanciato nel 2016, ha invitato hacker etici a identificare e segnalare vulnerabilità nei sistemi informativi del Pentagono. Più di 1.400 partecipanti hanno identificato oltre 138 vulnerabilità uniche che sono state prontamente mitigate, migliorando significativamente la sicurezza delle infrastrutture critiche. Questo caso dimostra l'efficacia di un

programma di bug bounty ben gestito nel rafforzare la sicurezza informatica a livello nazionale, fornendo un modello replicabile per iniziative simili in altri paesi.

3. Proposta per l'integrazione di figure specializzate nella prevenzione e risposta agli incidenti di cybersicurezza comparate alle forze dell'ordine

Dal nostro punto di vista è importante sottolineare l'esigenza di istituire ruoli specializzati ispirati ai modelli formativi militari, che siano non solo esperti in tecnologie e metodologie informatiche sicure, ma anche competenti nelle normative legali ed etiche pertinenti alla cybersicurezza. La creazione di tali figure professionali implica lo sviluppo di percorsi formativi dedicati che combinino competenze tecniche avanzate con una solida comprensione delle implicazioni legali ed etiche della gestione degli incidenti di sicurezza. Non è sufficiente frequentare un corso sulla sicurezza informatica per lavorare nel settore: il mondo digitale richiede professionisti equiparabili a quelli del mondo reale.

Questo garantirebbe che tali professionisti siano non solo in grado di riconoscere e contrastare efficacemente le minacce in tempo reale, ma anche di farlo nel rispetto totale dei principi di legalità, proporzionalità e tutela dei diritti civili. Con l'inclusione in un progetto di legge di disposizioni specifiche per:

- La chiara definizione dei requisiti professionali e formativi per le nuove figure della sicurezza informatica;

- L'istituzione di centri formativi specializzati, con programmi che combinino conoscenze tecniche e consapevolezza legale ed etica;

- Lo sviluppo partnership tra istituzioni statali, accademiche e del settore privato per la creazione di programmi avanzati di formazione;

Stiamo gettando le basi per un sistema nazionale di sicurezza informatica che sia resistente non solo dal punto di vista tecnologico, ma anche solido nel rispetto delle normative e dei valori fondamentali della nostra società. L'introduzione di queste figure specializzate rappresenta un passo cruciale verso la costruzione una cultura della sicurezza informatica diffusa, consapevole e flessibile alle mutevoli minacce cyber, garantendo sempre la protezione dei diritti umani e delle infrastrutture critiche.

ESEMPIO: L'Estonia, riconosciuta a livello mondiale per le sue avanzate infrastrutture digitali e la sua resilienza cyber, ha sviluppato l'Estonian Cyber Range, un ambiente di formazione e simulazione. Questo programma fornisce formazione pratica su scenari di attacco cyber realistici, abbinando le competenze tecniche a lezioni su normative legali e principi etici. Partecipanti provenienti da vari settori, inclusi quelli governativi e militari, attraverso questo programma, acquisiscono le competenze necessarie per identificare, prevenire e reagire a complesse minacce informatiche, elevando così il livello generale di preparazione del paese.

4. Proposta per la Creazione di Gruppi di Lavoro Nazionali sulla Sicurezza Informatica con la Partecipazione Attiva delle Piccole e Medie Imprese

Proponiamo l'istituzione di gruppi di lavoro nazionali focalizzati sulla sicurezza informatica, con l'obiettivo di riunire una vasta gamma di attori provenienti sia dal settore pubblico che da quello privato, compresa la cruciale partecipazione delle piccole e medie imprese italiane (PMI).

L'obiettivo principale di questa iniziativa è:

• Promuovere la Collaborazione Interdisciplinare: I gruppi di lavoro saranno piattaforme per lo scambio di conoscenze, esperienze e risorse tra enti governativi, grandi aziende, PMI, istituti accademici e organizzazioni di ricerca. Questo approccio si propone di creare un ambiente nazionale dedicato alla sicurezza informatica in cui le informazioni possono circolare liberamente e le migliori pratiche essere adottate rapidamente da tutti i portatori d'interesse.

• Sviluppare strategie coordinate: Attraverso una collaborazione sinergica, i gruppi mirano a elaborare e attuare strategie di sicurezza informatica che tengano conto delle particolarità e delle esigenze di tutti i settori coinvolti. Questo approccio coordinato permetterà di ottimizzare l'utilizzo delle risorse e rispondere in modo più efficace ed efficiente alle minacce cibernetiche.

• Coordinamento da parte di ACN: L'agenzia di cybersicurezza nazionale potrebbe avere un ruolo fondamentale nel coordinare le attività dei gruppi di lavoro, garantendo che le iniziative siano allineate con le priorità nazionali e che le informazioni sensibili siano gestite in modo sicuro.

ESEMPIO: Israele è rinomato per la sua eccellenza nel campo della sicurezza informatica, in parte grazie alla stretta collaborazione tra il suo settore industriale e le istituzioni accademiche. Un esempio emblematico di questa sinergia è il CyberSpark in Beer Sheva, dove aziende tecnologiche, università e unità militari lavorano fianco a fianco. Questa collaborazione ha portato

allo sviluppo di tecnologie di sicurezza all'avanguardia e alla formazione di una nuova generazione di esperti in cybersicurezza. Il successo di CyberSpark dimostra come i gruppi di lavoro nazionali possano fungere da catalizzatori per l'innovazione e la formazione nel settore della sicurezza informatica, contribuendo a creare un ecosistema nazionale robusto e resiliente.

Queste strategie rappresentano un impegno concreto verso la costruzione di un ecosistema di cybersicurezza nazionale robusto, inclusivo e resiliente, enfatizzando la necessità di un'azione coordinata che coinvolga tutti i portatori d'interesse nel campo della sicurezza nazionale. L'adozione di queste misure nel disegno di legge sottolineerebbe l'impegno dell'Italia a diventare un leader nella risposta alle sfide di cybersicurezza, promuovendo al contempo la cooperazione e la fiducia tra il governo, il settore privato e la comunità scientifica internazionale.