News Release

Comunicato stampa

Contatti Stampa:
Mario Gazzola 0039-342-7613134
mariog64@gmail.com, mario@posthuman.it

Ricerca BSA sulla cyber security nelle leggi UE individua lacune nella preparazione degli Stati membri

MILANO — 3 marzo 2015 — BSA | The Software Alliance presenta oggi la prima ricerca sulle legislazioni nazionali dell'Unione Europea in materia di cyber security, che individua diverse pericolose lacune e frammentazioni nella preparazione di alcuni Stati comunitari a bloccare le minacce informatiche.

Il rapporto valuta le leggi nazionali, i regolamenti e le politiche in tutti e 28 gli Stati membri dell'UE in relazione a 25 criteri ritenuti essenziali per un'efficace sicurezza informatica. Esso è destinato a fornire agli Stati membri dell'Unione europea uno strumento per valutare le proprie politiche in funzione di una serie di criteri chiave e a tracciare un percorso che contribuisca a delineare i principali elementi costitutivi di un forte quadro normativo sulla sicurezza informatica.

"Analizzando le protezioni informatiche in Europa se ne trae un quadro in qualche modo *irregolare*", afferma Thomas Boué, direttore policy di BSA EMEA. "Infatti, la maggior parte degli Stati membri riconoscono che la sicurezza informatica è una priorità, eppure alcune incoerenze nel loro approccio lasciano l'intero mercato comunitario vulnerabile alle minacce. La direttiva *Network and Information Security* potrebbe aiutare a stabilire un più affidabile livello base di sicurezza informatica e di resilienza, se si concentrasse meglio nell'allineare la predisposizione alla sicurezza delle infrastrutture digitali più critiche in Europa e introducesse processi armonizzati di reporting e condivisione delle informazioni in tutto il mercato unico".

Tra i principali risultati della ricerca si evince che:

- la maggior parte degli Stati membri dell'UE riconoscono che la sicurezza informatica sia una priorità nazionale, in particolare per quanto riguarda le infrastrutture critiche.
- Esistono però discrepanze notevoli tra le politiche di sicurezza informatica degli Stati membri, i rispettivi quadri giuridici e le capacità operative, con conseguenti lacune nella sicurezza informatica complessiva dell'Unione Europea.
- Quasi tutti gli Stati membri dell'UE hanno istituito gruppi di risposta agli incidenti per affrontare gli attacchi informatici; tuttavia, obiettivi ed esperienza di tali team varia da Stato a Stato.

- C'è una preoccupante mancanza di cooperazione sistematica fra pubblico e privato e di collaborazione sulla sicurezza informatica tra governi dell'UE, enti non governativi e partner internazionali.
- Per quanto riguarda specificamente l'Italia, la legislazione nazionale è stata aggiornata nel 2007, poi nel 2013 e 2014 sono stati attivati piani di cybersecurity che garantiscono al nostro Paese un solido quadro regolamentare in materia. La strategia italiana sulla cybersecurity considera prioritarie le partnership pubblico-privato, ma finora nessuna forma di cooperazione in tal senso è stata ancora formalizzata. Tuttavia, nel 2014 è stato costituito il CERT-PA, Computer Emergency Response Team della Pubblica Amministrazione, struttura preposta al trattamento degli incidenti di sicurezza informatica del dominio costituito dalle pubbliche amministrazioni: certamente un passo nella giusta direzione.

La ricerca di BSA incoraggia pertanto gli Stati membri dell'UE a concentrarsi su quattro elementi chiave di un solido quadro giuridico di sicurezza informatica:

1. costruire e mantenere un quadro giuridico e politico globale basato su una strategia di sicurezza informatica nazionale che si completi con piani di sicurezza informatica specifici di settore.
2. Individuare enti con chiare responsabilità per l'operatività in campo di sicurezza informatica, di risposta agli incidenti e ai casi di emergenza.
3. Generare fiducia e lavorare in partnership con il settore privato, le ONG, i partner internazionali e gli alleati.
4. Promuovere l'educazione e la consapevolezza dei rischi e delle priorità in materia di sicurezza informatica.

Allo stesso tempo, il rapporto mette in guardia i governi europei dall'evitare inutili regimi protezionistici che possono minare, anziché migliorare, le protezioni di sicurezza informatica. In particolare, gli Stati membri dovrebbero:

- Evitare le richieste non necessarie o irragionevoli che possono aumentare i costi e limitare la scelta, tra cui forme di certificazione specifiche per un solo Paese o obblighi di compiere determinati test; mandati specifici per contenuti locali; richieste di divulgare informazioni sensibili, come codici sorgente o chiavi di cifratura e restrizioni sui diritti esteri di proprietà intellettuale.
- Invece di modificare gli standard, supportare standard tecnici definiti dall'industria di riferimento e riconosciuti a livello internazionale.
- Evitare leggi di localizzazione dei dati e garantire la libera circolazione dei dati in tutti i mercati.
- Evitare le preferenze per tecnologie autoctone che ostacolano la concorrenza internazionale e danneggiano l'innovazione globale.

la ricerca completa su tutte le 28 nazioni, così come dettagliati focus su ciascun singolo Stato membro dell'Unione Europea, sono disponibili al sito www.bsa.org/EUcybersecurity.

BSA

BSA | The Software Alliance (www.bsa.org) è la principale organizzazione del settore software. Rappresenta nei confronti dei governi e del marketplace internazionale le principali aziende a livello

mondiale, che investono ogni anno miliardi di dollari per creare soluzioni volte a potenziare lo sviluppo economico e a migliorare la vita quotidiana di tutti. Attraverso la sede di Washington e i comitati attivi in oltre sessanta nazioni, BSA sperimenta programmi volti al rispetto della legalità nel campo del software, sostiene politiche pubbliche che favoriscono l'innovazione tecnologica e lo sviluppo del mondo digitale.
Ulteriori informazioni su www.bsa.org/italia.