G7 2017 ITALIA

ALLEGATO 3

AZIONI DEL G7 PER MIGLIORARE LA SICUREZZA INFORMATICA DELLE IMPRESE

Torino, 25-26 settembre 2017

OBIETTIVO 1 - DEFINIRE E ATTUARE PRATICHE DI GESTIONE DEL RISCHIO INFORMATICO

L'ampio utilizzo delle tecnologie dell'informazione e della comunicazione (ICT) comporta il rischio di un crescente numero di incidenti informatici e violazioni che possono determinare gravi disagi nella società moderna e ingenti danni economici alle imprese. Tali incidenti possono inoltre minare la fiducia di cittadini e imprese nei confronti della società digitale, scoraggiando l'utilizzo delle tecnologie informatiche. Carenti procedure di gestione del rischio possono rappresentare una minaccia per tutti i soggetti all'interno della catena del valore e delle reti di produzione, con conseguenze sulle economie nazionali e regionali. È pertanto necessario esplorare modalità per aumentare la consapevolezza sul rischio informatico, soprattutto tra le PMI, e incoraggiare l'adozione di buone pratiche tra i consumatori.

Analogamente, è importante sostenere le PMI e le start-up innovative sul piano della sicurezza informatica, per agevolare le loro attività di ricerca, specialmente nelle prime fasi di sviluppo. Ciò comporta anche investimenti, da parte delle stesse, nella sicurezza

informatica per fronteggiare le minacce legate alla digitalizzazione, tra cui quelle che mirano a sottrarre segreti commerciali.

A tal fine, noi Ministri G7 delle ICT e dell'Industria intendiamo:

1. incoraggiare le imprese, in particolare le PMI, al loro livello di senior management, a migliorare la consapevolezza e ad adottare efficaci pratiche di gestione del rischio cibernetico, tenendo conto di metodologie di analisi del rischio comparabili;
2. promuovere la collaborazione tra i governi e le imprese, in particolare le PMI, coinvolgendo le associazioni di categoria, il mondo accademico, le associazioni della comunità tecnologica, i ricercatori nel campo della sicurezza e il settore assicurativo legato ai rischi informatici, per migliorare la base di dati relativa agli impatti economici e aziendali degli incidenti di sicurezza informatica e di violazione dei dati;
3. incoraggiare e aiutare i consumatori ad adottare pratiche attente e proattive per proteggere la loro identità in rete e a utilizzare compiutamente i servizi fiduciari di loro scelta.

OBIETTIVO 2 – MIGLIORARE LA COOPERAZIONE

La cooperazione rappresenta il fattore chiave per rafforzare la sicurezza informatica. Esistono diversi livelli di cooperazione, tutti ugualmente importanti: tra organismi tecnico-operativi, tra governi e tra governi e imprese. Ognuna di queste tipologie di cooperazione dovrebbe essere migliorata.

La cooperazione efficace e costruttiva tra i paesi del G7, tra i vari CSIRT (gruppi per la risposta agli incidenti relativi alla sicurezza informatica) nazionali e tra i CSIRT e le imprese può aumentare la possibilità di prevenire e rispondere alle minacce informatiche attraverso canali affidabili e sicuri per lo scambio di informazioni concrete su minacce potenziali ed emergenti. In quest'ambito, il ruolo dei CSIRT nazionali è importante, in quanto principale punto di riferimento in particolare per la condivisione delle informazioni a livello tecnico e operativo.

Valutare l'esposizione delle imprese alle minacce informatiche e sviluppare procedure interne idonee può aiutare le imprese, in particolare le PMI, ad aumentare la sicurezza e la resilienza dei loro processi aziendali.

La mancanza di conoscenze rende le imprese vulnerabili alle minacce e agli attacchi informatici. I paesi del G7 dovrebbero puntare ad aumentare la cultura della sicurezza informatica e migliorare la consapevolezza in particolare tra le imprese.

Le infrastrutture critiche sono generalmente gestite dal settore privato, comprese le PMI. La condivisione di informazioni per la protezione delle infrastrutture critiche dalle minacce informatiche è fondamentale ai fini della resilienza e sicurezza dei servizi essenziali per i cittadini e le imprese.

La Protezione delle Infrastrutture Critiche Informatizzate (CIIP) fa parte dell'agenda digitale di molti paesi, come pure di molte organizzazioni internazionali. Alcuni paesi hanno già messo a punto un quadro nazionale e stanno rivedendo le proprie linee guida sull'argomento.

Per questo motivo, noi Ministri delle ICT e dell'Industria del G7 intendiamo valutare modalità per migliorare la cooperazione tra il settore pubblico e privato, PMI comprese, per costruire un ambiente per l'economia digitale basato sulla consapevolezza, la sicurezza e la fiducia.

A questo scopo intendiamo:

1. promuovere una collaborazione costruttiva tra i CSIRT nazionali dei paesi del G7 e tra i CSIRT e le imprese di tutte le dimensioni, al fine di scambiare informazioni riguardo alle minacce informatiche e alle vulnerabilità;
2. considerare modalità comuni per valutare l'esposizione delle imprese alle minacce cibernetiche e per valutare l'efficacia delle relative misure di contrasto;
3. incoraggiare la comunità internazionale, attraverso la collaborazione tra imprese, governi e società civile, a considerare una serie di approcci quali la "security-by-design", le pratiche di gestione del rischio, le valutazioni di conformità rilevanti per il mercato e gli adeguati processi di valutazione della sicurezza per migliorare quest'ultima attraverso tutta la catena del valore e per stimolare la fiducia nell'economia digitale;
4. condurre campagne di sensibilizzazione tra le PMI riguardo ai rischi cibernetici e alle modalità di gestione degli stessi;
5. sostenere iniziative finalizzate alla promozione di una cultura di cooperazione, specialmente tra i governi e le imprese, per una conoscenza più efficace riguardante le minacce cibernetiche e le vulnerabilità;

6. promuovere la condivisione di informazioni attraverso la collaborazione di operatori di infrastrutture critiche, tra cui gli ISAC (*Information Sharing and Analysis Centres*, centri di analisi e condivisione di informazioni) o loro equivalenti;
7. Promuovere, fra tutti i soggetti interessati, il dialogo globale a favore della cooperazione e della condivisione di buone pratiche, tra cui quelle per la gestione del rischio informatico, ai fini della prosperità economica.