Titolo della proposta

PROTEGGERE LA RETE E LE INFORMAZIONI:

la sicurezza come bisogno primario per lo sviluppo

Proponente

Gigi Tagliapietra – CLUSIT Associazione Italiana per la Sicurezza Informatica

Pillar di riferimento

Fiducia e sicurezza

I bisogni e lo scenario

La protezione della rete digitale e delle informazioni che essa trasporta, è un fattore determinante per la crescita delle imprese e per l'efficienza della Pubblica Amministrazione ma è anche una azione strategica che tutela una infrastruttura critica per l'intero Paese.

Alla diffusione sempre più estesa di applicazioni basate sulla rete, di servizi innovativi e di utilizzatori ad ogni livello, fa riscontro una crescita sempre più diffusa di utilizzi malevoli e di minacce vere e proprie alla continuità operativa che vede gli utenti non solo come obiettivi ma come inconsapevoli perpetratori di tali attacchi attraverso le Bot-Net.

Considerazioni

Ora più che mai la protezione della rete e delle informazioni è una condizione imprescindibile perché il sistema digitale nel suo insieme possa esistere e, come già definito a livello europeo, è impossibile affrontare il tema senza il coinvolgimento diretto degli utenti che non sono più semplici fruitori ma reali artefici dello sviluppo della rete nel suo insieme.

Occorre un'azione articolata perché gli utenti abbiano piena consapevolezza delle opportunità che vengono loro offerte ma in egual misura anche delle minacce di cui sono potenziali vittime o inconsapevoli complici.

L'alfabetizzazione di massa alla sicurezza non è una iniziativa "puntiforme" o una "giornata della sicurezza" ma una attività continuativa e permanente che adegua la risposta collettiva alle diverse forme che prendono le minacce.

Le priorità

Le priorità identificate sono:

- Realizzazione di un servizio di informazione e di supporto ai singoli cittadini, sul modello dei CERT che allarghi a tutti gli utenti e alle piccole imprese la disponibilità di un servizio di supporto in caso di incidente o di attacco.

- Alfabetizzazione di massa e continuativa alla sicurezza informatica con iniziative mirate alle diverse tipologie di utenza e alle diverse fasce di età coinvolte

- Attenzione particolare agli utenti della terza età (i cosiddetti “Silver Surfers”) che sono oggi tra i soggetti più a rischio e peraltro i più avvantaggiati dai servizi innovativi che la rete offre

- Tutela specifica delle reti della Pubblica Amministrazione Locale (Comuni e enti territoriali) che pur offrendo servizi vitali per le comunità di riferimento spesso non dispongono di idonee professionalità e sistemi di continuità operativa

Le azioni concrete

AREA DI INTERVENTO	AZIONI PRIORITARIE
La rete a larga banda	• È indispensabile finanziare esplicitamente iniziative di sicurezza informatica nell'ambito dei finanziamenti previsti per la diffusione della banda larga
Il mondo delle imprese	• Bisogna sostenere le attività legate alla protezione informatica delle imprese con finanziamenti e forme di defiscalizzazione, non limitandosi a rimborsare l'acquisto di hardware e software ma premiando la messa in campo di soluzioni concrete.
La tutela degli utenti più vulnerabili	• Le azioni di sensibilizzazione devono coinvolgere innanzitutto il mondo dei media, in particolare la televisione, e una collaborazione diretta e sinergica con le associazioni dei provider che sono un referente primario degli utilizzatori privati. • Bisogna avviare una specifica iniziativa dedicata al mondo della terza età che è l'utenza oggi a maggior rischio e rappresenta una percentuale di popolazione e di utilizzatori della rete in costante crescita.
Lo sviluppo di un'industria italiana della sicurezza	• Bisogna favorire lo sviluppo e l'utilizzo di software Open Source che, integrando e interagendo con i prodotti commerciali sappiano sviluppare soluzioni a misura del tessuto reale del mondo delle imprese e delle amministrazioni pubbliche. • In un'ottica di più lungo periodo bisogna puntare sullo sviluppo di soluzioni di sicurezza guardando alle tecnologie emergenti (RFID, domotica, automotive, DTT) in una attività coordinata con le università e i centri di ricerca.

AREA DI INTERVENTO	AZIONI PRIORITARIE
Il quadro normativo	• È necessario chiarire le ambiguità delle norme esistenti, e soprattutto essere cauti con le nuove norme, pubblicando per tempo le proposte per trarre vantaggio dal dibattito pubblico
La pubblica amministrazione	• È necessario che nelle forniture il costo di una soluzione di sicurezza sia valutato non solamente nel suo valore di acquisto ma, almeno, nella sua solidità nel tempo, nel suo costo di gestione e nella sua capacità di ridurre i costi dei danni derivati da incidenti e violazioni. • Si raccomanda l'avvio anche in Italia degli ISAC (Information Sharing and Analysis Center) perchè tanto nel settore privato che in quello pubblico, la creazione di "reti di fiducia" tra persone che operano ai massimi livelli è il fattore chiave per prevenire quanto più possibile incidenti gravi ma soprattutto per gestire efficacemente le situazioni di crisi.
Specificamente per la PA locale	• Bisogna avviare una specifica attività di sensibilizzazione ai temi della sicurezza facendo percepire la criticità dei sistemi che la PA locale si trova a gestire. • Bisogna accrescere le competenze interne di primo livello e incoraggiare la condivisione di risorse specialistiche sovracomunali. • Bisogna incoraggiare lo scambio di informazioni e la costituzione di ISAC specifici per la PA Locale.