



Proteggere la rete e le informazioni per permettere l'innovazione del sistema paese

**Documento approvato
dalla assemblea generale del CLUSIT**

Milano, 31 Maggio 2006



Contenuti:

Premessa	3
Executive Summary	4
Lo scenario	8
Le minacce	8
Gli attacchi "Zero Day"	8
Il nuovo volto dell'hacking	9
Le evoluzioni in atto	9
Il bisogno di una iniziativa specifica	9
La sicurezza come funzione strategica trasversale	11
Governance della sicurezza	11
Consapevolezza e azioni	12
Gli insiemi su cui agire	12
Il quadro normativo	13
La pubblica amministrazione	14
Lo specifico della PA locale	15
La rete a banda larga	17
Il mondo dell'impresa	18
La tutela degli utenti più vulnerabili	19
Lo sviluppo di un'industria italiana della sicurezza	21
Il Clusit	23

Premessa

È ormai accettato a tutti i livelli che la rete digitale (intendendo con la definizione generica l'insieme di infrastrutture, informazioni e servizi) è un sistema strategico indispensabile alla vita di un paese, delle sue imprese, dei suoi cittadini.

La sua crescente diffusione, la crescita della velocità di trasmissione, la sua utilizzazione sempre più mirata a contenuti e servizi di valore sia per le istituzioni che per le imprese e i singoli, è accompagnata da una crescita altrettanto preoccupante delle vulnerabilità e degli attacchi che ad essa vengono portati.

È necessario e urgente quindi porre grande attenzione al tema della sicurezza delle informazioni, non tanto come attività tecnologica in sé, ma come fattore abilitante, indispensabile all'utilizzo della tecnologia per ottenere innovazione, crescita e sviluppo.

Il nostro Paese sconta un ritardo preoccupante sul tema perchè, nonostante si sia fatto molto negli ultimi anni, la crescita dei rischi è superiore alla velocità con cui si cerca di recuperare il terreno perduto.

Con questo documento il CLUSIT, la principale associazione Italiana nella sicurezza informatica che raggruppa istituzioni, imprese, fornitori e singoli cittadini, intende segnalare all'attenzione del Governo e delle forze politiche le priorità d'intervento e le raccomandazioni circa le criticità più significative, suggerimenti che nascono dall'esperienza che il CLUSIT ha maturato in sei anni di attività finalizzata alla crescita della sicurezza complessiva dei sistemi informatici del nostro Paese.

Executive Summary

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.

Le minacce

Il fenomeno più grave a cui si sta assistendo è oggi rappresentato da una crescita costante e preoccupante della criminalità on-line con azioni che vanno dalla cattura di codici di accesso (Phishing) a vere e proprie truffe, la combinazione tra utilizzo criminale della tecnologia e la crescita della sua sofisticazione, creano una miscela particolarmente pericolosa.

Gli attacchi Zero Day

La finestra temporale che intercorre tra quando la vulnerabilità di un sistema informatico è identificata e documentata e il momento in cui viene rilasciato il primo codice maligno in grado di sfruttarla (exploit), si sta rapidamente assottigliando fino a giungere ai cosiddetti "Zero Day attack" ovvero attacchi che sfruttano immediatamente le vulnerabilità di un sistema prima che ne sia nota l'esistenza e approntata la difesa.

Minacce in grado di diffondersi su scala planetaria nel giro di pochi minuti hanno già fatto la loro comparsa!

Lo sviluppo tecnologico

Il wireless, la messaggistica istantanea, il Voice over IP e i servizi convergenti triple play, sono solo alcuni dei cambiamenti tecnologici che cittadini, imprese, organizzazioni pubbliche e operatori di telecomunicazione sono in procinto di abbracciare, con un aumento esponenziale del numero di utenti, purtroppo inversamente proporzionale al livello medio di consapevolezza delle relative implicazioni di sicurezza.

Governance e sicurezza

Data la serietà della situazione è indispensabile che tra i compiti che saranno affidati agli organismi che orienteranno lo sviluppo tecnologico e l'innovazione del Paese, vi siano precisi compiti di governance della sicurezza per garantire che le soluzioni proposte siano sicure, che i sistemi siano adeguatamente protetti e ne sia garantita la continuità operativa e il rapido ripristino in caso di incidente e che ai cittadini e agli utenti sia data ampia informazione circa le potenzialità offerte dalla rete digitale ma anche conoscenze e suggerimenti perchè possano difendersi da utilizzi criminali.

Gli insieme su cui agire

Il CLUSIT ha identificato alcune aree d'azione prioritarie, definendo insieme in cui è necessario agire con tempestività.

- Il quadro normativo
- La pubblica amministrazione con particolare riferimento alla PA locale
- La rete a larga banda
- Il mondo delle imprese
- La tutela degli utenti più vulnerabili
- Lo sviluppo di un'industria italiana della sicurezza

La sintesi delle raccomandazioni

Il documento che qui proponiamo identifica azioni concrete da intraprendere immediatamente per garantire che attraverso la sicurezza, l'innovazione sia non solo efficace ma addirittura possibile.

Questo è il quadro sintetico delle proposte per le sei aree di intervento:

AREA DI INTERVENTO	AZIONI PRIORITARIE
<i>Il quadro normativo</i>	<ul style="list-style-type: none"> • 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
<i>La pubblica amministrazione</i> <i>Specificamente per la PA locale</i>	<ul style="list-style-type: none"> • 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. • 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.

AREA DI INTERVENTO	AZIONI PRIORITARIE
<i>La rete a larga banda</i>	<ul style="list-style-type: none"> • È indispensabile finanziare esplicitamente iniziative di sicurezza informatica nell'ambito dei finanziamenti previsti per la diffusione della banda larga
<i>Il mondo delle imprese</i>	<ul style="list-style-type: none"> • 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.
<i>La tutela degli utenti più vulnerabili</i>	<ul style="list-style-type: none"> • 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.
<i>Lo sviluppo di un'industria italiana della sicurezza</i>	<ul style="list-style-type: none"> • 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.

Lo scenario

La chiara identificazione e comprensione dei rischi a cui sono esposti i sistemi informatici –aziendali, istituzionali, domestici– interconnessi in rete costituisce l'essenziale premessa di una cultura della sicurezza informatica che in sé rappresenta un cruciale fattore di abilitazione allo sviluppo del Paese: dalla consapevolezza non solo delle potenzialità, ma anche delle implicazioni di Sicurezza nell'accesso alla Rete e ai suoi servizi dipende infatti l'effettiva possibilità di trarre autentico e pieno beneficio dalle nuove tecnologie informatiche e di telecomunicazione (peraltro tra loro convergenti) per il beneficio dei singoli, delle aziende e del sistema pubblico.

Le minacce

Il fenomeno più grave a cui si sta assistendo è oggi rappresentato da una crescita costante e preoccupante della criminalità on-line con azioni che vanno dalla cattura di codici di accesso (Phishing) a vere e proprie truffe.

Non sono certo scomparse le minacce relative a ciò che viene definito malware in senso esteso, programmi maligni in grado di auto-propagarsi e incorporare meccanismi di attacco multiplo (le cosiddette minacce combinate, multivettoriali), anzi sono anch'esse in preoccupante crescita, ma la combinazione tra utilizzo criminale della tecnologia e la crescita della sua sofisticazione, creano una miscela particolarmente pericolosa.

Gli attacchi "Zero Day"

A proposito di vulnerabilità, la finestra temporale che intercorre tra quando la vulnerabilità di un sistema informatico è identificata e documentata e il momento in cui viene rilasciato il primo codice maligno in grado di sfruttarla (exploit), si sta rapidamente assottigliando.

Un tempo non molto lontano questa finestra era ampia 6 o più mesi, il che consentiva un ragionevole preavviso ai responsabili della sicurezza e agli amministratori per affrontare ciascuna vulnerabilità con una buona dose di pianificazione; un privilegio che ormai –comunque– non si ha più. La probabilità di confrontarsi con un "Day Zero" reale –ovvero vulnerabilità ed exploit rilasciati contestualmente– non è mai stata infatti più elevata come lo è oggi. Minacce in grado di diffondersi su scala planetaria nel giro di pochi minuti hanno già fatto la loro comparsa!

Ad esempio il worm Slammer ha dimostrato già nel lontano 2002 la capacità di raddoppiare il numero di sistemi compromessi ogni 8,5 secondi, essendo arrivato a colpire in soli 10 minuti il 90% di quelli che gli erano vulnerabili sul pianeta.

Le minacce flash, che impiegano meno di 30 secondi a diffondersi completamente, sono indubbiamente il prossimo passo per una comunità di hacker e criminali, sempre in cerca di nuove sfide i primi, di facili e lucrose fonti di profitto illecito i secondi. In considerazione dell'elevato tasso di adozione dei servizi Internet a banda larga nel nostro Paese e del sempre maggiore grado di connettività globale, sembra effettivamente plausibile che tali minacce faranno la propria comparsa nel giro di pochi anni.

Il nuovo volto dell'hacking

Contestualmente a queste dinamiche sul fronte delle minacce stiamo assistendo ad una sempre maggiore infiltrazione di hacker "professionisti" nelle grandi armate dei malintenzionati.

È significativo notare che in passato gli hacker e in generale gli autori di codici maligni hanno avuto generalmente bersagli non ben identificati e le loro stesse motivazioni, per quanto variegata, raramente esulavano dallo spirito goliardico e vandalico.

Negli ultimi anni invece la posta in gioco si è alzata, e con essa le mire di vere e proprie organizzazioni criminali o terroristiche, che trovano nello strumento informatico la propria via all'estorsione, al ricatto, al sabotaggio industriale, al terrorismo cibernetico. Maggiori risorse economiche a loro disposizione, obiettivi meglio identificati e identificabili, e la loro stessa organizzazione non faranno che rafforzare e accelerare lo sviluppo verso approdi strettamente criminali di ciò che definiamo malware.

Le evoluzioni in atto

La prospettiva più ampia in cui sviluppare un piano di politica nazionale in materia di Sicurezza Informatica deve poi prendere atto del fatto che l'Information Technology nel suo complesso sta evolvendo rapidamente, continuando ad espandersi in nuove aree e a definire nuove applicazioni.

Il wireless, la messaggistica istantanea, il Voice over IP e i servizi convergenti triple play, sono solo alcuni dei cambiamenti tecnologici che cittadini, imprese, organizzazioni pubbliche e operatori di telecomunicazione sono in procinto di abbracciare, con un aumento esponenziale del numero di utenti, purtroppo inversamente proporzionale al livello medio di consapevolezza delle relative implicazioni di sicurezza.

Il bisogno di una iniziativa specifica

È dunque avendo in mente anche questo crescente differenziale che risulta cruciale impostare fin da subito e con prospettiva di sviluppo strategico uno schema coordinato di iniziative, regolamentazioni, raccomandazioni atte ad allineare gli opportuni investimenti, meccanismi, requisiti e pratiche di sicurezza con l'utilizzo

diffuso e sempre più ubiquo della Rete e dei suoi servizi, non confondendo la Sicurezza Informatica come un fattore di intralcio allo sviluppo tecnologico informatico nel nostro Paese, quanto piuttosto intendendola e conseguentemente valorizzandola come risorsa cruciale e fattore di abilitazione –perciò stesso– di competitività e di sviluppo.

È evidente che la natura, la rapidità di propagazione e la poliedricità delle minacce emergenti, invocano l'impellente necessità di una politica di sicurezza informatica nazionale che si ponga l'obiettivo strategico di un'informatizzazione "sostenibile" nel nostro Paese oltre che di tutela dei cittadini, delle aziende, delle organizzazioni, della riservatezza e integrità dei rispettivi dati e dell'accesso e fruizione dei servizi in Rete.

La sicurezza come funzione strategica trasversale

Nelle indicazioni programmatiche che sono state presentate dall'attuale Governo durante la campagna elettorale, sono state indicate sei linee strategiche d'azione

- Le infrastrutture di rete
- L'Ict per "reinventare" la Pubblica Amministrazione
- L'Ict per la Competitività delle Imprese
- Lo sviluppo dei contenuti digitali in Rete
- Il "Technology Transfer"
- I Giovani, la Rete, i Diritti Digitali

La sicurezza rappresenta una funzione trasversale a tutte e sei, come vedremo in dettaglio qui di seguito, e deve essere identificata e garantita fin dalle fasi progettuali come una condizione essenziale allo sviluppo di sistemi innovativi o di supporto all'innovazione.

È ormai comprovato che qualsiasi intervento di securizzazione "a posteriori" quando non addirittura impossibile, è certamente più costoso e inefficiente e la mancanza di idonee misure di sicurezza ritarda l'attuazione e diffusione di progetti che dal punto di vista dei contenuti e delle finalità sono in sé encomiabili.

Governance della sicurezza

Il Governo ha altresì presentato un chiaro disegno di governance dell'innovazione con il Consiglio Nazionale per l'Innovazione, il Comitato Strategico per l'Innovazione e un Organismo Tecnico di coordinamento per le attività di progettazione, standardizzazione e monitoraggio.

Anche in questo caso occorre che tra i compiti di governance vi sia la garanzia che le soluzioni proposte siano sicure, che i sistemi siano adeguatamente protetti e ne sia garantita la continuità operativa e il rapido ripristino in caso di incidente e che l'azione combinata delle diverse iniziative punti ad accrescere il livello complessivo di sicurezza informatica del Paese che, come abbiamo già detto, presenta gravi vulnerabilità.

Consapevolezza e azioni

È fuor di dubbio che l'attività primaria sia quella di far crescere a tutti i livelli la consapevolezza del valore della rete come risorsa strategica e, in quanto valore, la necessità della sua protezione a tutti i livelli.

Le attività di "awareness", che spesso sono scambiate per campagne pubblicitarie, richiedono invece un insieme di azioni coordinate in direzioni diverse e simultanee, un impegno continuo e tempi lunghi perchè si possa raggiungere un livello di diffusione e comprensione accettabile.

Esistono in proposito molti esempi in Europa di cui fare tesoro (pensiamo, ad esempio al BSI tedesco) e anche nel nostro Paese non sono mancate iniziative lodevoli che però, data la loro estemporaneità, perdono con il tempo la loro efficacia.

La sensibilizzazione è una condizione di base ma sono le azioni concrete e le attività mirate che debbono segnare un preciso indirizzo innovativo nella sicurezza delle informazioni.

Gli insiemi su cui agire

Il CLUSIT ha identificato alcune aree d'azione prioritarie, definendo insiemi in cui è necessario agire con tempestività.

- Il quadro normativo
- La pubblica amministrazione con particolare riferimento alla PA locale
- La rete a larga banda
- Il mondo delle imprese
- La tutela degli utenti più vulnerabili
- Lo sviluppo di un'industria italiana della sicurezza

Il quadro normativo

Un'altro aspetto senz'altro importante è quello della chiarezza e correttezza delle normative. Abbiamo molte normative ambigue, spesso contraddittorie e soggette a interpretazione. Noi tecnici stessi ci rendiamo conto che l'ICT nel suo insieme e la sicurezza più in particolare, è un contesto in rapida evoluzione e che introduce concetti e problematiche realmente nuovi, e che non è affatto facile prevedere gli sviluppi delle tecnologie, le conseguenze ed i risvolti delle norme.

Azione

È necessario chiarire le ambiguità delle norme esistenti, e soprattutto essere cauti con le nuove norme, pubblicando per tempo le proposte in modo da trarre vantaggio dal dibattito pubblico; ad esempio, molte storture contenute nel decreto Urbani (non tutte) sono state corrette proprio in seguito ai commenti dati dalla comunità.

Bisogna avere l'umiltà di capire che nessun tecnico/politico/superconsulente o commissione ristretta è in grado di fornire da solo le competenze necessarie.

Talune iniziative legislative, pensiamo al travagliato iter della legge sulla privacy, partono da principi assolutamente condivisibili e forti ma per eccesso di dettaglio prendono poi forme attuative eccessivamente farraginose o che in poco tempo sono del tutto inefficaci (pensiamo alla imposizione di aggiornare gli antivirus almeno ogni 6 mesi: con le minacce attuali il dettame della legge è del tutto inefficace). Per non dire della perdita di credibilità di norme che si è costretti a rinviare continuamente nel tempo.

In altri casi, pensiamo ai decreti emessi sulla data-retention in conseguenza agli attacchi terroristici di Londra, forse per dimostrare una rapidità d'azione, si emettono normative generiche, inattuabili in termini pratici e inefficaci tecnicamente rispetto agli obiettivi che si intendevano raggiungere.

Si da poi il caso di norme, pensiamo al decreto per la disciplina dei servizi a sovrapprezzo, che presentate come encomiabile iniziativa per difendere gli utenti dalle truffe legate ai sistemi che chiamano numeri telefonici ad alto costo all'insaputa degli utilizzatori, introducono concetti (l'erogazione di servizi a sovrapprezzo basati su indirizzi IP) che aprono falle ancora più pericolose di quelle che si volevano chiudere.

La Pubblica Amministrazione

Non c'è dubbio che la diffusione crescente dell'utilizzo delle tecnologie dell'informazione nella Pubblica Amministrazione rappresenti un cambiamento significativo non solo nei suoi modelli organizzativi ma soprattutto nel rapporto con la vita quotidiana di milioni di cittadini.

In questo contesto i riferimenti alla sicurezza sono espliciti e strutturali tanto nei mezzi (Firma digitale, posta elettronica certificata, carte elettroniche) che nelle modalità di fruizione. E non potrebbe essere altrimenti. Senza sicurezza, ad esempio, nella validità, autenticità e disponibilità delle informazioni, senza la difesa di tali informazioni da intrusioni e abusi l'intero progetto vedrebbe minata la sua stessa esistenza.

È del tutto evidente come la PA stia compiendo grandi sforzi per agire simultaneamente sui due fronti, quello della digitalizzazione dell'informazione e quella della sua protezione e dobbiamo valutare positivamente questo processo, anche se ancora contraddittorio, che vede i due aspetti intrinsecamente connessi e non come nel recente passato in cui ci si preoccupava della sicurezza quando i sistemi erano ormai attivi (e, purtroppo, esposti a grandi rischi).

Azione

La prima area d'azione riguarda il modello di valutazione del costo dei sistemi di sicurezza nella PA. Di certo tutti vorrebbero sistemi di protezione estremamente sicuri, a bassissimo costo e ad altissime prestazioni ma queste tre condizioni sono, almeno per il momento, inconciliabili. Nella PA in passato hanno prevalso i criteri di scelta di tipo economico e le stesse gare d'appalto assegnano punteggi molto rilevanti alla voce "prezzo" e quindi non potremmo aspettarci sistemi sicuri o performanti. In questo senso dobbiamo auspicare un cambio di rotta, quanto meno che identifichi il costo di una soluzione di sicurezza non 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.

La seconda area d'azione riguarda le iniziative di scambio di informazioni, è questa un'attività di importanza strategica perchè la risposta a minacce di cui i contorni non sono prevedibili e con attacchi a propagazione immediata, la risposta non può essere affidata alla sola tecnologia.

È un fatto estremamente positivo che stiano crescendo e coordinando le proprie iniziative i CERT (I team di sorveglianza e di risposta agli incidenti) all'interno della PA è però preoccupante il ritardo accumulato e che non pare colmabile senza investimenti più coraggiosi.

Ma un ritardo ancora più grave lo stiamo segnando nel campo della raccolta e condivisione di informazioni che possono aiutare a prevenire incidenti che potrebbero avere conseguenze devastanti.

Azione

A questo proposito il CLUSIT raccomanda l'avvio anche in Italia degli ISAC (Information Sharing and Analysis Center) sul modello attivo da molti anni negli USA 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.

Lo specifico della PA locale

Esistono in Europa 112.119 entità di governo locale (fonte Eurostat) e anche nel nostro Paese gli Enti Locali rappresentano una quantità numerica estremamente rilevante (solo i comuni sono più di 8.000) .

Ciò che le accomuna oggi è l'utilizzo diffuso delle tecnologie dell'informazione sia per l'interscambio tra enti e con l'amministrazione centrale che per la gestione diretta di servizi che per l'erogazioni di servizi ai cittadini.

In più le amministrazioni locali gestiscono informazioni "strategiche" per la vita dei cittadini, informazioni che hanno un elevato valore per la specifica comunità a cui fanno riferimento e molte di esse offrono spazi di accesso e connettività a scuole, biblioteche, centri sociali.

Ma ciò che le accomuna è anche una insufficiente conoscenza tecnica in materia di sicurezza, budget scarsi o nulli ma soprattutto l'inconsapevolezza della criticità delle informazioni e dei sistemi che gestiscono rispetto a una visione complessiva della rete.

Se si condivide il concetto, tipico nel mondo della sicurezza, che un sistema è "forte" quanto il suo elemento "più debole", dobbiamo dire che gli Enti Locali rappresentano per l'intera rete un elemento di **grave vulnerabilità**.

Gli incidenti verificatisi di recente nei sistemi informativi di una grande città ci hanno dato solo un campanello d'allarme che sarebbe colpevole non ascoltare.

Ma l'attenzione da porre verso la PA locale deve anche tenere conto del fatto che essa è il primo punto di contatto con i cittadini e che è sempre in prima linea nella gestione di incidenti o di emergenze e non farà eccezione anche in caso di incidente informatico grave.

Azione *Bisogna avviare una specifica attività di sensibilizzazione ai temi della sicurezza soprattutto facendo percepire la criticità dei sistemi che la PA locale si trova a gestire.*

Azione *Bisogna accrescere le competenze interne di primo livello e incoraggiare la condivisione di risorse specifiche sovracomunali su un modello concettuale analogo a quello "infermiere-medico-specialista" tipico del mondo sanitario.*

Azione *Bisogna incoraggiare lo scambio di informazioni (ISAC) e la costruzione di reti "trusted" in grado di rilevare e circoscrivere efficacemente anomalie e attacchi e formare alla ripartenza in caso di incidente.*

Gli Enti Locali devono diventare non solo erogatori di servizi affidabili e sicuri ma essere parte attiva nella realizzazione di ambienti tutelati e sicuri, partendo dalle reti scolastiche, ed essere in prima linea nella alfabetizzazione diffusa dei propri cittadini.

La rete a banda larga

Il discorso sull'infrastruttura di rete è estremamente articolato ma riteniamo prioritaria la securizzazione della rete a larga banda.

Più le connessioni veloci e continue si diffondono, più si alza il rischio che un computer non protetto entri in rete divenendo sia vittima di intrusioni che veicolo di attacchi agli altri sistemi. Un attacco di "distributed denial of service" che faccia leva su milioni di inconsapevoli utenti di rete ad alta velocità, vulnerabili perchè nulla è stato fatto per proteggerli potrebbe avere effetti devastanti per l'intera rete.

Una rete ad alta velocità totalmente indifesa nelle sue connessioni terminali rappresenta inoltre un fattore di propagazione esponenziale di qualsiasi tipo di "infezione" informatica.

Azione

Come abbiamo già avuto modo di segnalare al Governo in occasione della nostra assemblea del 27 maggio 2005, è indispensabile inserire specifiche iniziative di sostegno alla sicurezza informatica nell'ambito dei finanziamenti previsti per la diffusione della banda larga.

È inoltre necessaria un'operazione di sensibilizzazione di tutti gli utenti delle linee a banda larga, ADSL e fibra, affinché capiscano l'importanza di dotarsi di adeguati sistemi di protezione.

Il mondo dell'impresa

Nelle aziende più grandi ormai la consapevolezza ad alto livello è certamente diffusa (anche se non altrettanto le necessarie azioni concrete che dovrebbero seguire), sia per il grande rilievo dato dai mezzi di comunicazione ai temi della sicurezza e anche perchè il forte utilizzo personale della rete e della posta rende tangibile ai singoli l'indispensabilità di tali servizi.

Nelle aziende di dimensioni più contenute ci si è illusi di una sorta di "immunità" dovuta proprio alla dimensione modesta ma i codici maligni di tipo generalizzato, spyware, worm, virus, per non parlare dello spam, hanno ormai reso evidente che siamo tutti bersagli perchè siamo passati "dalla spada alla mitragliatrice".

Nelle piccole e medie imprese il ruolo del computer per lo svolgimento del lavoro quotidiano è talmente determinante che per talune di esse, pensiamo agli esportatori o alle aziende che vivono di ordini on-line, è davvero questione di vita o di morte.

Azione

Nelle iniziative di sostegno e finanziamento all'innovazione bisogna incoraggiare in modo specifico le attività legate alla protezione informatica delle imprese, non limitandosi a rimborsare l'acquisto di hardware e software ma premiando la messa in campo di soluzioni concrete, realizzate specificamente per il mercato italiano delle PMI, possibilmente da parte di aziende italiane e con ampio utilizzo di soluzioni Open Source per favorire la system integration.

La tutela degli utenti più vulnerabili

Preparare i propri cittadini ad utilizzare in modo sicuro gli strumenti che presto saranno la principale via di interazione con le amministrazioni, le banche e le aziende a vario titolo è un compito preciso delle istituzioni a tutti i livelli.

Non si tratta di semplicemente raccomandare l'utilizzo di prodotti, nè tantomeno spaventare l'utenza elencando tutti i possibili pericoli di truffe e abusi in cui possono incorrere in rete.

Come già evidenziato in sede europea nel gruppo di lavoro sulla security awareness dell'ENISA, occorre fare leva fattori positivi e sui valori e i vantaggi che la rete è in grado di offrire, inserendo il discorso della sicurezza come fattore positivo di tutela e protezione non solo di beni materiali ma anche di valori etici come la privacy e la confidenzialità.

Azione

Le azioni da intraprendere 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 in quanto, nella maggior parte dei casi, il loro primo punto di contatto tecnologico.

Un ulteriore prezioso canale di comunicazione, informazione e consapevolezza è rappresentato dalle associazioni culturali, dal mondo no-profit, dalle associazioni dei consumatori con le quali condividere un progetto di alfabetizzazione diffusa e continua.

Esistono però speciali categorie di cittadini che necessitano di una tutela particolare.

Certamente il mondo dei minori è al primo posto e in questo senso va ricordato fra l'altro che il nostro Paese è stato il primo al mondo (Carta dei diritti dei minori in rete "Onde" 1998) a porre l'attenzione sul tema, invitando, fra l'altro a un approccio positivo e non censorio.

A sua volta il CLUSIT da anni ha attivo un progetto specifico per la promozione della salvaguardia dei minori in rete e partecipa al massimo livello alle iniziative istituzionali specifiche a cui si è dato vita in questi anni.

Ma vi è una nuova categoria di soggetti che sono particolarmente esposti ed indifesi e che quindi necessitano di specifica tutela nell'accesso alla rete ed ai suoi servizi: gli anziani.

Per le persone anziane la rete rappresenta un insostituibile strumento di inclusione sociale oltre che di fruizione di servizi e la loro positiva apertura alle tecnologie, associata ad una inconsapevolezza dei rischi in cui possono incorrere, li rende estremamente vulnerabili.

Azione

Alle iniziative generiche di formazione ed educazione alla sicurezza informatica va quindi associata una specifica iniziativa dedicata al mondo della terza età che, fra l'altro, rappresenta una percentuale di popolazione molto significativa e in costante crescita.

Lo sviluppo di un'industria italiana della sicurezza

Il mercato italiano dei prodotti e dei servizi di sicurezza è stimato oggi in circa 700 milioni di Euro (fonte IDC) con una previsione al 2008 a 930 milioni e un tasso di crescita aggregato che supera il 18%.

Una recente indagine condotta dal CLUSIT tra i propri associati, ha mostrato come la maggior parte delle aziende italiane attive nel mercato della sicurezza, sia composta da imprese di dimensioni contenute: l'87% ha meno di 20 dipendenti, il 40% fattura meno di 500 mila euro all'anno.

Il 70% di esse opera su base locale dove realizza più dei 2 terzi del proprio fatturato e sono pochissime quelle che sviluppano prodotti originali e ancora meno le aziende in grado di esportare e di operare al di fuori dei confini nazionali.

Ma non c'è da sorprendersi. L'offerta di soluzioni di sicurezza è lo specchio del sistema su cui si basa nel nostro Paese anche l'offerta ICT più in generale e, in buona sostanza è lo specchio del sistema produttivo in cui oltre 4 milioni di aziende, il 99% del totale delle imprese, ha meno di 20 dipendenti.

Non è pensabile un drastico cambiamento di questa struttura ma non è nemmeno accettabile una resa incondizionata ad un ruolo di semplici rivenditori ed installatori di prodotti di importazione.

Il dato più significativo che emerge dai dati di analisi del mercato è la crescita significativa dei servizi legati al mondo della sicurezza che nel 2008 rappresenteranno più del 50% del mercato complessivo: Il nostro vero capitale potrebbe essere la competenza nell'adottare correttamente le tecnologie, nuove o vecchie che siano.

Per rispondere alle nuove sfide imposte dalla securizzazione della rete occorreranno sempre più "funzionalità" che non pure "tecnologie" e sistemi con alto contenuto innovativo e "creativo" che possano rispondere alla sofisticazione degli attacchi che si affacciano all'orizzonte e nel contempo siano adeguate alla specificità e articolazione del tessuto produttivo e amministrativo del nostro Paese.

Azione

In questo contesto bisogna favorire lo sviluppo e l'utilizzo di software Open Source che, integrando e interagendo con i prodotti commerciali sappiano sviluppare soluzioni a misura sia del tessuto reale tanto del mondo delle imprese che delle amministrazioni pubbliche.

Azione

In un'ottica di più lungo periodo bisogna puntare invece 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.

IL CLUSIT

Il CLUSIT, i cui soci rappresentano oltre 400 aziende e organizzazioni, è la più importante associazione italiana nel campo della sicurezza informatica.

Al CLUSIT aderiscono aziende, istituzioni e singoli individui, che rappresentano l'intero Sistema-Paese.

Il Clusit collabora, a livello nazionale, con diversi Ministeri, Authority e Istituzioni, con la Polizia Postale e con altri organismi di controllo. Svolge una intensa attività di supporto e di scambio con le Confederazioni Industriali, numerose Università e centri di ricerca e con le associazioni professionali e dei consumatori.

In ambito europeo partecipa a molteplici iniziative in partnership con i CLUSI (Belgio, Francia, Svizzera, Lussemburgo), collabora con diverse istituzioni e Università e sostiene attivamente le attività di ENISA (European Network and Information Security Agency).



CLUSIT

Associazione Italiana per la Sicurezza Informatica

Sede legale presso:

Dipartimento di Informatica e Comunicazione

Università degli Studi di Milano

Via Comelico 39 - 20135 MILANO

www.clusit.it – info@clusit.it

tel. 347 23 19 285