La sicurezza delle reti e dei sistemi informativi: il ruolo degli ingegneri dell'informazione

Massimiliano Pittau

Bari, 8 settembre 2011

Il caso Solo in serata ripreso il servizio per i convogli a lunga percorrenza. Esclusa l'azione di hacker o il sovraccarico

Trenitalia, le biglietterie in tilt per ore

Guasto al sistema informatico Ibm, la stessa società dei disagi alle Poste

Servizi pubblici. Nuovi problemi anche ieri per pagamenti e bollettini in tutta Italia - Nel pomeriggio situazione normalizzata

Software bloccati, le Poste in tilt

Nel mirino dell'azienda l'azione di Ibm e Hp - L'ipotesi della richiesta danni

Software in panne, Piazza Affari nel caos

Un guasto informatico ha paralizzato le contrattazioni di ieri fino alle 15.30 - Proteste da Londra

Sotto scacco dei pirati online

Oltre 450 milioni di utenti privati dei dati personali e delle carte di credito

Ipotesi e fantaipotesi

Errore nella progettazione dei software per i listini

Il caso L'azione di Anonymous Italy

Hacker danno l'assalto al sito del governo Assedio per 40 minuti

Giappone. Violati un milione di account

Attacco hacker ai server della Sony

L'intrusione

«Playstation, in vendita dati di 2 milioni di carte»

Grand theft data

Technology The capture of personal details belonging to millions of Sony's PlayStation Network users highlights the growing value of online activities – to criminals as well as businesses, writes **Richard Waters**

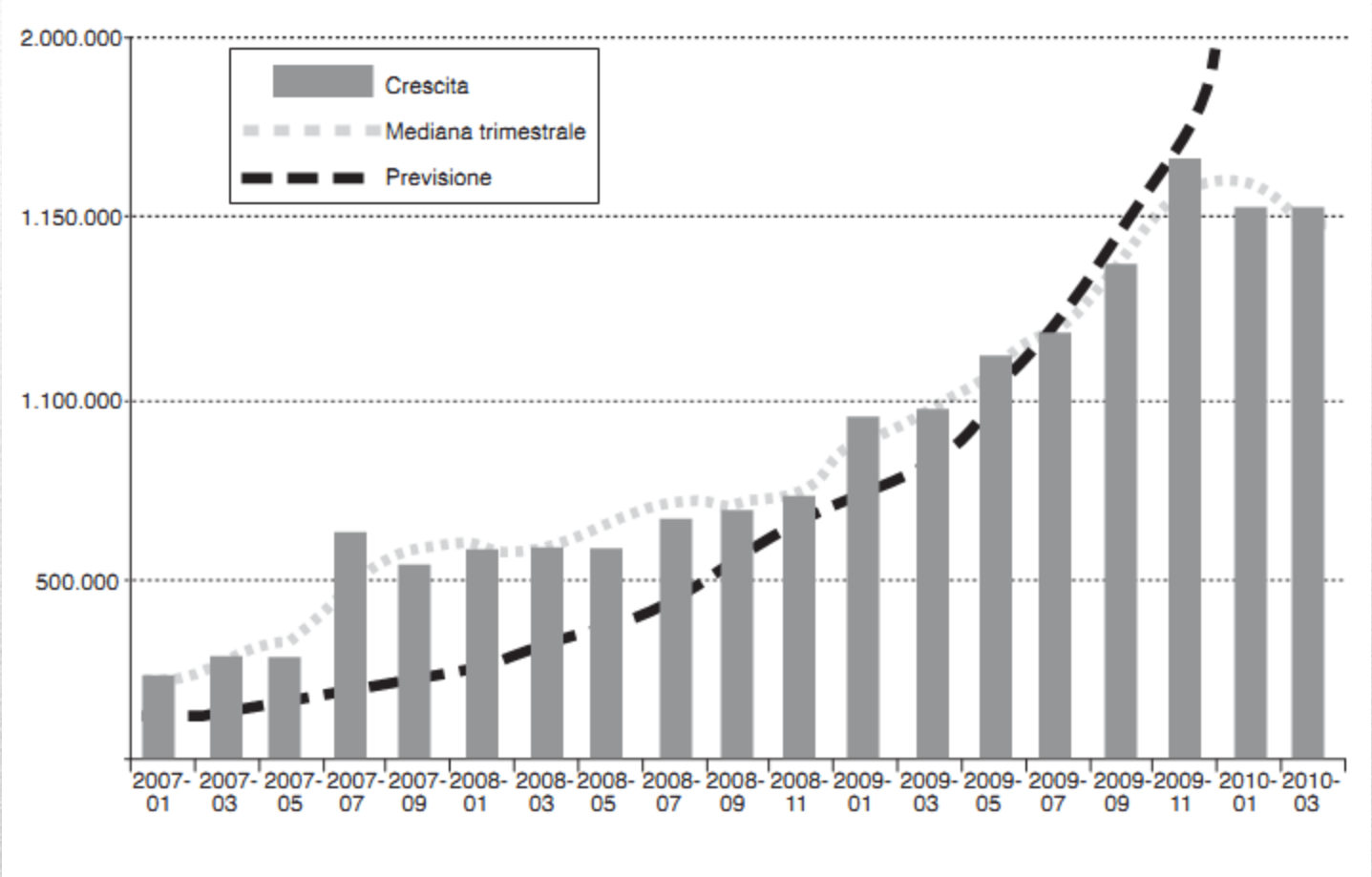
Sicurezza e Internet I punti deboli e i consigli per evitare i blackout dei siti e della posta elettronica

Incendi, guasti, hacker: i buchi della Rete

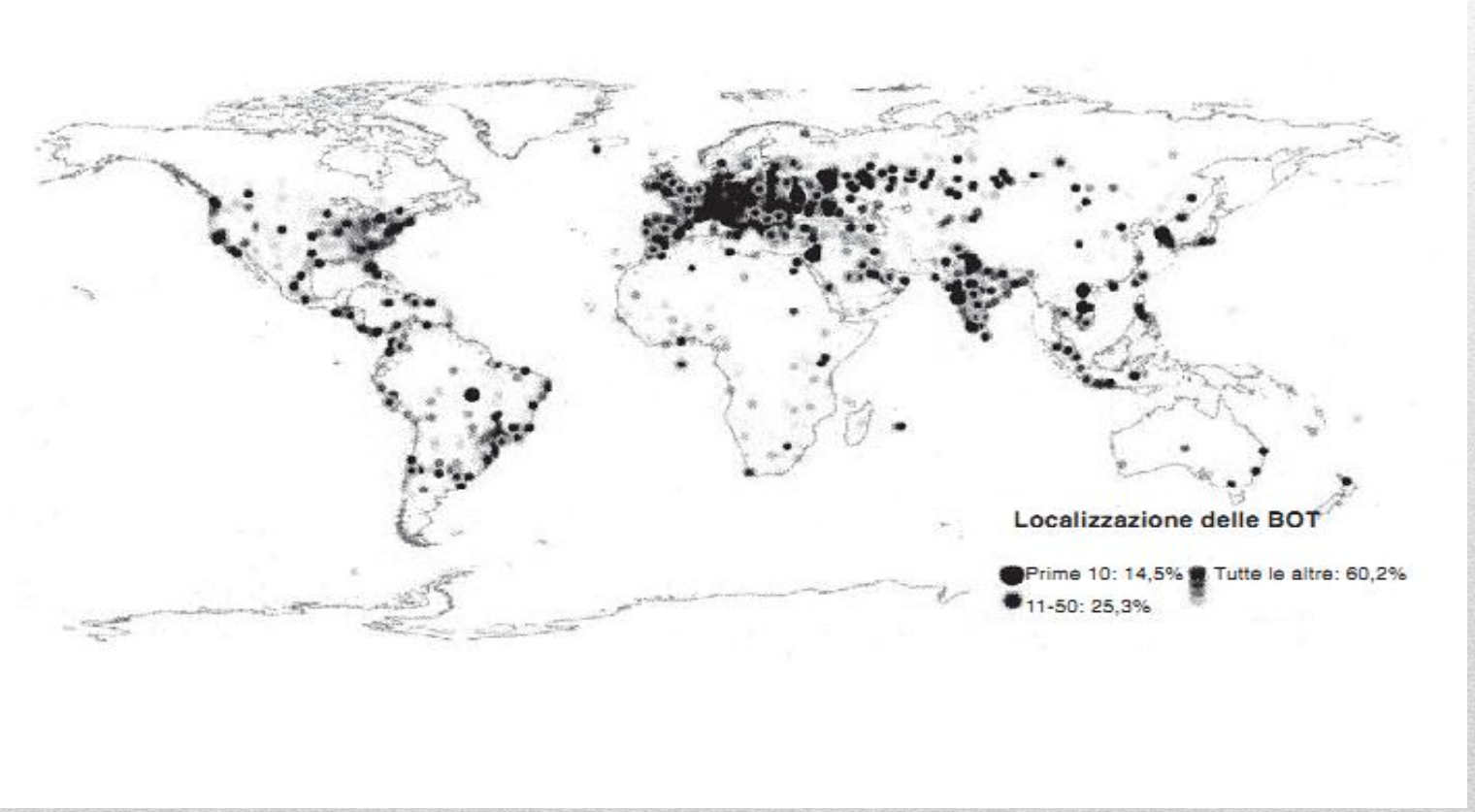
Le preoccupazioni dopo il caso Aruba. Gli esperti: rischi seri se non si investe

La Sicurezza della Rete una Comodità a Caro Prezzo

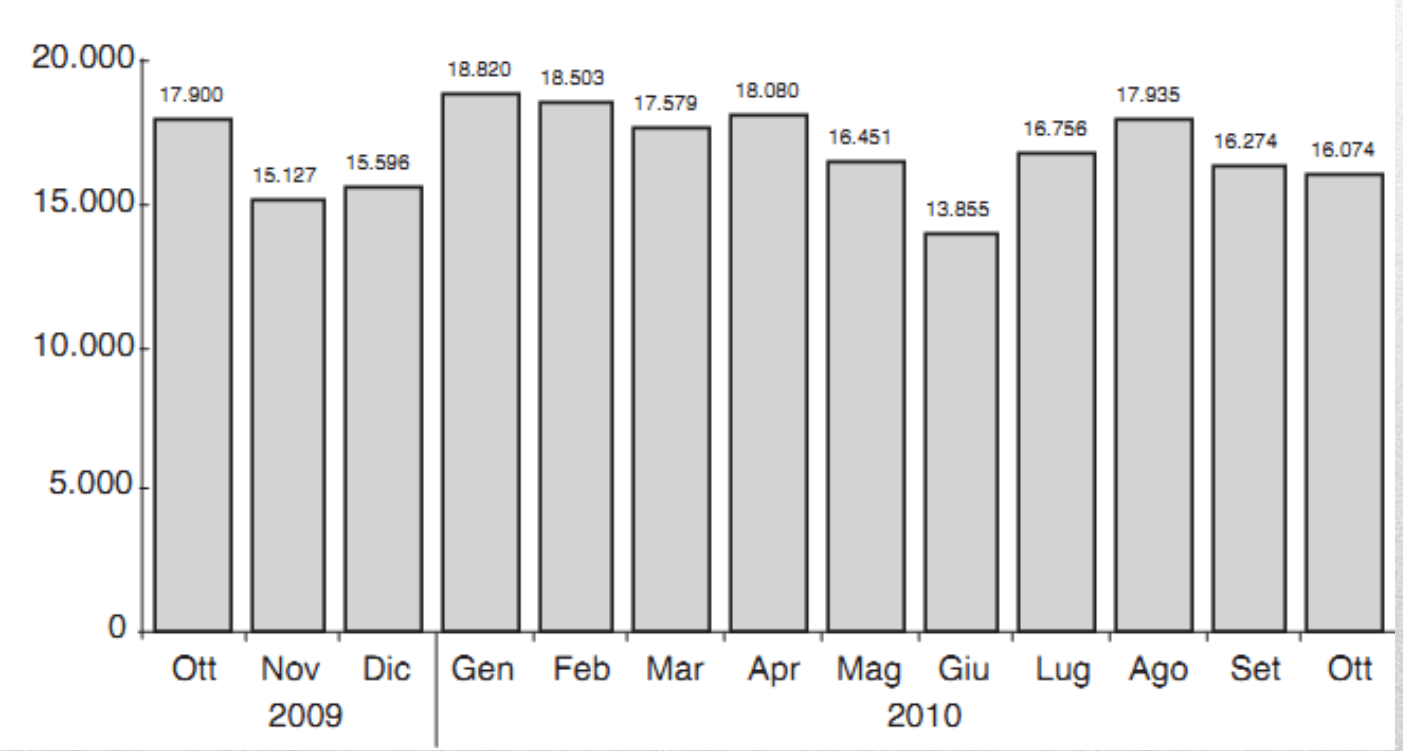
LA CRESCITA DEI MALWARE NEL MONDO



DISTRIBUZIONE DELLE BOTNETS (ottobre 2010)



ANDAMENTO CAMPAGNE PHISHING NEL MONDO



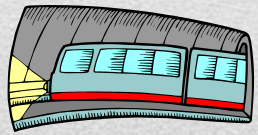
VERSO IL BIG ONE INFORMATICO?

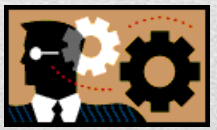
INDAGINE WORLD ECONOMIC FORUM DI GENNAIO 2011

Nei prossimi **10 anni, elevata probabilità** di:

- rischio avaria delle *Infrastrutture Critiche Informatizzate* (con impatti a catena su sistemi di governo, comunicazioni, distribuzione di energia, trasporti)

Costo: 250 miliardi di Euro





- caduta dei sistemi di pagamento e transazioni on line

Costo: 150 miliardi di Euro

IL MERCATO EUROPEO DELLA SICUREZZA SUI NETWORK E SUI SISTEMI INFORMATIVI (NIS)

Nel 2010 il mercato NIS vale complessivamente

15,5 miliardi di euro

1. Hardware **1,7 miliardi**
2. Software **6,6 miliardi**
3. Servizi **7,2 miliardi**

L'EUROPA SI MUOVE

Percezione **rischi** e **costi potenziali** ha spinto l'UE ad emanare negli anni una serie di Comunicazioni, Direttive e Decisioni per:

- rafforzare il sistema di *governance* dei sistemi ICT;
- definire un sistema di regole comuni per proteggere le **infrastrutture critiche informatizzate**.

NUOVI OBBLIGHI A CARICO DELLE IMPRESE DI COMUNICAZIONE

- Nel 2009 viene emanata **Direttiva 2009/140/CE** che, **per incrementare la sicurezza e l'integrità delle reti e dei servizi di comunicazione**
- Alle imprese di comunicazione si impone **di adottare idonee misure di sicurezza nella gestione dei rischi. Alle autorità di controllo viene assegnata la facoltà di impartire istruzioni vincolanti per valutare la sicurezza e l'integrità dei servizi e delle reti.**
- Le imprese **devono sottostare a verifiche** (a loro carico) sulla sicurezza effettuate da un organismo qualificato **indipendente** o dall'autorità nazionale.

ATTENZIONE AL SETTORE ICT

- La **direttiva 114/08/CE** ha individuato nel settore dell'*Information and Communication technology* l'area **infrastrutturale più critica**.
- Un non corretto funzionamento delle *Infrastrutture Critiche Informatizzate* (anche per un periodo limitato) può incidere negativamente sull'**economia** di singoli o gruppi e sulla **sicurezza** di cose e persone.

LE INFRASTRUTTURE CRITICHE INFORMATIZZATE

Il quadro normativo europeo su protezione delle "*infrastrutture critiche informatizzate*" (aggiornato con la Comunicazione n.163/2011 della Commissione al Parlamento Eu, «*Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale"*) *individua*

5 MACRO OBIETTIVI

5 MACRO OBIETTIVI EU

1. Preparazione e prevenzione attacchi
2. Individuazione e risposta
3. Mitigazione e recupero
4. Cooperazione internazionale
5. Definizione criteri per individuare infrastrutture critiche

1.PREPARAZIONE E PREVENZIONE

- Ogni Stato membro deve istituire un CERT (COMPUTER EMERGENCY RESPONSE TEAM) di cui si è definito **una base minima di capacità, servizi e "requisiti essenziali"**.
- I CERT nazionali sono **elementi-chiave** delle capacità nazionali in termini di preparazione, scambio di informazioni, coordinamento e reazione agli attacchi informatici.
- Ad oggi, 20 Stati membri hanno istituito il CERT ma entro la fine del 2011 ogni Stato membro dovrà disporre di un CERT operativo. **Ad oggi il Cert italiano sembra non essere completamente operativo.**

2. INDIVIDUAZIONE E RISPOSTA

E’ prevista la creazione di un Sistema europeo di condivisione delle informazioni e di allarme (EISAS). Durante il 2011 l’ENISA (*European Network and Information Security Agency*) assisterà gli Stati membri nel creare il sistema nazionale di condivisione delle informazioni e di allarme (ISAS). Nel 2012 sarà, invece, la volta dell’integrazione di tutti i sistemi ISAS nazionali nell’EISAS.

3.MITIGAZIONE E RECUPERO

- Sono previsti "*Piani di emergenza ed esercitazioni nazionali*".
- Alla prima esercitazione paneuropea «Cyber Security Exercise» hanno partecipato attivamente 22 Stati europei (tra i quali l'Italia) più 8 osservatori.
- **Entro il 2012 tutti gli Stati membri dovranno avere un piano di emergenza nazionale e predisporre esercitazioni periodiche di reazione e ripristino**.

ITALIA:POCHE IDEE MA CONFUSE

- Norme nate per effetto dell'impulso europeo in materia.
- **Strategie** differenti per la sicurezza: dalla Pa Digitale alle Infrastrutture Critiche, dai Crimini informatici alla sicurezza delle Ict del sistema finanziario, sino alla protezione dei dati personali.
- **Sostanziale difficoltà dei decisori a seguire un disegno strategico complessivo e unitario, con l'effetto di aver prodotto una ridondanza di strutture e soggetti non sempre coordinati tra loro.**

IL RITARDO ITALIANO NELLA «SOCIETA' DIGITALE»

- **59,0%** delle famiglie italiane ha accesso a Internet (**70,1%** in Europa)
- **48,9%** delle famiglie italiane ha accesso a «banda larga» (**60,8%** in Europa)
- **17,6%** degli italiani usa home-banking (**36,0%** in Europa)
- **17,4%** dei cittadini usa servizi di E-goverment (**31,7%** in Europa)
- **14,7%** degli italiani acquista on line (**40,4%** in Europa)
- **3,8%** delle imprese italiane vende prodotti on-line (**13,4%** in Europa);

LOTTA AI CRIMINI INFORMATICI IN ITALIA

- Su scia attentati terroristici, Parlamento vota la legge 155/2005 *"misure urgenti per il contrasto del terrorismo internazionale"* per miglior coordinamento tra i diversi organi di sicurezza.
- Nel provvedimento, all'articolo 7-*bis* (sicurezza telematica), si definisce, **per la prima volta**, un quadro normativo per la protezione delle «*infrastrutture critiche nazionali*» dagli attacchi informatici.

INFRASTRUTTURE CRITICHE INFORMATIZZATE

- Con il Decreto del Ministro dell'Interno del 9 gennaio 2008 il nostro paese, anticipando la direttiva europea, ha provveduto ad individuare, solo in via generale, **infrastrutture critiche informatizzate** di interesse nazionale (tra l'altro: sistemi ed i servizi informatici di supporto ai Ministeri, le infrastrutture di *utility* pubbliche che operano su aree metropolitane non inferiori a 500.000 abitanti, i sistemi It della Banca d'Italia).

- Questa disposizione, come è stato fatto osservare da alcuni interlocutori istituzionali, *ha risentito di una quadro complessivo di "incompletezza normativa" non esistendo all'epoca della sua emanazione una disciplina specifica proprio per l'individuazione e designazione delle Infrastrutture Critiche Nazionali (ICN).*

PUBBLICA AMMINISTRAZIONE

- La sicurezza in ambito PA digitale è governata dal *Codice della Amministrazione Digitale* (CAD) recentemente aggiornato (D.Lgs. 30 dicembre 2010, n. 235)
- Nello specifico, è previsto (art.12) - tra l'altro - che *"**Le pubbliche amministrazioni adottano le tecnologie dell'informazione e della comunicazione nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati, con misure informatiche, tecnologiche, e procedurali di sicurezza**, secondo le regole tecniche di cui all'articolo 71"*
- E' inoltre previsto che **le regole tecniche (art. 71) individueranno "*le modalità che garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture* "** (art.51).

ART. 71 REGOLE TECNICHE

1. ***Le regole tecniche previste nel presente codice sono dettate, con decreti del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione, di concerto con i Ministri competenti, sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, ed il Garante per la protezione dei dati personali nelle materie di competenza, previa acquisizione obbligatoria del parere tecnico di DigitPA.***

- **LE REGOLE TECNICHE NON SONO STATE ANCORA ADOTTATE**

PROGETTO ITALIA SICUR@

- Il progetto *Italia Sicur@* ha l'obiettivo di realizzare un programma di formazione, per *specializzare gli ingegneri sulle tematiche di sicurezza.*
- Sono coinvolti CNI, Fondazione Ugo Bordoni, DigitPA.

Obiettivi:

- facilitare uso di nuove tecnologie;
- accrescere consapevolezza per misure di sicurezza ICT;
- acquisire elementi conoscitivi per **la messa punto regole sicurezza (art. 71 del CAD)**.

IL VALORE DEL MERCATO PUBBLICO ICT

Secondo l'ultima relazione dell'AVCP il **valore** dei contratti aggiudicati nel 2010 relativamente ai **servizi informatici (consulenza, sviluppo di software, Internet e supporto) è pari a**

2,41 miliardi di euro.

(il valore dei contratti aggiudicati per **servizi architettonici, di costruzione, ingegneria e ispezione** è pari a **349 milioni di euro**).

Codice dei Contratti pubblici

Il D.Lgs. 163/2006 è **privo** di norme specifiche che regolino:

- contenuti e validazione progettazione
- collaudo

dei servizi e dei sistemi di informazione.

Nuovo Regolamento (DPR 207/2010)

Dispone (art. 279) una prima, **generica e insufficiente**, definizione dei contenuti della progettazione (di regola in un unico livello) per tutti i servizi e le forniture:

- relazione tecnica-illustrativa;
- indicazioni e disposizioni per i documenti inerenti la sicurezza;
- calcolo della spesa per l'acquisizione del bene o del servizio;
- prospetto economico degli oneri complessivi necessari per l'acquisizione del bene o del servizio;
- capitolato speciale descrittivo e prestazionale;
- schema di contratto.

Nuovo Regolamento (DPR 207/2010)

- Di norma la progettazione «è predisposta dalle amministrazioni aggiudicatrici mediante **propri dipendenti in servizio**» (art. 279, comma 2).
- **Possono essere posti a gara solo** i contratti aventi ad oggetto «prestazioni particolarmente complesse (..), richiedono l'apporto di una pluralità di competenze (..), caratterizzate dall'utilizzo di componenti (..) innovativi o dalla necessità di elevate prestazioni (..)» (art. 300, comma 2, lett. b).
- La stazione appaltante **può stabilire di sottoporre a verifica** il progetto.
- Non collaudo ma «**verifica di conformità**» del servizio fornito (art. 312 e ss).

UNA NUOVA CULTURA NELL'ICT…

- I contenuti della **progettazione**
- Le procedure di **verifica** del progetto
- Le attività di **collaudo**

devono raggiungere

per i **servizi e le infrastrutture ICT** lo **stesso standard** (per complessità e terzietà) richiesto per le **opere ed i lavori pubblici.**

…PER LO SVILUPPO DI NUOVE FIGURE PROFESSIONALI ED IMPRENDITORIALI

Il mercato pubblico dell'ICT può diventare il **volano** per lo sviluppo di nuove **realtà imprenditoriali e professionali** attive nella predisposizione di **servizi connessi alla sicurezza delle reti e infrastrutture ICT** di potrà giovarsi anche il **sistema delle PMI** che non ha ancora sviluppato una **adeguata domanda di sicurezza**.