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

Roma, 1 luglio 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

4

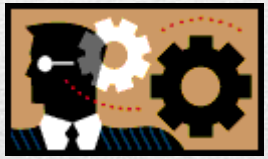
IL BIG ONE INFORMATICO?

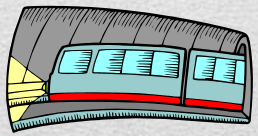
INDAGINE WORLD ECONOMIC FORUM DI GENNAIO 2011

Secondo i decisori intervistati, nei prossimi **10 anni,** probabilità 20%, di

rischio avaria, con impatti a catena su:

- sistemi di governo ;
- comunicazioni;
- distribuzione di energia;
- trasporti.





Costo: 250 miliardi di Euro

Possibile caduta **dei sistemi di pagamento e transazioni on line** che porterebbe a crescita di frodi on line e **perdita di fiducia** .

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**

ESISTE UN PROBLEMA SICUREZZA NELL'ICT

L'EUROPA SI MUOVE

Percezione **rischi** e **costi potenziali** ha spinto l'EU a definire negli anni una serie di norme per:

- rafforzare il sistema di *governance* dei sistemi ICT;
- definire negli Stati membri un sistema di regole comuni per proteggere:

a) **infrastrutture critiche** (produzione e trasporto di energia; telecomunicazioni; circuiti finanziari; sistema sanitario; trasporto, distribuzione e trattamento acque; servizi di emergenza; filiera alimentare);

b) **infrastrutture critiche informatizzate**.

NUOVI OBBLIGHI A CARICO DELLE IMPRESE DI COMUNICAZIONE

- Nel 2009 viene emanata **Direttiva 140** che, **per incrementare la sicurezza e l'integrità delle reti e dei servizi di comunicazione**, modifica la Direttiva quadro 2002/21/Ce, introducendo due nuovi articoli (13 bis e 13 ter).
- Alle imprese di comunicazione si impone **di adottare idonee misure di sicurezza nella gestione dei rischi e si rafforzano i poteri delle autorità di controllo, introducendo la facoltà di impartire istruzioni vincolanti alle imprese per valutare la sicurezza e l'integrità dei loro servizi e delle loro 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 della *Information and Communication technology* l'area **infrastrutturale più critica**.
- Nell'ambito delle infrastrutture critiche si parla, da alcuni anni anche di ***Critical Information Infrastructure (CII).***
- Un loro non corretto funzionamento (anche per un periodo limitato) potrebbe incidere negativamente sull'economia di singoli o gruppi, **mettendo a rischio economia ma anche sicurezza di cose e persone**.

LE INFRASTRUTTURE CRITICHE INFORMATIZZATE

Il quadro normativo europeo su protezione delle "*infrastrutture critiche informatizzate*" aggiornato con

- Comunicazione n.163/2011 della Commissione al Parlamento Eu, «*Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale",* dove si fa il punto della situazione alla luce della precedente direttiva n. 149/2009 dove si definiva un piano d'azione (CIIP) sviluppato su

5 MACRO OBIETTIVI

5 MACRO OBIETTIVI EU

1. Preparazione e prevenzione attacchi;
2. Individuazione e risposta;
3. Mitigazione e recupero;
4. Cooperazione internazionale;
5. Criteri per individuare infrastrutture critiche nel settore delle TIC

1.PREPARAZIONE E PREVENZIONE

- Si è definito **una base minima di capacità, servizi e "requisiti essenziali"** che le CERT (COMPUTER EMERGENCY RESPONSE TEAM) nazionali devono possedere.
- Le 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.**
- Nel 2009 ha visto la luce anche il Forum europeo degli Stati membri (EFMS) per favorire gli scambi tra autorità pubbliche delle "buone pratiche" in materia di:

a) criteri per l'individuazione delle infrastrutture TIC (ICT) europee;

b) priorità, principi e orientamenti europei per la resilienza e la stabilità di internet.

2. INDIVIDUAZIONE E RISPOSTA

- Verrà creato un Sistema europeo di condivisione delle informazioni e di allarme (EISAS). Durante il 2011 l'ENISA 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*" quale strumento da sviluppare.
- 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**.

4.COOPERAZIONE INTERNAZIONALE

- Sono stati elaborati **principi e orientamenti** europei per la **resilienza** e la **stabilità** di internet.

5. CRITERI PER LE INFRASTRUTTURE CRITICHE NEL SETTORE DELLE ICT

- Dovranno essere definiti *criteri settoriali per l'individuazione delle infrastrutture critiche europee nel settore delle ICT* e come le discussioni tecniche abbiano già portato ad una prima versione di questi criteri per le comunicazioni (fisse e mobili) e internet.

ITALIA:POCHE IDEE MA CONFUSE

- Norme nate per effetto dell'impulso europeo in materia.
- **Strategie** differenti per la sicurezza, non sempre coordinate tra loro: dalla Pa Digitale, alle Infrastrutture Critiche, dai Crimini informatici alla sicurezza delle Ict del sistema finanziario, sino alla protezione dei dati personali.
- **Ma 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.**

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 (GURI n. 101 del 30 aprile 2008) il nostro paese, anticipando la direttiva europea, ha provveduto ad individuare le **infrastrutture critiche informatizzate** di interesse nazionale, annoverando tra di esse i sistemi ed i servizi informatici di supporto alle funzioni istituzionali di Ministeri, agenzie ed enti da essi vigilati, operanti nei settori dei rapporti internazionali, della sicurezza, della giustizia, della difesa, della finanza, delle comunicazioni, dei trasporti, dell'energia, dell'ambiente, della salute, nonché le infrastrutture di *utility* pubbliche che operano su aree metropolitane non inferiori a 500.000 abitanti (comunicazioni, dei trasporti, dell'energia, della salute e delle acque) e infine i sistemi It della Banca d'Italia.

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

SISTEMA FINANZIARIO NAZIONALE

- Nel 2004 Banca d'Italia ha emanato Normativa di Vigilanza "*Continuità operativa in casi di emergenza"*, che impone alle 800 banche italiane di dotarsi di un Piano di Continuità Operativa (*Business Continuity Plan).*
- Come previsto dalla Banca Centrale Europea, nel 2007 la Banca d'Italia ha emanato le disposizioni per la continuità operativa degli operatori finanziari in caso di attacco informatico.

PUBBLICA AMMINISTRAZIONE

- La sicurezza in ambito PA digitale è governata dal *Codice della Amministrazione Digitale* (CAD). Il Cad è stato **aggiornato** con decreto legislativo del 30 dicembre 2010, n. 235 ("Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82 - Codice dell'Amministrazione Digitale)
- Gli **aspetti di sicurezza sono stati ribaditi** nella consapevolezza del ruolo trasversale che la materia riveste lungo tutto l'articolato del Codice.
- 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.***

- 1-ter. Le regole tecniche di cui al presente codice sono dettate in conformità alle discipline risultanti dal processo di standardizzazione tecnologica a livello internazionale ed alle normative dell'Unione europea.
- 2. Le regole tecniche vigenti nelle materie del presente codice restano in vigore fino all'adozione delle regole tecniche adottate ai sensi del presente articolo.
- **LE REGOLE TECNICHE NON SONO STATE ANCORA ADOTTATE**

IL VALORE DEL MERCATO PUBBLICO ICT

Secondo la relazione 2010 dell'AVCP (Autorità vigilanza sui contratti pubblici di lavori, servizi, forniture) 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.

- Ad essi vanno aggiunti **77 milioni di euro** per pacchetti software e sistemi di informazione.
- Vale, invece, **349 milioni di euro** quella relativa ai **servizi architettonici, di costruzione, ingegneria e ispezione**.

Codice dei Contratti pubblici

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

- contenuti progettazione
- validazione progettazione
- collaudo

dei servizi e dei sistemi di informazione.

Nuovo Regolamento (DPR 207/2010)

Prima, **generica e insufficiente**, definizione dei contenuti della progettazione per servizi e forniture, articolata di regola in un unico livello contenente:

- la relazione tecnica-illustrativa con riferimento al contesto in cui è inserita la fornitura o il servizio;
- le indicazioni e disposizioni per la stesura dei documenti inerenti la sicurezza;
- il calcolo della spesa per l'acquisizione del bene o del servizio con indicazione degli oneri della sicurezza non soggetti a ribasso;
- il prospetto economico degli oneri complessivi necessari per l'acquisizione del bene o del servizio;
- il capitolato speciale descrittivo e prestazionale;
- lo 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 sotto il profilo tecnologico ovvero che richiedono l'apporto di una pluralità di competenze ovvero caratterizzate dall'utilizzo di componenti o di processi produttivi innovativi o dalla necessità di elevate prestazioni per quanto riguarda la loro funzionalità» (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).

PROGETTO ITALIA SICUR@

- Il progetto *Italia Sicur@* ha l'obiettivo di realizzare un programma di formazione, per *specializzare gli ingegneri CNI sulle tematiche di sicurezza*.
- CNI, Fondazione Ugo Bordoni, DigitPA.
- Indirizzato a realtà meno "aggiornate" a livello tecnologico.

Obiettivi:

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