ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

La Sicurezza Nelle Infrastrutture Critiche

Angelo Gallippi – Privacy & ICT Manager
Unione Nazionale Consumatori

INDICE DELLA PRESENTAZIONE :

QUATTRO DOMANDE

1. *Cos'è una IC?*
2. *Quali sono le IC?*
3. *Quali sono i soggetti interessati alle IC?*
4. *Cosa minaccia le IC?*

1.

"un elemento, un sistema o parte di questo … che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini, e il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni"

(*Direttiva europea 2008/114/CE, art. 2*)

2. Quali sono le IC?

- **Energia** elettrica, gas, petrolio (produzione, trasmissione, distribuzione)
- **Trasporti** merci e passeggeri (aerei, navali, ferroviari, stradali)
- Telecomunicazioni e telematica
- Risorse idriche e gestione delle acque reflue
- Sanità, ospedali e reti di servizi e interconnessione
- Ordine pubblico, Difesa e Pubblica amministrazione
- Reti a supporto del governo, centrale e territoriale, e per la gestione delle emergenze (Protezione civile)
- Banche e servizi finanziari
- Agricoltura, produzione e distribuzione delle derrate alimentari

3. Quali sono i soggetti interessati alle IC?

Data la loro ampia tipologia, alla protezione delle nostre IC è interessata una pluralità di soggetti istituzionali. I principali sono:

settore energetico

Enel, Eni, Snam Rete Gas, Terna

settore dei trasporti

Anas, Autostrade per l'Italia, Enac, Enav, Ferrovie dello Stato (Trenitalia e Rfi), Sea-Aeroporti

ministeri

Interno, Infrastrutture e trasporti, Difesa, Lavoro e Salute; Sviluppo economico *

- Dipartimento Protezione Civile
- Banca d'Italia
- Centro Nazionale Anticrimine Informatico per la Protezione delle IC
- Agenzia Spaziale Italiana

---

* il Dipartimento Comunicazioni coordina e supervisiona la sicurezza delle reti e dell'informazione

4. Cosa minaccia le IC?

cause

- **naturali** (alluvioni, terremoti, eruzioni vulcaniche)
- **umane**
  - volontarie (guerra, terrorismo, *cybercrime*, vandalismi, sabotaggi, scioperi)
  - involontarie (errori, omissioni)
- **guasti tecnici**

Si tratta di pericoli reali per lo sviluppo e il benessere sociale di un Paese, che sembrano essere accresciuti dalla estremizzazione dei fenomeni climatici e dalla tormentata situazione socio-politica mondiale.

Pertanto molti governi hanno messo a punto studi e progettato misure precauzionali per ridurre il rischio che le IC vengano a mancare in caso di guerra, disastri naturali, scioperi, vandalismi o sabotaggi. Tale attività viene definita

Protezione delle IC - *Critical Infrastructure Protection* (CIP).

Attualmente i processi alla base dei servizi e dei beni prodotti dalle IC sono gestiti attraverso risorse informatiche; pertanto in questi casi si parla di IC Informatizzate e, di conseguenza, di

Protezione delle IC Informatizzate

Critical Information Infrastructure Protection (CIIP),

ed è a queste che si riferiscono le principali raccomandazioni delle istituzioni comunitarie.

LA SITUAZIONE NEGLI STATI UNITI

Gli Stati Uniti hanno cominciato a studiare la protezione delle IC nel 1996. Ma sono stati i tragici eventi dell'11 settembre 2001 ad avere accresciuto l'interesse per la tematica, che è stata portata ai primissimi posti nell'agenda governativa con:

- l'istituzione del *Department of Homeland Security* (2002)
- l'emanazione del *National Infrastructure Protection Plan* (2006)

L'esempio degli Stati Uniti è stato seguito da altri Paesi fra cui: Gran Bretagna, Germania, Svezia, Canada e Olanda, che hanno elaborato specifiche azioni coerenti con le diverse realtà territoriali e infrastrutturali.

LA SITUAZIONE IN EUROPA

L'Ue è fortemente impegnata a migliorare la protezione delle IC sul proprio territorio, promuovendo a livello scientifico e tecnologico attività di ricerca, mentre a livello normativo e regolamentare ha inquadrato la sua strategia 2007-2013 nel

Programma europeo di protezione delle IC

European Program on Critical Infrastructure Protection (EPCIC)

Ecco una breve cronistoria delle iniziative al riguardo.

2004

giugno

Il Consiglio europeo chiede alla Commissione di elaborare una strategia globale per la protezione delle IC.

ottobre

La Commissione risponde adottando la comunicazione

La protezione delle IC nella lotta contro il terrorismo

2005

settembre

Viene adottata una prima decisione relativa al finanziamento di un progetto pilota che prevede azioni preparatorie destinate a rafforzare la lotta al terrorismo. Tale decisione sarà seguita il 26 ottobre 2006 da una seconda decisione per il finanziamento del progetto pilota relativo al Piano.

novembre

La Commissione adotta un **Libro Verde** relativo a un EPCIP.

dicembre

Il Consiglio “Giustizia e Affari Interni” chiede alla Commissione di presentare una proposta di EPCIP.

2006

dicembre

La Commissione

- adotta una Comunicazione relativa a un EPCIP;
- presenta una proposta di direttiva relativa all'individuazione e alla designazione delle IC europee con l'obiettivo di potenziar-ne la protezione.

dicembre

Il Consiglio europeo accetta il progetto della Commissione per la proposta di un EPCIP. Nel suo ambito è delineata anche una

Rete informativa di allarme sulle IC europee

Critical Infrastructure Warning Information Network (CIWIN)

che veicoli la condivisione rapida e ottimizzata di informazioni tra le autorità dei diversi Stati membri. CIWIN sarà proposta nell'ottobre 2008 e approvata dal Parlamento nell'aprile 2009.

2007

febbraio

Viene adottato il programma specifico

Prevenzione, preparazione e gestione delle conseguenze in materia di terrorismo e di altri rischi correlati alla sicurezza

2008

dicembre

Il Consiglio dell'Ue emana la

Direttiva 2008/114/CE

relativa all'individuazione e alla designazione delle IC europee e alla valutazione della necessità di migliorarne la protezione.

Essa è focalizzata soltanto sulle infrastrutture dei settori dell'energia e trasporti.

In base alla direttiva, ogni azienda "critica" deve dotarsi di:

- un **responsabile della sicurezza unico**, che funga da punto di contatto per tutte le problematiche di sicurezza;
- un **Piano della sicurezza dell'operatore**, che contenga una dettagliata analisi delle diverse minacce, vulnerabilità e, soprattutto, delle varie contromisure da adottare in funzione delle specifiche situazioni di rischio.

Il Piano dovrà poi essere validato e approvato dalle autorità pubbliche.

LA SITUAZIONE IN ITALIA

Dopo una discussione iniziata in Senato a gennaio scorso — quindi a oltre due anni dall'emanazione della direttiva — anche l'Italia ha recepito la direttiva, con il decreto legislativo di attuazione pubblicato sulla Gazzetta Ufficiale del

5 maggio 2011.

Le nuove norme hanno l'obiettivo di potenziare la sicurezza delle grandi infrastrutture energetiche e dei trasporti del Paese nei confronti di azioni terroristiche o criminali, e aumentarne la robustezza rispetto a guasti accidentali ed eventi naturali.

Comunque il **13 maggio** scorso (ossia otto giorni dopo l'entrata in vigore della direttiva in Italia), è stata convocata una conferenza della Commissione europea (DG Home) per avviare una revisione della direttiva stessa, che quasi sicuramente porterà a includere le infrastrutture Ict tra le quelle critiche europee, in aggiunta alle attuali energetiche e dei trasporti.

RECENTI CRASH DELLE IC

La necessità di includere le infrastrutture Ict tra le IC è dimostrata dal fatto che non passa giorno, si può dire, senza la notizia di un ciber-attacco volto a mettere fuori uso un sistema informativo o a rubare le informazioni degli utenti.

Le vittime più recenti dei pirati informatici sono stati i siti di servizi d'intrattenimento, di importanti banche e di istituzioni pubbliche.

Ecco una scelta dei casi più significativi.

inizio maggio

Citigroup, la più grande azienda al mondo di servizi finanziari, conferma che i suoi server di Citi Account Online sono stati violati e gli hacker potrebbero avere trafugato le informazioni di centinaia di migliaia di utenti della banca.

L'attacco ai server, nei quali sono stipati dati quali nomi, numeri di conto e indirizzi *email*, avrebbe riguardato l'1% dei 21 milioni di clienti statunitensi possessori di una carta di credito.

Altre informazioni, quali date di nascita, numeri di previdenza sociale e codici di sicurezza delle carte non sarebbero stati compromessi, perché custoditi in un altro luogo.

fine maggio

Google rende noto di avere sventato un tentativo di furto delle password di centinaia di account di posta elettronica Gmail, tra cui quelle di funzionari del governo americano, alti responsabili politici americani e di Paesi asiatici tra i quali la Corea del Sud, giornalisti, militari e attivisti del dissenso cinese per i diritti umani.

Secondo la società, gli attacchi sembrano provenire dalla cittadina cinese di Jinan, sede di un'accademia dove vengono reclutati dall'esercito giovani talenti del software, la *Lanxiang vocational school*.

Già un anno fa l'istituto cinese era finito al centro dei sospetti come fonte di un'altra offensiva diretta contro decine di aziende hi-tech negli Stati Uniti, l'Operazione Aurora. E in seguito Google aveva spostato il suo motore di ricerca da Pechino a Hong Kong, dove le restrizioni della censura sono minori.

Secondo gli esperti, l'attacco a Gmail non sembra avere utilizzato tecniche molto sofisticate, ma è notevole per il livello di accuratezza del tono e del linguaggio utilizzati per tentare di trarre in inganno alti ufficiali del governo. Gli hacker, infatti, hanno utilizzato la tecnica dello *spear phishing*, la medesima impiegata per i furti dai conti correnti online, che consiste nell'inviare agli obiettivi identificati messaggi personalizzati che sembrano completamente legittimi al fine di carpire la password.

Dear iup Owner,

We are currently upgrading our data base and e-mail center. We are deleting all iup email account to create more space for new accounts. To prevent your account from closing you will have to update it below so that we will know that it's a present used account.

CONFIRM YOUR EMAIL IDENTITY BELOW
E-mail Username : ....
E-mail Password : .....

This message is from iup messaging center

Thank you for using iup!
Warning Code:VX2G99AAJ

Thanks,
iup Team
https://webmail.iup.Edu/

Una volta entrati nella casella di email, gli hacker modificano le impostazioni per ottenere una copia dei documenti inviati, che in tal modo arrivano senza sforzi nelle loro mani. Infatti chi è caduto nella trappola, ogni volta che spedisce una comunicazione a un suo contatto include tra i destinatari, in modo inconsapevole, anche i pirati informatici.

A differenza del *phishing* tradizionale, che sottrae informazioni da singoli utenti, le frodi di *spear phishing* hanno come obiettivo quello di penetrare all'interno dell'intero sistema informatico di una società.

Tuttavia Google ha comunicato che la campagna di “furto mirato” ha colpito singoli utenti, ma non era indirizzata alle sue infrastrutture, come invece era accaduto un anno fa.

1-7 giugno

Blackout del sistema informativo di **Poste italiane**, non ancora del tutto risolto il 10 giugno. Non è un attacco hacker, ma dimostra la scarsa attenzione per la sicurezza da parte di uno dei principali gruppi bancari italiani.

13 giugno

Finisce nel mirino degli hacker il sistema informativo del **Fondo Monetario Internazionale**. Un portavoce dell'FMI parla di "un attacco cibernetico significativo" e "su larga scala". La violazione sarebbe andata avanti da mesi e, secondo gli analisti, sarebbe opera di un governo straniero. L'FMI ha accesso a dati e informazioni sensibili di 187 nazioni del mondo. Non si conosce ancora l'entità dei danni, che potrebbero essere piuttosto estesi.

15 giugno

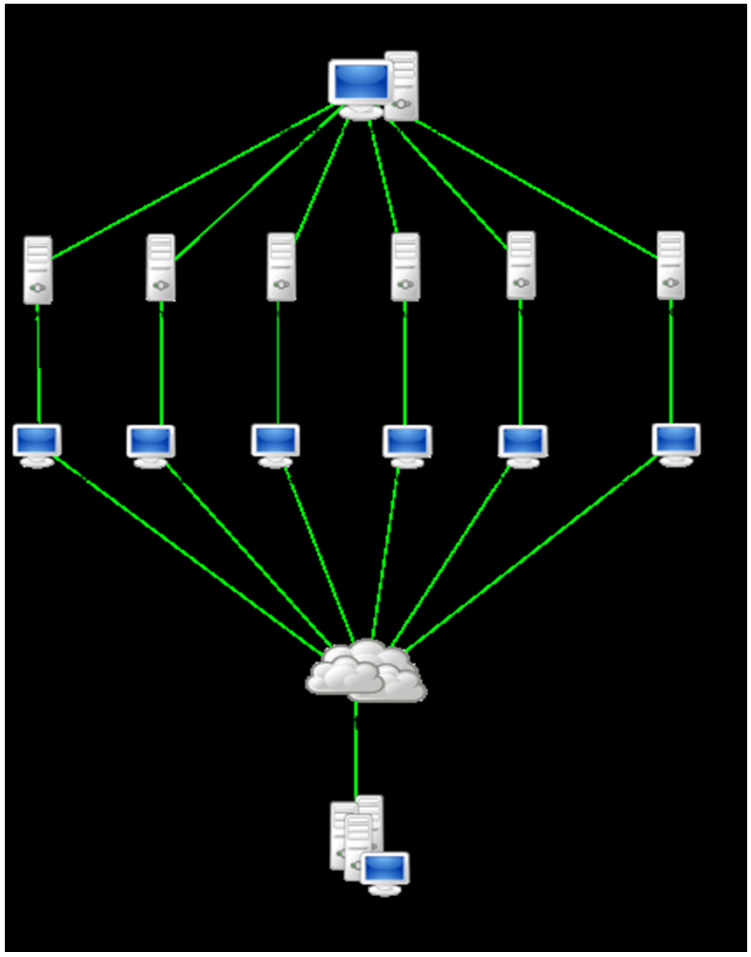
Gli hacker colpiscono il sito Web della **Cia**, l'agenzia di spionaggio per l'estero degli Usa. La tecnica utilizzata è quella del *Denial of Service* (negazione di servizio), che inonda di richieste un server fino a mandarlo in tilt. Il sito sarebbe diventato inaccessibile dalle città di Londra, New York, San Francisco e Bangalore.

L'attacco è stato rivendicato da Lulz Security, una sigla salita agli onori della cronaca negli ultimi mesi per gli attacchi a **Sony**, **Nintendo**, varie emittenti Usa e il sito del **Senato Usa**.

I responsabili alla sicurezza dell'agenzia minimizzano l'accaduto, dichiarando che questi hacker vogliono solo che i riflettori vengano puntati su di loro.

Ricordo che questo tipo di attacco utilizza in genere molti pc inconsapevoli, detti *zombie*, sui quali in precedenza è stato inoculato un programma appositamente creato per attacchi DoS, e che si attiva ad un comando del cracker creatore.

Se il programma maligno si è diffuso su molti computer, può succedere che migliaia di pc violati da un cracker, ovvero una *botnet*, producano inconsapevolmente e nello stesso istante un flusso di dati che travolgono come una valanga anche i link più capienti del sito bersaglio.



CONCLUSIONI

Elementi positivi

- L'attenzione globale verso i problemi della sicurezza informatica è in aumento, come dimostrano i dati dell'ultimo studio di Gartner sul mercato mondiale del software per la sicurezza dei sistemi It.

  Tale mercato valeva 16,5 miliardi di dollari nel 2010, con un incremento del 12% rispetto ai 14,7 miliardi fatturati nel 2009, quando si ebbe un netto declino delle performance causato dalla crisi economica e dai tagli ai budget It.

  Alcuni produttori hanno registrato una crescita addirittura a due cifre, e gli altri un buon recupero.

- Come accennato, il perimetro di definizione delle IC è in corso di ampliamento a livello europeo, ed è auspicabile che la sua estensione, almeno alle reti di Tlc, avvenga in tempi brevi.

  In tal modo la direttiva 2008/114/CE si applicherà anche ad esse, con un sicuro innalzamento del livello di sicurezza in molti settori vitali della società.

- Infine, l'Ue ha stabilito che per la fine del 2012 i 27 Stati membri e le istituzioni Ue dovranno avere:
  - attivato i **Computer Emergency Response Teams** (CERT);
  - sviluppato un primo **piano di emergenza** in ambito di *cyber-security*;
  - promosso l'adozione di principi condivisi per assicurare la stabilità di Internet, anche per il **cloud computing**;
  - approfondito le **partnership** strategiche.

- In Italia sono sviluppate da tempo una cultura e un'attenzione - tecnica, scientifica e accademica - qualificate per il tema della vulnerabilità delle IC e per gestire al meglio le conseguenze della crescente interconnessione sulla vita del Sistema Paese.

  Anche le relazioni annuali del **Sistema di Informazione per la Sicurezza della Repubblica** dedicano un'attenzione che è cresciuta negli anni alla *cyber security*, considerata marginale fino a qualche anno fa e nel 2010 inserita invece tra le "sfide crescenti".

  Sono anche attive diverse organizzazioni finalizzate a costruire e sostenere una cultura interdisciplinare per lo sviluppo di strategie, metodologie e tecnologie in grado di gestire correttamente le IC, tra le quali mi limito a citare l'Associazione Italiana Esperti Infrastrutture Critiche, senza fine di lucro.

Bibliografia e sitografia :

Wil A. H. Thissen, Paulien Minke Herder, *Critical infrastructures: state of the art in research and application*, Springer, 2003, 304 pp.

Per una panoramica a 360° sulle IC in generale:
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, *La sicurezza delle reti nelle infrastrutture critiche*, Roma, 2005, in: www.isticom.it/documenti/news/pub_003_ita.pdf

Per una definizione delle IC in ambito Usa:
Critical Infrastructures: What Makes an Infrastructure Critical? (Report for Congress), 2003, in: *www.fas.org/irp/crs/RL31556.pdf*

Il testo della direttiva 2008/114/CE si trova in:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF