Rapporto

2013

sulla sicurezza ICT

in Italia

Presentazione al Security Summit

Tavola Rotonda del 12.03.2013

Modera: Gigi Tagliapietra, Presidente Clusit

Partecipano:

- Paolo Giudice, Segretario Generale Clusit
- Giovanni Todaro, IBM Security Systems Leaderl
- Alessandro Vallega, Oracle Security Business Development Manager e Responsabile di Oracle Community for Security
- Andrea Zapparoli Manzoni, CD Clusit

In sala: gli altri autori del rapporto.

Clusit
Associazione Italiana per la Sicurezza Informatica

Rapporto Clusit 2013 sulla sicurezza ICT in Italia

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

I numeri del Rapporto 2012

- **Aziende coinvolte**: oltre 150
- **Autori ed esperti che hanno lavorato al Rapporto**: oltre 100
- **Media**: il Rapporto è stato presentato ad oltre 30 testate, con alcune decine di articoli pubblicati
- **Distribuzione al Security Summit**: il volume cartaceo è stato distribuito ai Summit di Milano, Roma e Verona, per un totale di oltre 1.000 copie
- **Invio ad Istituzioni, Aziende, Giornalisti**: il volume cartaceo è stato spedito a funzionari governativi ed a componenti degli organismi che promuovono l'Agenda Digitale, a funzionari della PA legati al mondo ICT ed ai CIO, CSO e CISO di Grandi Aziende
- **Formato elettronico:** alcune migliaia di copie sono state inviate a chi ne ha fatto richiesta tramite i siti del Clusit e del Security Summit.

Rapporto Clusit 2013 sulla Sicurezza ICT in Italia – 3a edizione

CONTENUTI

- Panoramica degli eventi (cybercrime e incidenti informatici) più significativi del 2012, verificatisi in Italia e nel mondo, con tendenze per il 2013 e +
- Contributo della Polizia Postale e delle Comunicazioni.
- Analisi del mercato italiano della sicurezza ICT e tendenze degli investimenti delle aziende. Analisi e prospettive del mercato del lavoro nel nostro settore.
- Focus on (7): Mobile Security, Social Media Security, Cloud Security, Sicurezza in Sanità, e-Commerce, il protocollo IPv6, Il salvataggio delle informazioni e la continuità di servizio.

Clusit
Associazione Italiana per la Sicurezza Informatica

Presentazione il 12.03.2013 al SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT **di Milano**

PUNTI DI ATTENZIONE

- Ad un anno dal Rapporto 2012, (come avevamo previsto…) ci troviamo oggi di fronte ad una vera e propria emergenza globale nella quale niente e nessuno può più ritenersi al sicuro, in particolare:
  - Tutti sono diventati bersagli (Cittadini, Aziende, VIP, Governi, IC…)
  - Tutte le piattaforme sono attaccate (sempre più SCADA e Mobile)
  - Le protezioni tradizionali sono diventate trasparenti per le minacce
- Nel 2012 gli attacchi sono aumentati del 252%, due ordini di grandezza più delle contromisure. Questa forbice si sta allargando.
- Il tempo delle *chiacchiere* è finito. Siamo arrivati al punto in cui è necessario agire, subito, rapidamente e con grande efficacia.

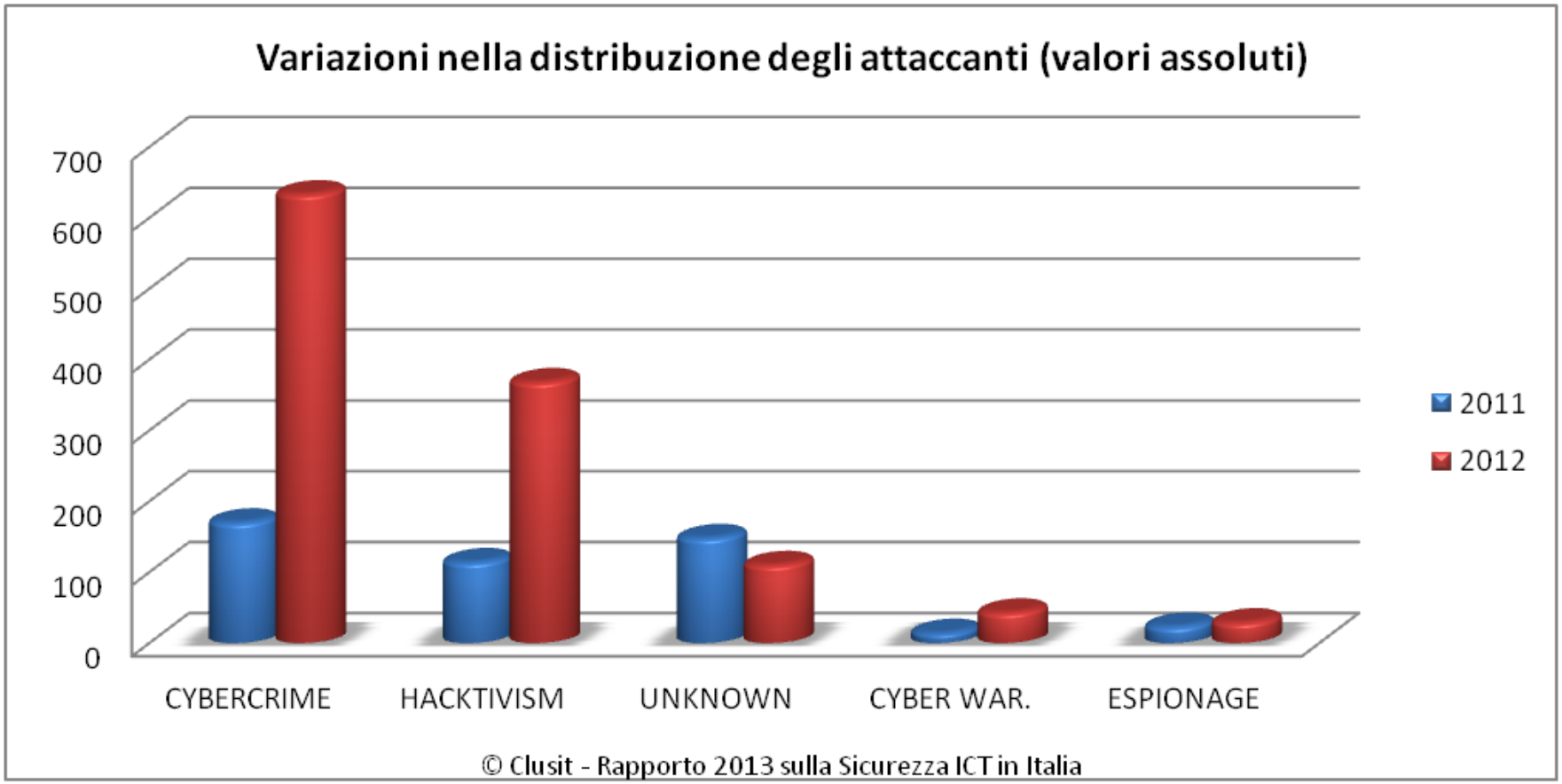
Panoramica cybercrime – Analisi dei principali incidenti a livello internazionale

TREND

VITTIME PER TIPOLOGIA	2011	2012	Totale	Incremento
Institutions: Gov - Mil - LEAs - Intelligence	153	374	527	244,44%
Others	97	194	291	200,00%
Industry: Entertainment / News	76	175	251	230,26%
Industry: Online Services / Cloud	15	136	151	906,67%
Institutions: Research - Education	26	104	130	400,00%
Industry: Banking / Finance	17	59	76	347,06%
Industry: Software / Hardware Vendor	27	59	86	218,52%
Industry: Telco	11	19	30	172,73%
Gov. Contractors / Consulting	18	15	33	-16,67%
Industry: Security Industry:	17	14	31	-17,65%
Religion	0	14	14	1400,00%
Industry: Health	10	11	21	110,00%
Industry: Chemical / Medical	2	9	11	450,00%
TOTALE	**469**	**1.183**	**1.652**	**252,24**

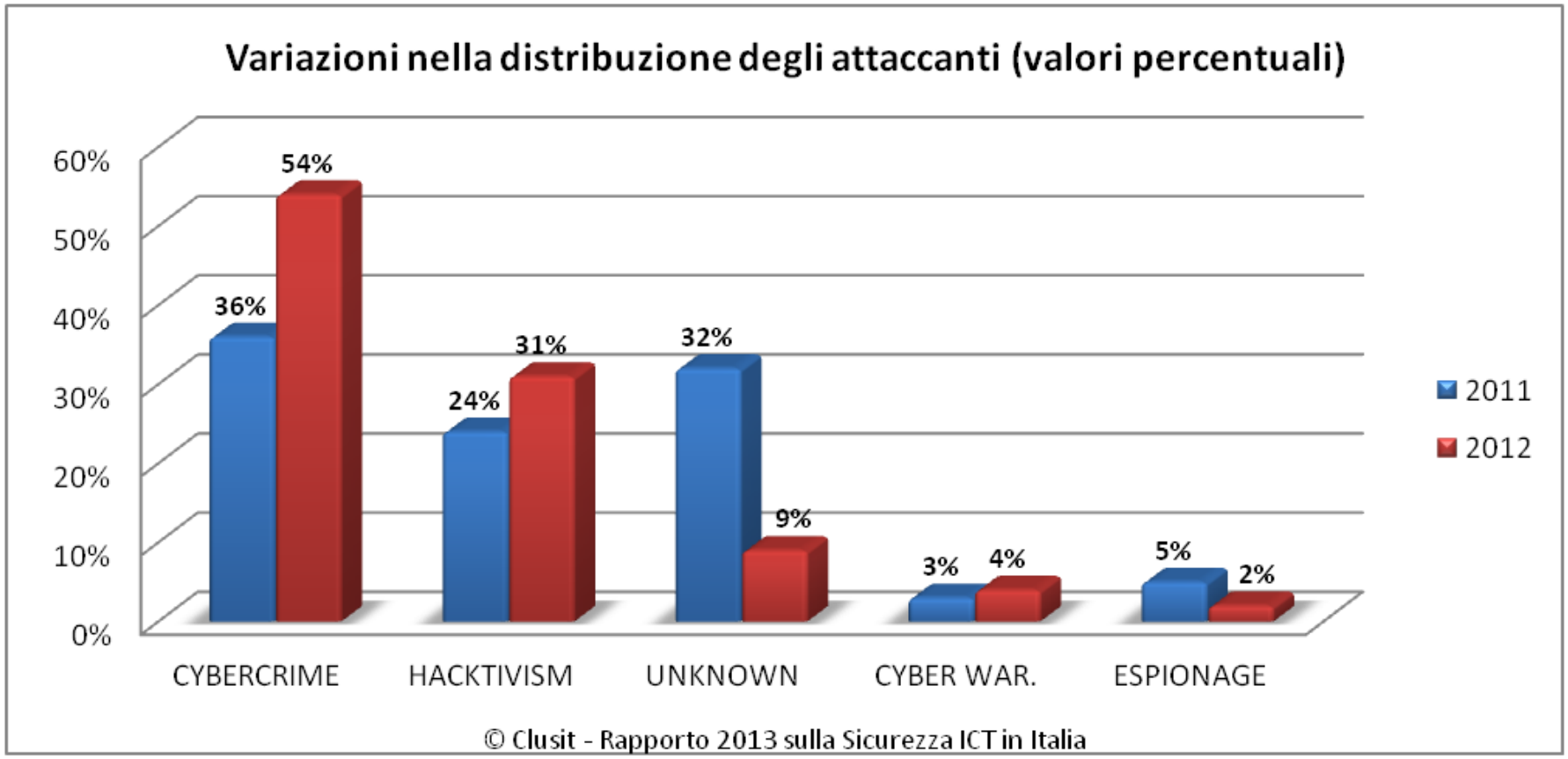
Distribuzione delle vittime (su 1.652 attacchi analizzati). Social, Cloud e Online Services crescono del 900%, e-Health 450%, Banche 347%

Panoramica cybercrime – Analisi dei principali incidenti a livello internazionale



Distribuzione degli attaccanti in valori assoluti (su 1.652 attacchi analizzati, di cui 1.183 nel 2012). Media + 254%, Cyber Crime + 370%

Panoramica cybercrime – Analisi dei principali incidenti a livello internazionale



Distribuzione degli attaccanti in percentuale. Il Cyber Crime passa dal 36% al 54%. Gli attaccanti sconosciuti diminuiscono al 9% (buon segno).

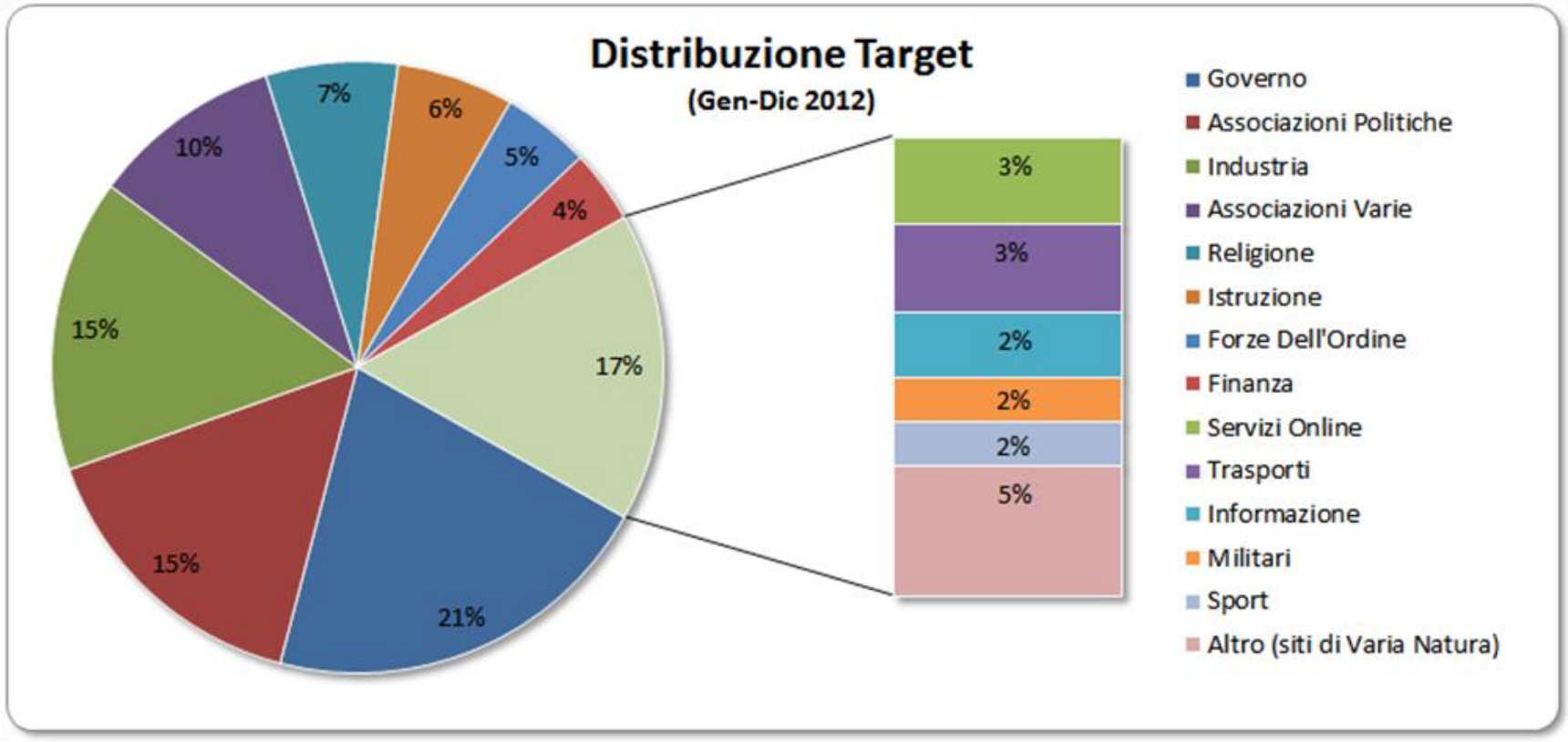
IL PARADOSSO ITALIANO

- I navigatori attivi in Italia (per mese medio) sono 27,5 M (ago 2012).
- Gli utenti di Social Network sono l'85,6% degli utenti online (23 M)
- Il 28% della popolazione usa uno smartphone (17 M)
- In un contesto del genere, solo il 2% degli Italiani dichiara di avere piena consapevolezza dei rischi informatici e di prendere contromisure.
- Mancano i dati, ma per analogia con altri Paesi (dove i dati ci sono) in Italia il costo degli incidenti informatici si può valutare in alcuni miliardi di euro / anno (perdite dirette ed indirette), escluso il furto di IP.
- Siamo un Paese avanzato, ma non abbiamo politiche di ICT Security efficaci (educazione, prevenzione, gestione degli incidenti) e non investiamo.
- Usiamo tanto e male le tecnologie, il che ci espone a rischi enormi.

UN ANNO PERDUTO

- Nonostante il varo della tanto sospirata Agenda Digitale Italiana, che sulla carta include una serie di importanti Linee di Azione sulla Cyber Security, in Italia negli ultimi 12 mesi dal punto di vista della sicurezza informatica applicata non è cambiato nulla di sostanziale.
- Risultato: nel 2012 l'Italia è al nono posto a livello globale per la diffusione di malware e soprattutto al primo posto in Europa (quarto posto a livello mondiale) per numero di PC infettati e controllati da cyber criminali (le cosiddette botnet).
- Nel 2012 8,9 milioni di italiani sono stati colpiti da una qualche forma di crimine realizzato via Internet (sono diventati i reati più diffusi)
- Solo Eurograbber (ZitMo) ha coinvolto in Italia 16 istituti bancari ed 11.893 utenti, causando il furto di oltre 16 milioni di euro in pochi giorni.

ATTACCHI SIGNIFICATIVI NOTI



Fonte: Paolo Passeri – www.hackmageddon.com

Panoramica cybercrime – principali tendenze per il 2013 e +

TENDENZE

- Cybercrime : in mancanza sia di barriere all'ingresso che di forme efficaci di contrasto e disincentivazione, altri gruppi si uniranno a quelli già oggi in attività. Aumenteranno fortemente sia i crimini informatici, sia quelli tradizionali veicolati e/o commessi con l'ausilio di sistemi ICT.
- Hacktivism : non più di massa, ma potenzialmente sempre più distruttivo. In particolare aumenteranno attacchi DDoS e data leakage.
- Cyber Espionage: "il più grande trasferimento di ricchezza della storia umana". Attacchi sempre più sofisticati sponsorizzati da governi, corporations e gruppi criminali in un contesto di "tutti contro tutti".
- Cyber Warfare : non ci sarà cyber war aperta, almeno per 1-2 anni, ma tutti si preparano attivamente a combatterla, investendo ingenti risorse. Schermaglie ed incidenti con frequenza crescente (Cyber Cold War).
- Crescente rischio di "Black Swans" ed instabilità sistemica diffusa.

Analisi del mercato italiano della sicurezza ICT

Il campione intervistato

- 207 aziende italiane di ogni dimensione
- 108 che offrono prodotti e servizi di ICT security (vendors)
- 99 User, appartenenti a tutti i settori economici.

- Investimenti: il mercato è cresciuto nel 2012 e continuerà a crescere nel 2013
- Quali settori investono di più ? In testa Finance e Energia/Utilities, seguono Telecomunicazioni e Servizi Informatici, e poi: Pubblica Amministrazione, Manifatturiero, Sanità, Commercio, Difesa, Trasporti.
- In che ambiti si investe ? In testa Compliance, Disaster Recovery / Business Continuity, soluzioni di sicurezza per Dispositivi Mobili (in grande crescita!), Governance/Audit; il mercato del Cloud, che i vendors vedono come al primo posto, sembra non essere invece una priorità immediata per le aziende.

Analisi del mercato italiano della sicurezza ICT (e mercato del lavoro)

- Dopo un 2012 in cui le aziende hanno subito sempre più attacchi, sembra aumentata la sensibilizzazione al tema della sicurezza ICT, sebbene tuttora insufficiente.
- Il 50% delle aziende che hanno subito attacchi hanno preso contromisure di carattere tecnologico. Il 33% hanno preso contromisure di carattere organizzativo e/o di processi. Solo una minoranza, però, ha aumentato il budget dedicato alla security.

- L'andamento del mercato del lavoro nel nostro settore: si è registrata una leggera crescita nel 2012 , che dovrebbe continuare nel 2013.
- Le figure professionali più richieste: è cresciuta la richiesta di figure tecniche; costante la richiesta di figure consulenziali, analisti, security auditor, security advisor, project/program Mgmt.

FOCUS ON - Social Media Security (1)

- Oggi non esiste al mondo un ambito nel quale da un lato le attività malevole abbiano maggiore probabilità di successo ed i rischi siano minori per i malintenzionati, e dall'altro gli errori umani e gli incidenti possano propagarsi con maggiore velocità dei Social Network.
- Per la loro natura, e per il sostanziale disinteresse dei loro gestori, i Social Network sono il paradiso per ogni genere di cyber criminale, spia, stalker, pedofilo, cyber-bullo, etc.
- Nel dicembre 2012, Facebook ha collaborato con l'FBI per eliminare una botnet di 11 milioni di PC (una delle più grandi di sempre), realizzata attaccando gli utenti tramite lo stesso Social Network
- Lo spam tradizionale che nel 2012 è diminuito di oltre il 50% ha solo cambiato modalità di diffusione migrando sui Social Network (costa meno, è più efficace e rende di più),facendo milioni di vittime *al giorno*.

FOCUS ON - Social Media Security (2)

- In Italia la penetrazione dei Social Network in ambito aziendale è circa del 50% (con punte del 70% in alcune aree geografiche come la Lombardia), ed è destinata ad aumentare ulteriormente nel corso di quest'anno.
- E' di fondamentale importanza adottare un insieme di processi di Social Business Security: strumenti di analisi e moderazione in tempo reale della conversazione, di monitoraggio contro frodi ed attacchi basati su malware, di tutela legale, di formazione continua del personale, di prevenzione delle minacce e di gestione degli incidenti, sia per evitare danni economici o d'immagine e cause legali (Active Defense) che per rimediare ove si siano già verificati (Crisis Management).
- Andare sui Social senza protezioni, cultura e cautele adeguate (=non improvvisate) costituisce un rischio certo di compromissione. (es. Burger King, Jeep, NBC, Palazzo Chigi, etc solo nell'ultima settimana)

FOCUS ON - Mobile Security (1)

2012, Scenario globale: è cresciuta la consapevolezza delle problematiche di Mobile Security e quindi l'offerta in termini di soluzioni e prodotti.

Crescono i rischi legati all'uso di device mobili che navigano su internet.

Il 2012 ha rappresentato una impennata impressionate sia in termini di volumi di malware che di nascita di nuovi malware e il 2013 conferma la tendenza.

In Italia: abbiamo una forte crescita nell'uso di smart device: il 55% degli utenti di smart device ha acquistato il primo telefono\tablet nel 2012, un tasso di crescita impressionante in periodo di crisi economica.

Dal fronte dei vendor è aumentata l'offerta, concentrando l'interesse principalmente su: l'introduzione di software antivirus\antimalware sul device; il management di device mobili con soluzioni del tipo BYOD ; un focus su DLP e content analisys di ciò che viene visitato\trasmesso con questi device .

Nel 2012 la piattaforma più colpita è stata android ma questo è dovuto alla sua maggior diffusione piuttosto che a "debolezze" intrinseche della piattaforma.

FOCUS ON - Mobile Security (2)

Uso degli Smart Device: l'uso che si fa dei device mobili e le applicazioni che si scaricano sono punti focali di attacco di malware o hacking.

Anche l'uso di social engineering attraverso i social network o il deploiment di applicazioni "infette" risulta particolarmente fruttuoso negli smart device per: la poca diffusione di strumenti di difesa a bordo del device e la maggiore disattenzione degli utenti nei confronti di questi strumenti.

Altro elemento di rischio è l'uso di questi device per accedere alla posta elettronica. Il 60% degli utenti italiani accede alla posta da smarthphone e tablet, con maggiori difficoltà nel riconoscere phishing o target attaks.

Estensione della superfice di attacco italiana: si è drammaticamente allargata senza che vi sia stata una equivalente presa di coscienza da parte dei gestori IT. Le ragioni di questo allargamento risiedono nell'impressionane aumento dell'uso di smart device, nel loro uso promisquo ed ubiquo ed in una certa inerzia degli utilizzatori. Le aziende italiane, però, prevedono di aumentare gli investimenti in sicurezza (vedi survey Clusit).

FOCUS ON - Cloud Security (1)

Lo scenario: nel 2012 il fenomeno del cloud computing è entrato nella fase di maturità in molti mercati del mondo e ha consolidato le relazioni con altre tendenze dominanti dell'information Technology quali ad esempio il mobile.

Il mercato: nuove soluzioni di sicurezza erogate in modalità cloud (Security as a Service - SecaaS), con un marcato incremento della numerosità dei prodotti offerti e delle tipologie di servizi.

Gli incidenti del 2012: dal punto di vista dei data breach, i servizi cloud non hanno avuto un'attenzione maggiore rispetto ai servizi erogati o gestiti in modo tradizionale. Gli episodi che si sono verificati sulle grandi cloud pubbliche rientrano nella media.

È invece emerso il problema della disponibilità dei servizi . Le brevi interruzioni dei servizi erogati da Amazon, in alcuni datacenter americani, hanno evidenziato l'esigenza, di dotarsi di contromisure specifiche a garanzia della continuità del servizio.

FOCUS ON - Cloud Security (2)

Gli Stati Uniti e la Federal Cloud Strategy: creata per diffondere il cloud all'interno delle agenzie federali. Comprende il programma "Federal Risk and Authorization Management Program" (FedRAMP) gestito dalla GSA.

In Europa: La Commissione Europea dedica alla sicurezza nel cloud continue iniziative. È stata bandita una gara per lo sviluppo di progetti sul tema "Governmental Clouds & Incident Reporting", che si occupano di: incident reporting in ambito cloud nelle telecomunicazioni; definiizione di linee guida per rendere più sicure le infrastrutture dei Cloud Provider.

In Italia: a livello legislativo, è iniziato un percorso che ha portato a definire gli obiettivi dell'Agenda Digitale Italiana e a costituire l'Agenzia per l'Italia Digitale. Il cloud (e sembra la sua sicurezza) è visto come un tema di assoluta centralità.

Nuove sfide: il cloud nelle applicazioni militari, cui si interessa in particolare l'esercito americano, e il cloud per le infrastrutture critiche, che vede l'Europa molto attiva, con un ruolo preminente.

Per maggiori informazioni e per chiedere una copia del rapporto in formato digitale:

rapporti@clusit.it