Associazione Italiana
Information Systems Auditors

ISACA
Capitolo di Milano

Investire sui progetti di formazione per la sicurezza delle informazioni

4

Managers
Employees
Professionals
Students

di Vito Villa
www.information-security.it

Hidden Slide

Presentation Abstract

- Le agenzie di stampa riportano sempre più frequentemente di attacchi informatici subiti dalle più grandi società multinazionali, nonostante stanzino ingenti investimenti per la protezione delle infrastrutture e delle informazioni.
- Ciò è reso possibile non solo dalla continua mutazione delle strategie e delle tecniche adottate dai gruppi organizzati che portano avanti questi attacchi ma anche da una complessa leva sui fattori umani che sono quasi sempre l'elemento scatenante.
- L'evoluzione delle tecnologie e l'utilizzo sempre più diffuso di procedure informatiche – nel lavoro come nella vita privata - richiede una crescente preparazione a tutti i livelli delle gerarchie aziendali e una speciale attenzione per evitare il rischio di **perdere, danneggiare** o **farsi sottrarre** i dati trattati.
- La **prevenzione** riveste dunque in questo contesto una particolare importanza, ed uno dei suoi elementi cardine è la **formazione e l'educazione** attraverso la quale fornire una serie di nozioni di carattere informativo e comportamentale, volte ad **aumentare la consapevolezza e la responsabilità** nel trattamento di dati mediante strumenti informatici, supporti cartacei o comunicazioni verbali.
- Nonostante questa formazione sia già diffusa al personale informatico/IT, oggi è sempre più necessario ridurre il gap di conoscenza con tutte le altre funzioni aziendali soprattutto per quanto riguarda l'adozione di un corretto approccio nel trattamento delle informazioni.
- Nel corso degli anni, molte soluzioni di e-learning sono state sviluppate per cercare di colmare il gap della formazione sulla sicurezza informatica. Ma alla luce della sempre più rapida evoluzione tecnologica, sono ancora efficaci oggi questi strumenti? E' sufficiente una spunta/check sulla lista di conformità dei vari regolamenti oggi in vigore per molti settori aziendali?

- Lavoro nel mondo dell'Informatica da + di 30 anni.
- Inizio la carriera come sviluppatore SW.
- Nella Sicurezza informatica da circa 20 anni.
- Ho lavorato per una grande multinazionale americana nel settore tecnico di prevendita, come responsabile tecnico dei clienti e come regional product manager.
- Da un paio d'anni mi occupo di un progetto per formare le direzioni aziendali e gli impiegati sulla sicurezza delle informazioni.

Vito Villa

Agenda

- "Cronaca nera" informatica
- L'era dei tanti cambiamenti
  - Rivoluzioni industriali
  - Il cambiamento delle minacce informatiche
- L'approccio delle aziende italiane all'Information Security
- Il "fattore umano" come pilastro fondamentale per la prevenzione agli incidenti di sicurezza informatica
- Intervenire sul "fattore umano" per ridurre il gap della conoscenza

I 10 incidenti rappresentativi del 2014

Vittima	Attaccante	Tecniche usate
JP Morgan Chase	Cyber Espionage, State Sponsored?	Known vulnerabilities, APT
Home Depot	Cyber Crime	APT, custom malware
Target	Cyber Crime	Vulnerabilities, malware
Ebay	Cyber Crime	Multiple
Operazione "Newscaster"	Cyber Espionage (Iran?)	Social Engineering
Gruppo Benetton	Cyber Espionage (Siria?)	Custom malware?
Operazione "Putter Panda"	Cyber Espionage (Cina?)	Multiple
Sony	Cyber Crime, State Sponsored?	Multiple
Anthem	Cyber Crime	APT, Custom Malware
Korea Hydro & Nuclear Power	Hacktivist	Sconosciute

Fonte: Rapporto Clusit 2015

ANSA.it Software&App

Fai la ricerca | Il mondo in immagini | Vai alla Borsa | Vai al Meteo

Cronaca | Politica | Economia | Regioni + | Mondo | Cultura | Tecnologia | Sport | FOTO | VIDEO | Tutte le sezioni +

PRIMOPIANO • HI-TECH • INTERNET & SOCIAL • TELECOMUNICAZIONI • SOFTWARE & APP

ANSA.it › Tecnologia › Software & App › In Italia 11 mld danni per perdite dati

In Italia 11 mld danni per perdite dati

Solo 10% aziende al passo con i tempi per protezione

Redazione ANSA

ROMA

02 dicembre 2014
18:59
NEWS

Suggerisci
Facebook
Twitter
Google+
Altri
A+ A A-
Stampa
Scrivi alla redazione

Archiviato in

Economia, affari e finanza
Mass Media
Perdite
Macroeconomia
Ricerche, Sviluppo
Vanson Bourne

© ANSA

CLICCA PER INGRANDIRE

Tra perdite di dati sensibili per guasti o errori e interruzioni inattese dei sistemi informatici, le aziende italiane negli ultimi 12 mesi hanno perso 11,2 miliardi di euro. A rivelarlo è l'EMC Global Data Protection Index, studio condotto da Vanson Bourne, che ha interpellato 3.300 dirigenti IT di medie e grandi aziende in 24 Paesi, rilevando che a livello mondiale la perdita è stata di 1.700 miliardi di dollari.

In Italia solo il 10% delle aziende è al passo con i tempi per la protezione. "Tutto questo - sottolinea lo studio -, in uno scenario nazionale in cui l'80% delle aziende intervistate ha registrato, negli ultimi dodici mesi, un blocco inaspettato nei propri sistemi informatici o una perdita di dati sensibili, che hanno portato per il 38% a una perdita della produttività, per il 22% a un decremento del fatturato e per il 36% al ritardo nello sviluppo di un prodotto". In totale, emerge dall'inchiesta, "il

ULTIMA ORA TECNOLOGIA

19:17 Attacco hacker a Sony, rubati molti dati
18:26 Lollipop, la diffusione è sotto lo 0,1%
16:29 Internet per 16% italiani solo da mobile
15:52 Simulacro iPad Air 'maxi' in un video
13:35 In Italia 11 mld danni per perdite dati
13:09 Un'App per tagliare bolletta smartphone
11:59 Computer deduce meglio uomo dati studi
10:54 Bmw prova Google Glass in test pre-serie
10:01 Google supera Apple nelle scuole Usa
16:01 Aids, la mela di Apple si tinge di rosso

› Tutte le news

+ LETTI | Ultima Settimana

6082 volte
BlackBerry, 550 dollari se lasci iPhone

5730 volte

CORRIERE DELLA SERA.it

Economia Digitale

ACCEDI | Cerca

Home Opinioni Economia Cultura Spettacoli Cinema Sport Salute Tecnologia Scienze Motori

< TECNOLOGIA ECONOMIA DIGITALE

Tocca il tasto dell'eleganza con LG G2
In REGALO l'esclusiva cover PIQUADRO
SCOPRI DI PIÙ
Regolamento completo su lgpromo.it

L'ATTACCO SU SCALA GLOBALE

Due milioni di password rubate da un solo virus

Colpite utenze di Facebook, Twitter, Gmail con Pony Botnet Controller, malware capace di controllare il pc infetto

Social network ★ 33

Sicurezza informatica ★ 8

Economia ★ 132

NASCONDI

66% PREOCCUPATO

62 8

DA GUARDARE

Ascolta | Stampa | Email

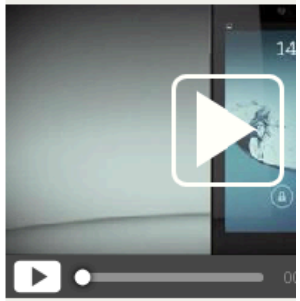
NOTIZIE CORRELATE

- Twitter a Wall Street: i conti e gli account falsi, quali sono le preoccupazioni degli investitori (06/11/2013)

MILANO - Due milioni di password rubate da Facebook e

TECNOLOGIA TV

Arriva YotaPhone, lo smartpho doppio schermo



Tecnologia | 05 dicembre 2013

Link: http://video.corriere.it/arriv

3 9

ATTENTI AL CLIC

Facebook torna il virus degli occhiali

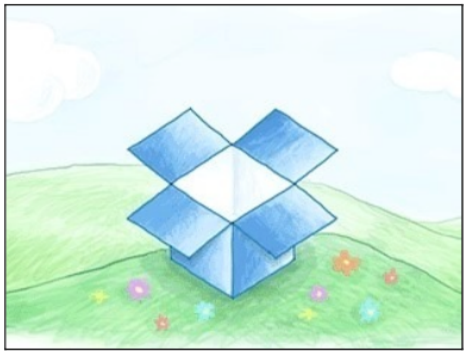
Comparso nel 2012, ritorna la pubblicità dei Ray Ban scontati che, se cliccata, ruba i nostri contatti e se procediamo nell'acquisto anche i dati della carta di credito

di Alessio Lana

27 Ottobre 2014
www.corriere.it

Dropbox sotto attacco? ...Colpa degli utenti!

14 Ottobre 2014



- Un gruppo di hackers rivendica di aver rubato le credenziali di quasi sette milioni di account del popolare servizio, e a dimostrazione del fatto ha pubblicato online i dati di accesso di 400 utenti.
- Dropbox però nega che il furto sia avvenuto dal proprio servizio: la colpa è del riuso delle password su account diversi, abitudine ancora diffusa.

Fonte: http://www.ictbusiness.it

G Data Security Labs alle prese con lo spyware ComRAT

Gli esperti dei G DATA Security Labs hanno scoperto e analizzato una nuova variante del complesso programma spyware Agent.BTZ. Lo spyware ComRAT attacca network ad alto potenziale con l'obbiettivo di rubare dati sensibili

www.channelbiz.it

Non solo password. Chi decide deve sapere cosa accade in ufficio

Dai problemi con le password a quelli che riguardano i servizi cloud il numero di pericoli alla sicurezza che i dipendenti portano con loro in ufficio è sufficiente a mettere sul chi vive chi vigilia sulla sicurezza aziendale

www.techweekeurope.it

Gli hotspot WiFi pubblici e aperti sono insicuri

Avast ha condotto un esperimento sulle reti WiFi pubbliche a livello globale, denunciando la presenza di gravi lacune nella sicurezza delle Wi-Fi aperte. Gli utenti asiatici sarebbero più a rischio degli utenti europei e americani

www.itespresso.it

La cyber security è un rischio strategico per l'azienda

Il fattore umano è spesso ignorato o sottovalutato, ma ormai è un elemento critico della difesa IT

www.techweekeurope.it

Rapporto ISTR 2014 di Symantec sul 2013 : grandi perdite di dati e attacchi focalizzati nel panorama della sicurezza IT

Dall' Internet Security Threat Report 2014 di Symantec: gli attacchi sono sempre più mirati e serve una cultura aziendale della sicurezza IT

www.techweekeurope.it

L'opinione di Clusit

La situazione non cambia molto in ambito aziendale. Il Ponemon Institute ha condotto nel 2011 una indagine (pubblicata nel 2012), finalizzata ad evidenziare il costo medio nel nostro Paese relativo alla compromissione di un record contenente dati personali[76]. Il risultato è stato eloquente: per ogni compromissione di un record personale un'azienda spende in Italia 78 euro tra indagini, notifiche, spese legali e costi legati all'interruzione del business.
A rinforzare il concetto che la sicurezza non è solo protezione del dato da fattori esterni ma anche, e soprattutto, da fattori interni (che hanno natura principalmente culturale), lo stesso studio ha evidenziato che la prima causa per la perdita di informazioni personali (39%) non è costituita da attacchi criminali, ma da negligenza ed errori umani.
Anche per quanto riguarda lo spionaggio industriale non esistono dati ufficiali, ma solo "sensazioni" colte dal mercato ed alcune case histories (rigorosamente protette da NDA e non pubbliche). Il bersaglio principale sono le nostre PMI ad alto valore aggiunto, che stanno subendo una significativa emorragia di proprietà intellettuale, senza nemmeno accorgersene, da parte di cyber-vampiri di ogni nazionalità. Così il nostro know-how, il nostro design, i nostri brevetti finiscono nelle mani dei competitor, con danni incalcolabili (e che nessuno calcola). Le aziende chiudono anche per questo, al giorno d'oggi.
Sempre in tema di scarsa cultura della sicurezza informatica i nostri giova-

73 http://www.reuters.com/article/2012/12/17/us-eu-cybersecurity-idUSBRE8BG0Z220121217
74 http://www.symantec.com/it/it/about/news/release/article.jsp?prid=20121004_01
75 http://www.webmaori.com/blog/utenti-internet-in-italia-maggio-2012.html
76 http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-italy.en-us.pdf

Recessione economica

- Ricerca di maggiore efficienza nei processi
- Maggiore utilizzo dell'Informatica per il business

Evoluzione tecnologica

Rivoluzione Industriale
(Wikipedia.it)

- La rivoluzione industriale fu un processo di evoluzione economica o industrializzazione della società che da sistema agricolo-artigianale-commerciale divenne un sistema industriale moderno caratterizzato dall'uso generalizzato di macchine azionate da energia meccanica e dall'utilizzo di nuove fonti energetiche inanimate (come ad esempio i combustibili fossili), il tutto favorito da una forte componente di innovazione tecnologica e accompagnato da fenomeni di crescita, sviluppo economico e profonde modificazioni socio-culturali e anche politiche.
- Talvolta ci si riferisce agli effetti dell'introduzione massiccia dell'elettronica, delle telecomunicazioni e dell'informatica nell'industria come alla terza rivoluzione industriale, che viene fatta partire dal 1970.
- La rivoluzione industriale comportò una profonda ed irreversibile trasformazione che parte dal sistema produttivo fino a coinvolgere il sistema economico nel suo insieme e l'intero sistema sociale.

Evoluzione della tecnologia --> rivoluzione industriale

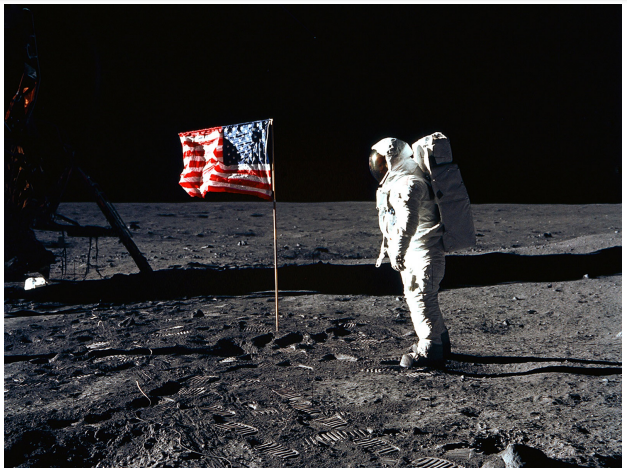
Mobile computing

Cloud computing

Internet of Things

Decina di anni

Il Mobile Computing



Uno smartphone di oggi è migliaia di volte più potente dell'Apollo Guidance Computer

Il Mobile Computing

The faithful gather in 2005 near St. Peter's to witness Pope John Paul II's body being carried into the Basilica for public viewing.

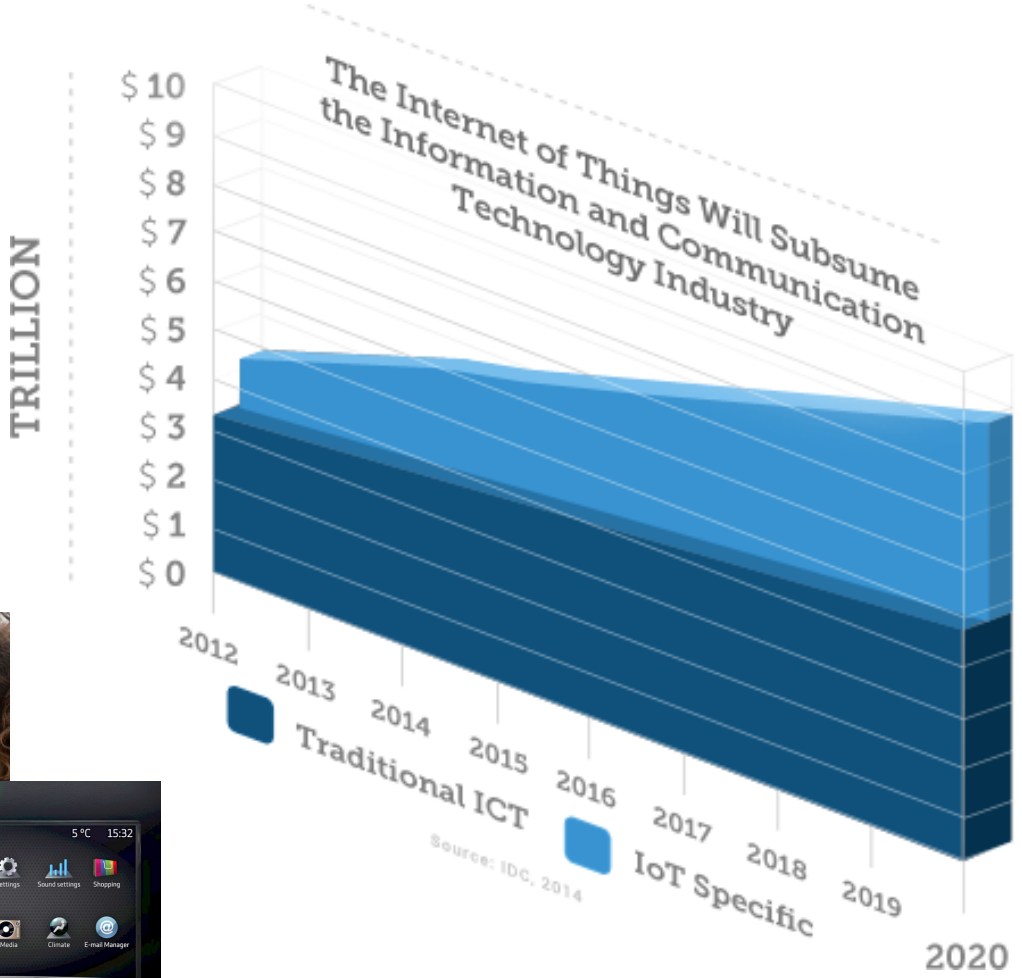
St. Peter's Basilica at the Vatican, on March 13, 2013.

Fonte: http://photoblog.nbcnews.com

Il Cloud Computing

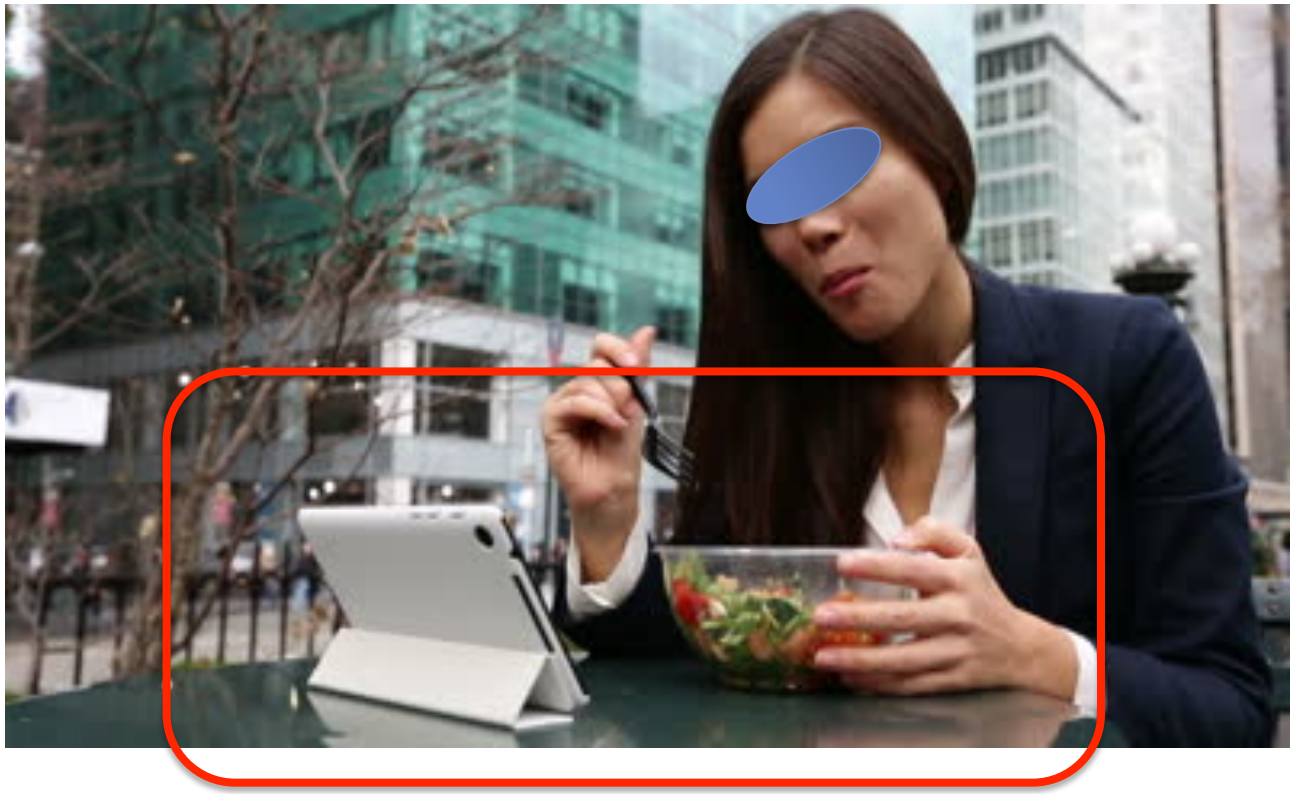
- Wikipedia: si indica un paradigma di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati.
- Un mercato che solo in Italia vale circa 1Mld eur/ anno.
- Maggiore Governance dei sistemi e maggiore sicurezza delle informazioni.
- Si creano i fondamenti tecnologici a basso costo per gestire dati provenienti dall'Internet of Things.

Internet Of Things



http://www.emc.com/leadership/digital-universe/2014iview/internet-of-things.htm

Le nuove tecnologie cambiano il nostro modo di lavorare

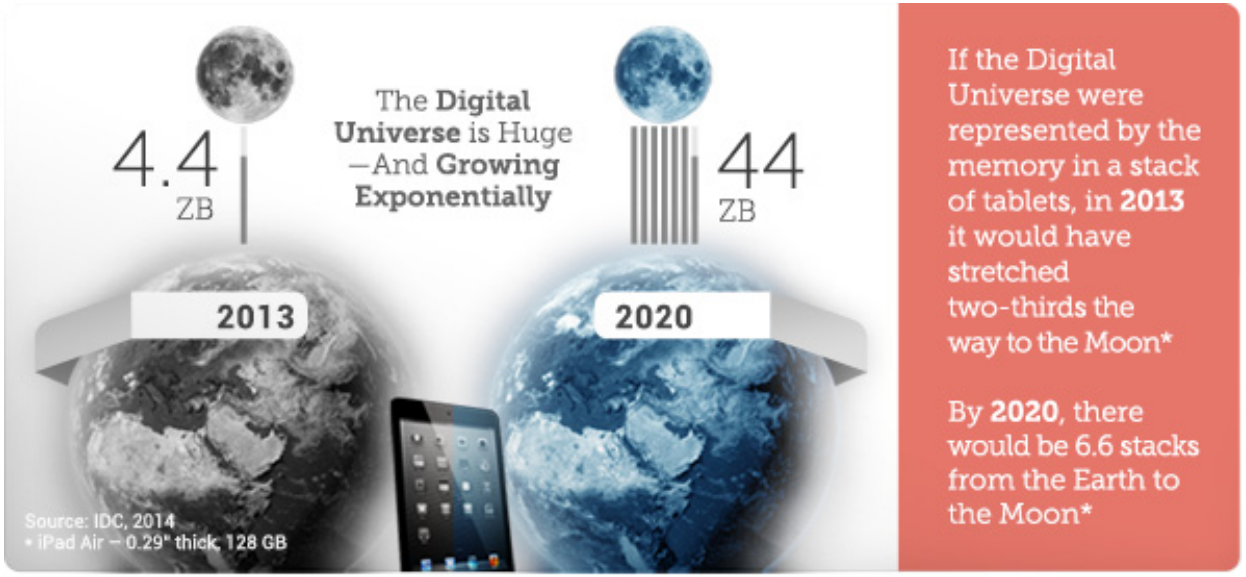


… e di conseguenza la nostra vita

- Il 75% degli adulti ha ammesso che quando va in bagno, usa il cellulare

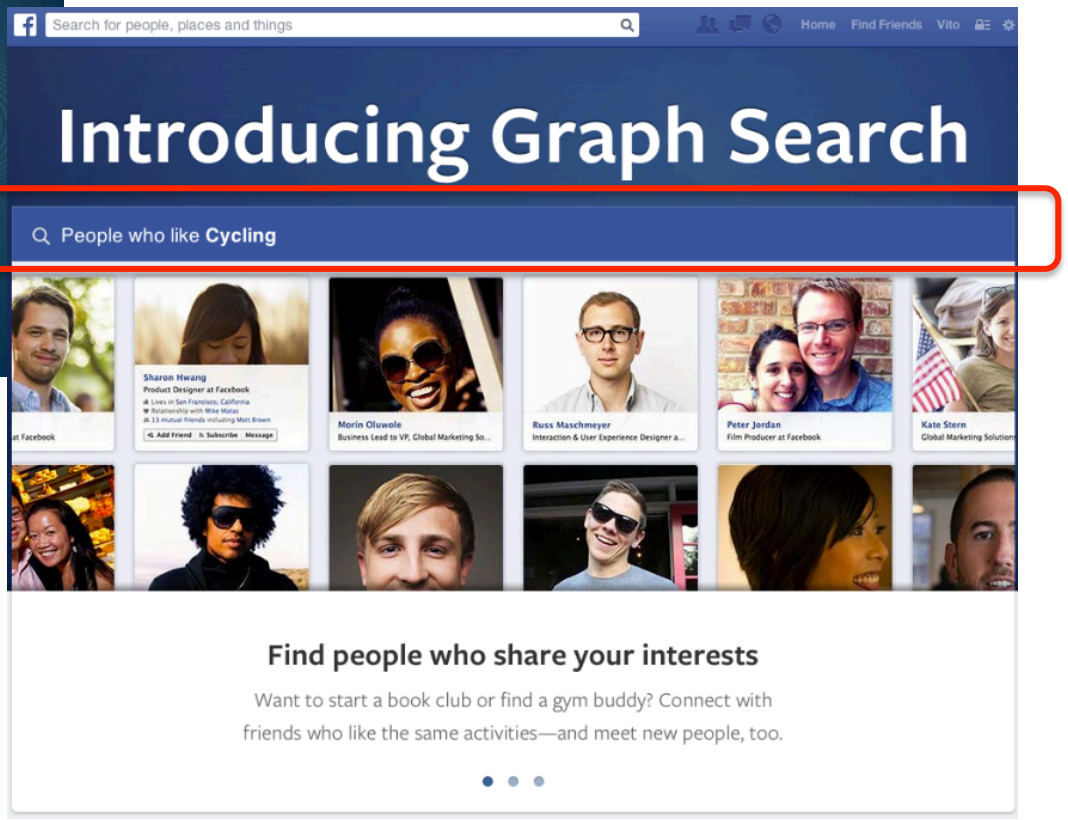
Fonte: http://www.dailymail.co.uk

I Social Media rappresentano la nuova frontiera delle informazioni



Fonte: http://www.emc.com

La nostra "vita" è online…



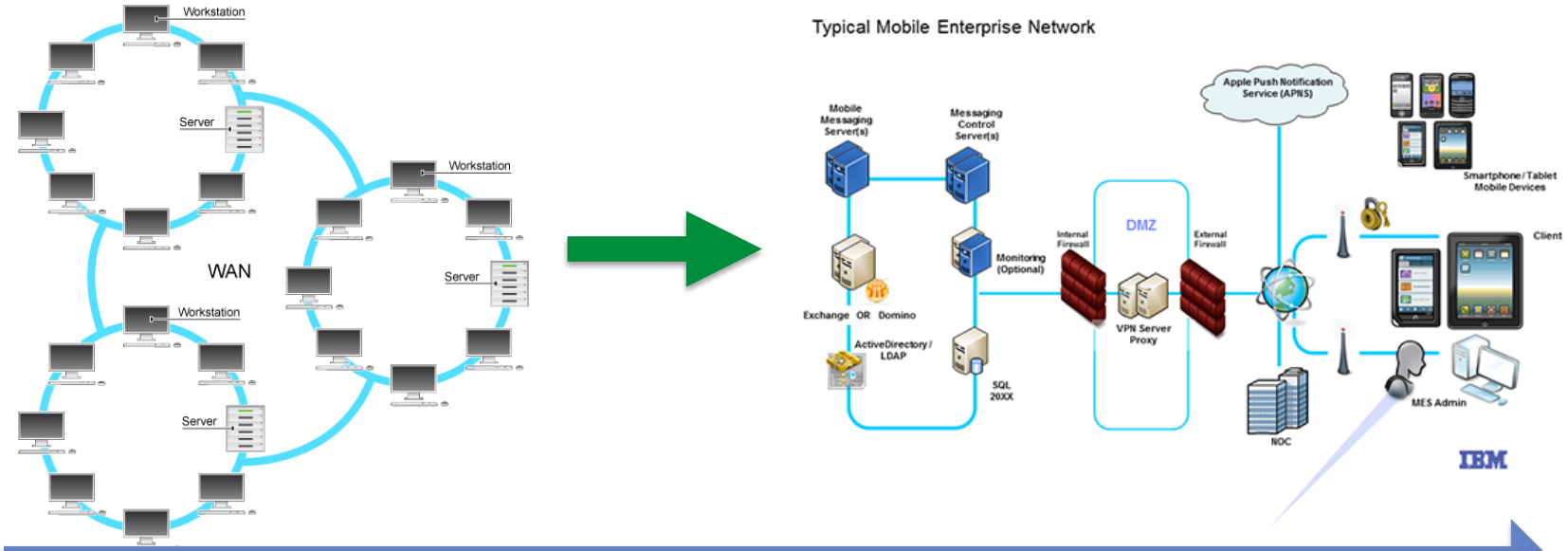
Fonte: www.facebook.com

Internet

- Internet più veloce per supportare la "Crescita esponenziale dei dati" ed il transito delle informazioni per il Cloud Computing → Fibra e 4G
- CloudComputing e BigData analytics diventano strategici per le aziende
- Analisi dei comportamenti dei "cybernauti" → analisi delle informazioni per il business

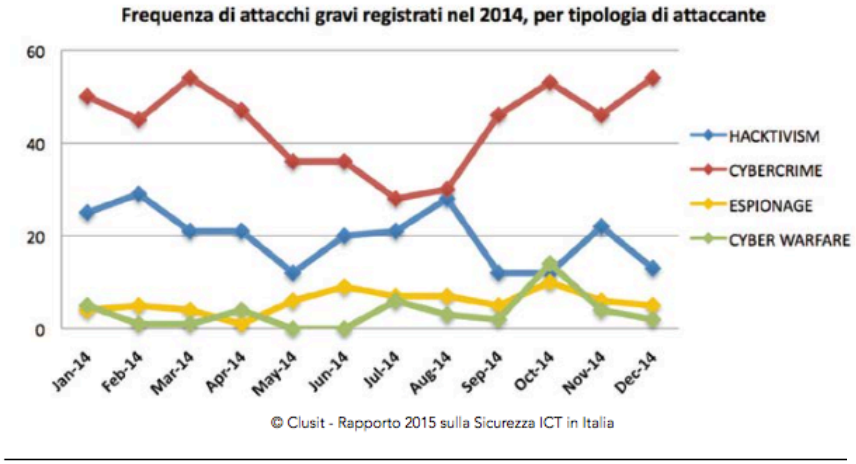
Il perimetro della Rete Aziendale si disgrega

- In un contesto attuale, il perimetro della rete aziendale si disgrega sempre più rispetto al passato rendendo sempre più difficile il controllo e il confinamento delle informazioni.



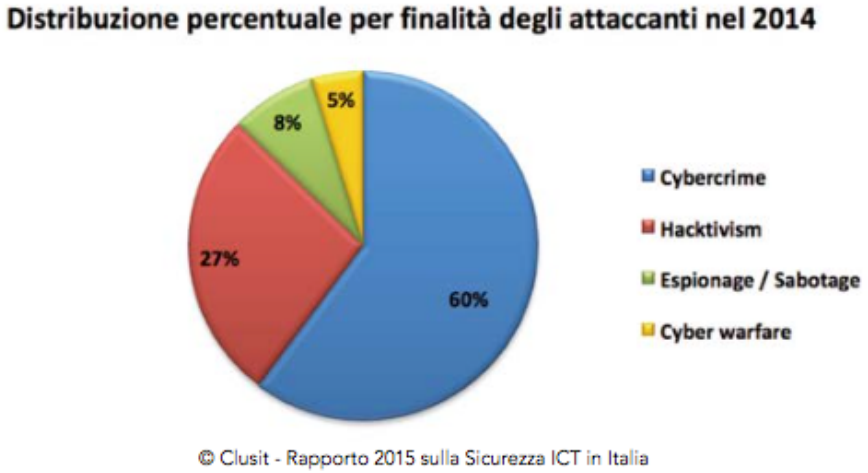
Il Cybercrime rispetto alle altre forme di attacco

Attacchi organizzati per rubare informazioni e soldi



[51] Tenendo in considerazione l'aggiornamento dei criteri di classificazione applicati ai dati 2014.

© Clusit 2015



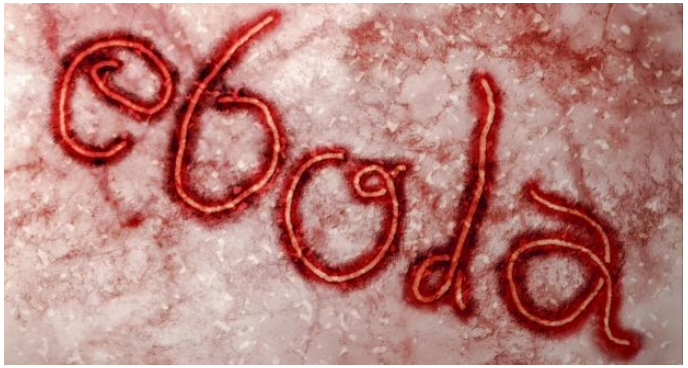
Fonte: Rapporto Clusit 2015

Il cambiamento del Malware

- Joke
- Virus
- Trojan Horse
- Worm
- Macro Virus

- Phishing (*)
- Bot Network
- Rootkit
- Ramsonware
- Criptolockers
- RAT
- C&C Servers

Social Engineering



(*) Non è un Malware ma una forma di attacco per veicolare i Malware o rubare informazioni

Malware: Cosa sta cambiando?

- Usano tecniche di evasione per nascondere/modificare i logs
- Obiettivo di infettare – NON serve fare notizia
- Sono intelligenti
  - Polimorfismo
  - NON funzionano in ambienti di sandboxing
  - Persistenti ossia rimangono a lungo sul computer prima di agire
  - Usano tecniche per riavviarsi automaticamente
- Comunicano con l'esterno (C&C Server)
- Sono in grado di usare tutte le periferiche dei PC e dei dispositivi mobili

Keyloggers

il Fatto Quotidiano.it ≡ SEZIONI BLOG FATTO TV ABBONATI FQ SHOP

Bologna, studenti hacker alzavano i voti rubando password ai prof: nei guai in 13

Archivio

Frode informatica aggravata e falso in atto pubblico commesso da privato: rischiano dai due ai sei anni di carcere gli alunni di un istituto tecnico del capoluogo. La procura dei minori: "Faremo accertamenti anche in altre scuole"

di David Marceddu | 13 dicembre 2014 COMMENTI

Il sistema utilizzato dagli studenti era noto al mondo degli hacker: attraverso dei programmi scaricabili da internet per pochi euro e poi installati sui pc presenti nelle aule, i cosiddetti *software keylogger*, le giovani talpe informatiche entravano nei registri e modificavano i loro voti. ….

Fonte: http://www.ilfattoquotidiano.it

Ramsonware

Fonte: http://www.northeastern.edu

Cryptolockers

Tue 11/25/2014 5:56 AM

sda@sda-expresso24.com

To

SDA EXPRESS COURIER

Gruppo Posteitaliane

Il vostro pacchetto con il codice di spedizione **G12328548** è arrivato al **21 ottobre 2014**. Corriere non ha espresso un pacco per te. Stampare l'etichetta di spedizione e mostrarlo in ufficio postale più vicino per ottenere il pacchetto.

Scarica etichetta di spedizione

Se il pacco non viene ricevuto entro 30 giorni lavorativi Sda Express ha il diritto di chiedere un risarcimento da voi per esso sta tenendo nella quantità di 4,75 EUR per ogni giorno di conservazione. È possibile trovare le informazioni sulla procedura e le condizioni di pacchi tenendo l'ufficio più vicino.

Tutela della Privacy

Informativa ai sensi dell'art. 13 del d. lgs n. 196 del 30 giugno 2003

I dati personali legittimamente acquisiti, a vario titolo, dalla SDA Express Courier S.p.A. potranno essere inseriti in apposite banche dati informatiche e cartacee nel rispetto delle disposizioni vigenti di cui al d.lgs n. 196/2003. Il mantenimento dei dati personali è finalizzato a permettere a SDA Express Courier S.p.A. di offrire agli utenti servizi commerciali personalizzati, consentendo agli stessi utenti di usufruire di servizi ulteriori e/o aggiuntivi, rispetto a quelli già utilizzati. I dati potranno essere comunicati a società controllanti, controllate o collegate, o comunque affidatarie di servizi per conto di SDA Express Courier S.p.A.

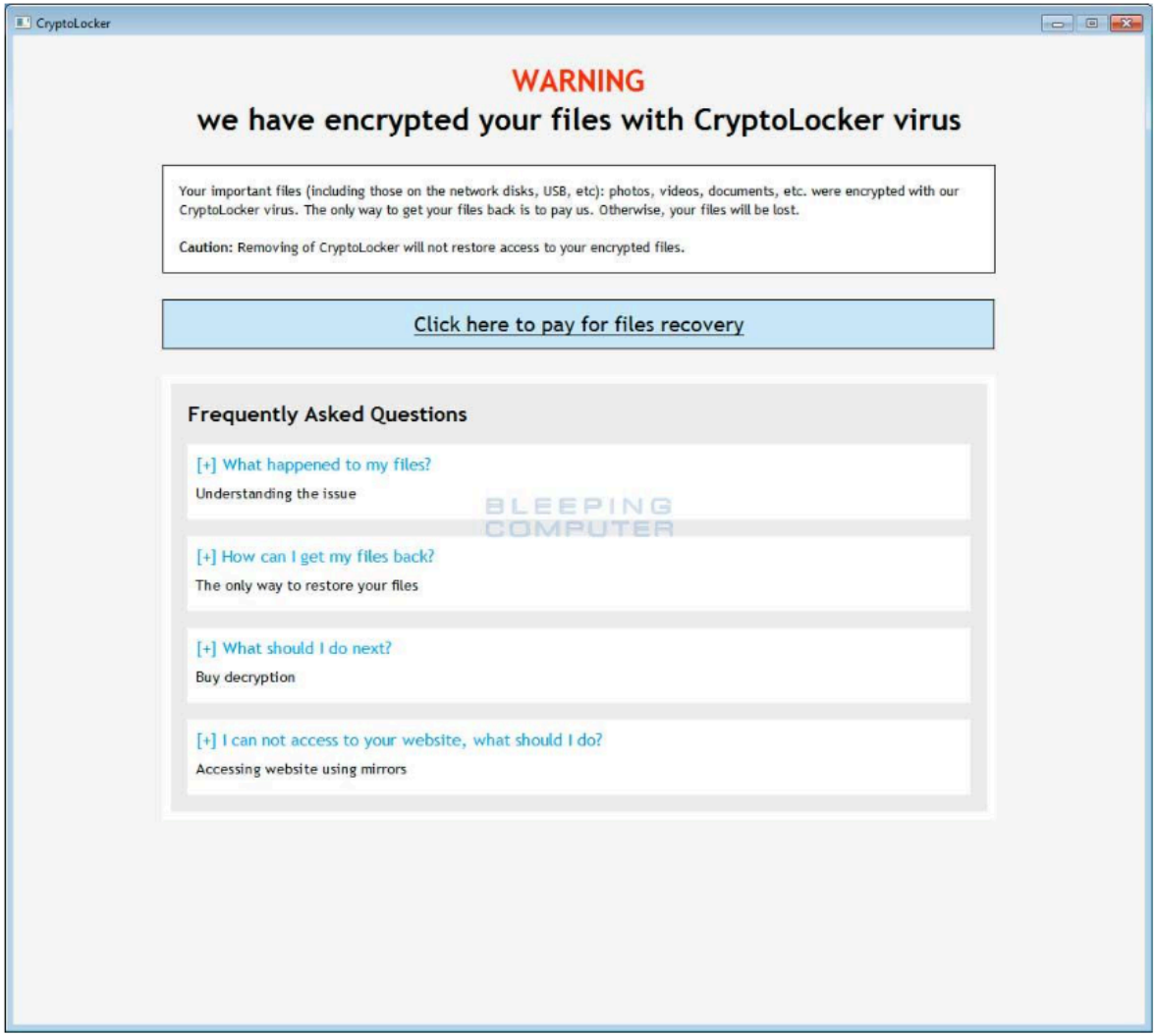
Questo è un messaggio generato automaticamente. Clicca qui per cancellarti.

Fonte: www.trendmicro.com

Cryptolockers

Fonte: www.trendmicro.com

Cryptolockers



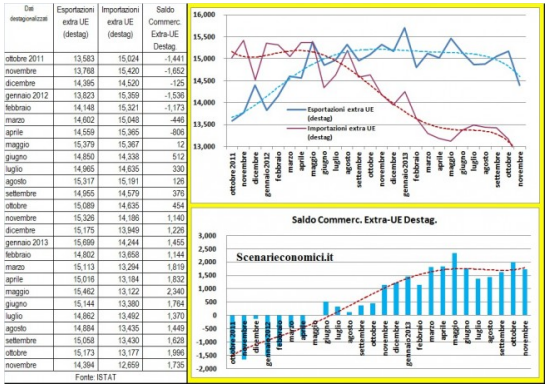
Fonte: www.trendmicro.com

Informazioni

- Sono il valore di una società.
- Le informazioni sono state anche definite come il "PETROLIO" del nuovo millennio
- Non sono solo presenti sul sistema informatico centrale dell'azienda!!
- Sistemi aziendali, ERP, Dischi/Chiavette Portatili, Email, Siti Web, Social Media.
- Le informazioni, sempre più, "Viaggiano" con noi
- Business per il Cybercrime

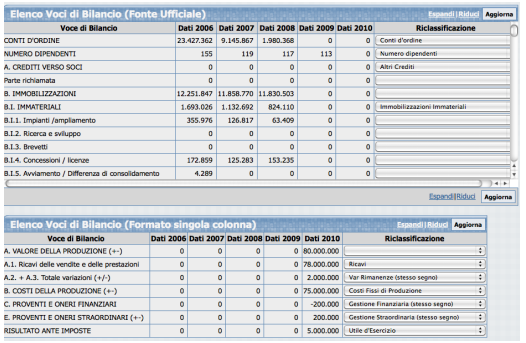
Quali sono le informazioni che una società deve proteggere? E … quanto valgono per le aziende?

- Dati bancari
- Dati finanziari
- Elenchi clienti
- Progetti
- Rete commerciale
- Il fatturato dell'azienda



Dati destagionalizzati	Esportazioni extra UE (destag)	Importazioni extra UE (destag)	Saldo Commerc. Extra-UE Destag
ottobre 2011	13,583	15.024	-1.441
novembre	13,768	15.420	-1.652
dicembre	14,395	14.520	-125
gennaio 2012	13,823	15.359	-1.536
febbraio	14.148	15.321	-1.173
marzo	14.602	15.048	-446
aprile	14.559	15.365	-806
maggio	15.379	15.367	12
giugno	14.850	14.338	512
luglio	14.965	14.635	330
agosto	15.317	15.191	126
settembre	14.955	14.579	376
ottobre	15.089	14.635	454
novembre	15,326	14,186	1,140
dicembre	15,175	13.949	1,226
gennaio 2013	15,699	14.244	1,455
febbraio	14,802	13.658	1,144
marzo	15,113	13.294	1,819
aprile	15.016	13.184	1,832
maggio	15,462	13.122	2,340
giugno	15.144	13.380	1,764
luglio	14,862	13.492	1,370
agosto	14.884	13.435	1,449
settembre	15.058	13.430	1,628
ottobre	15.173	13.177	1,996
novembre	14.394	12.659	1,735

Fonte: ISTAT



Elenco Voci di Bilancio (Fonte Ufficiale)						
Voce di Bilancio	Dati 2006	Dati 2007	Dati 2008	Dati 2009	Dati 2010	Riclassificazione
CONTI D'ORDINE	23.427.362	9.145.867	1.980.368	0	0	Conti d'ordine
NUMERO DIPENDENTI	155	119	117	113	0	Numero dipendenti
A. CREDITI VERSO SOCI	0	0	0	0	0	Altri Crediti
Parte richiamata	0	0	0	0	0	
B. IMMOBILIZZAZIONI	12.251.847	11.858.770	11.830.503	0	0	
B.I. IMMATERIALI	1.693.026	1.132.692	824.110	0	0	Immobilizzazioni immateriali
B.I.1. Impianti /ampliamento	355.976	126.817	63.409	0	0	
B.I.2. Ricerca e sviluppo	0	0	0	0	0	
B.I.3. Brevetti	0	0	0	0	0	
B.I.4. Concessioni / licenze	172.859	125.283	153.235	0	0	
B.I.5. Avviamento / Differenza di consolidamento	4.289	0	0	0	0	

Espandi|Riduci Aggiorna

Elenco Voci di Bilancio (Formato singola colonna)						
Voce di Bilancio	Dati 2006	Dati 2007	Dati 2008	Dati 2009	Dati 2010	Riclassificazione
A. VALORE DELLA PRODUZIONE (+-)	0	0	0	0	80.000.000	
A.1. Ricavi delle vendite e delle prestazioni	0	0	0	0	78.000.000	Ricavi
A.2. + A.3. Totale variazioni (+/-)	0	0	0	0	2.000.000	Var Rimanenze (stesso segno)
B. COSTI DELLA PRODUZIONE (+-)	0	0	0	0	75.000.000	Costi Fissi di Produzione
C. PROVENTI E ONERI FINANZIARI	0	0	0	0	-200.000	Gestione Finanziaria (stesso segno)
E. PROVENTI E ONERI STRAORDINARI (+-)	0	0	0	0	200.000	Gestione Straordinaria (stesso segno)
RISULTATO ANTE IMPOSTE	0	0	0	0	5.000.000	Utile d'Esercizio

Espandi|Riduci Aggiorna

Ma la lista è di gran lunga maggiore a quanto elencato!!

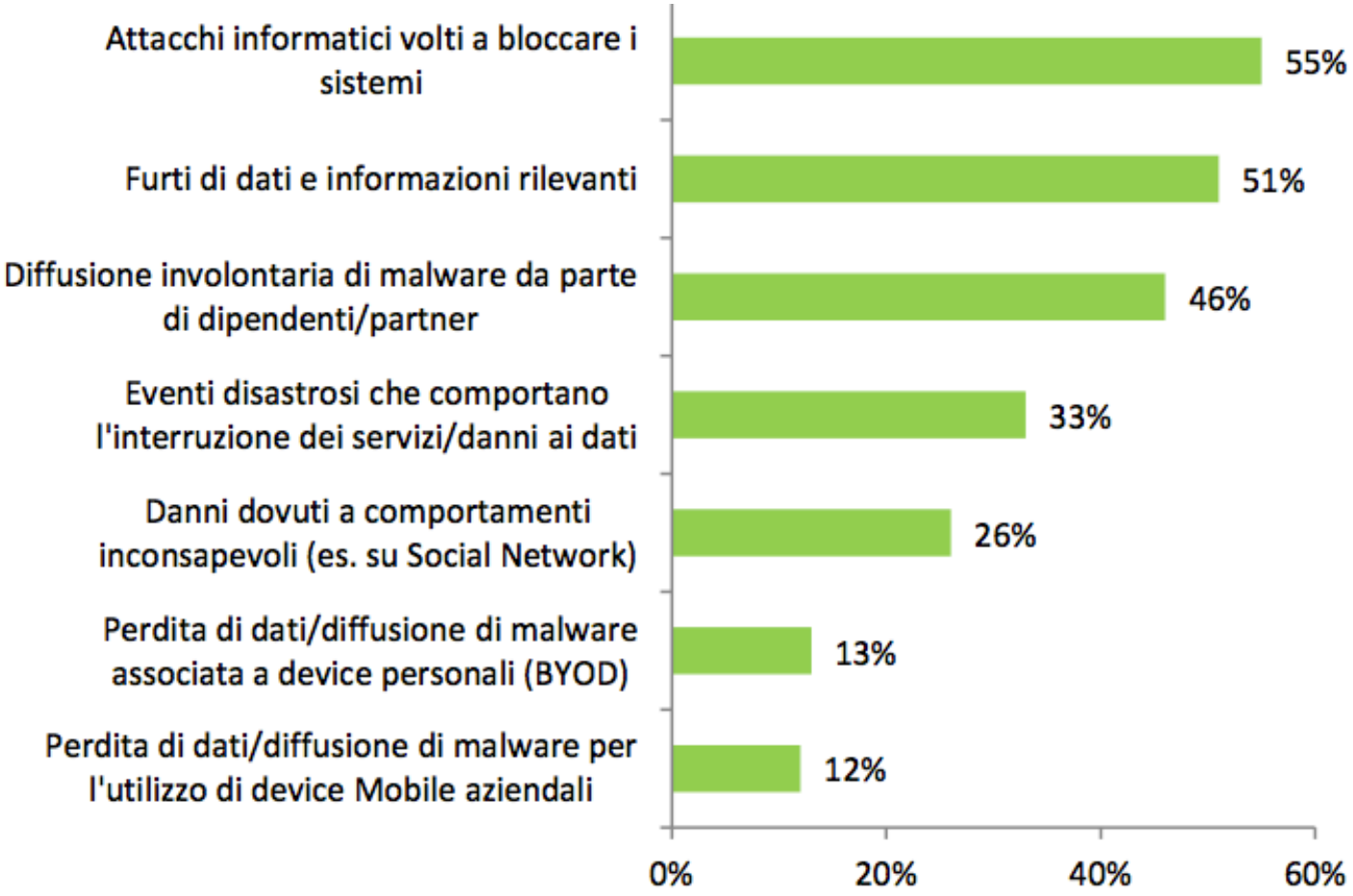
Approccio aziende italiane alla cybersecurity

Secondo uno studio condotto nel 2013 da *The Innovation Group*, le aziende italiane:

- Non assegnano sufficiente importanza ai temi **Mobile, Social Media e BYOD (Bring Your Own Device).**
- Scarsa consapevolezza degli **attacchi Advanced Persistent Threats, Zero day e Scada.**
- Sottostimano le perdite economiche legate a incidenti dovuti a cyber attack.

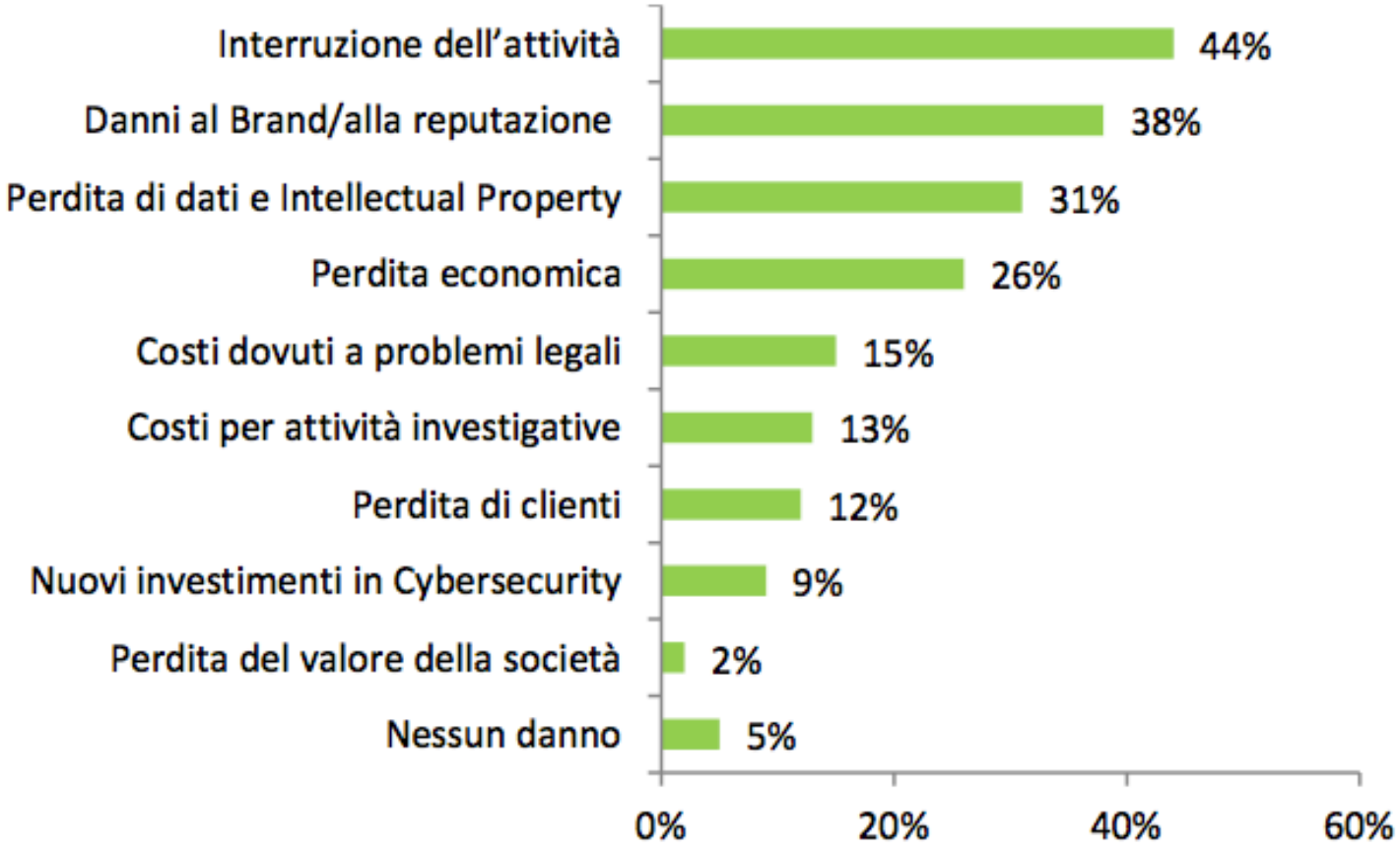
Fonte: http://theinnovationgroup.it

Principali rischi informatici percepiti dalle aziende italiane



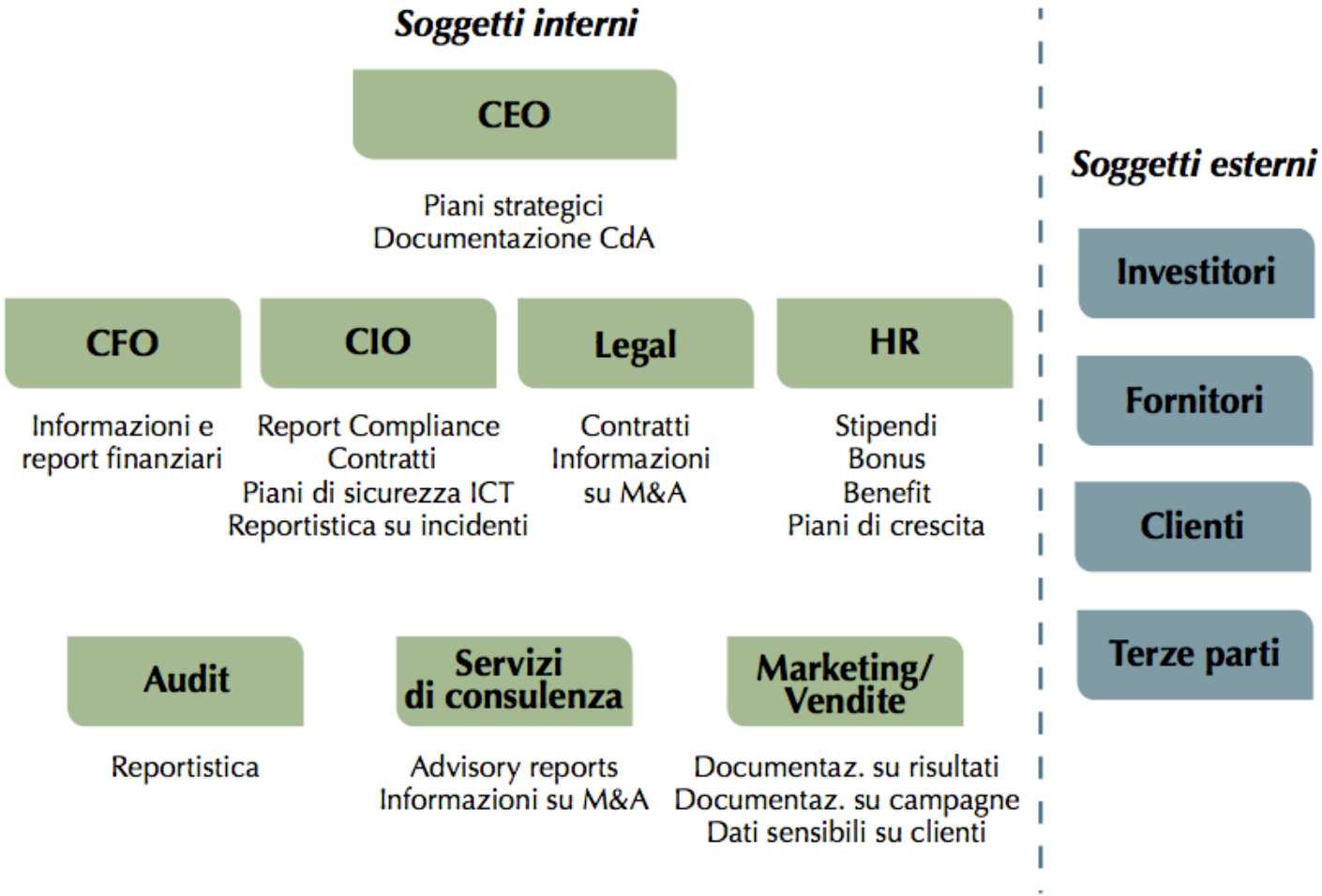
Fonte: Cybersecurity Survey, TIG, aprile 2013. N=115

Conseguenze degli attacchi informatici



Fonte: Cybersecurity Survey, TIG, aprile 2013. N=115

Tipici soggetti target per attacchi e frodi informatiche



Fonte: NetConsulting su fonti varie, 2013

Un lavoratore con buone intenzioni

- Un "**lavoratore dalle buone intenzioni**" è un addetto che ha legittimo accesso alle informazioni ma che espone la società - senza una particolare intenzione - ad un rischio di non rispetto del regolamento sulla sicurezza.

ISY
Information Security easy²
Information Security
Cloud Computing
Internet of things
Risparmio
economico
Cyber Attack
Mobile
Efficienza
Email attachment
Rete aziendale
4G
WEB
Social Media
Processi
Governance
BYOD
Big
Informazioni in crescita esponenziale
Attacco
data
cambiamento
Phishing
Rootkit
Social
Fattore umano
Minaccia
Internet
Engineering
Informatica
ANALISI
Database
Cryptolocker
Recessione economica
Petrolio
C&C Server
target
Conoscenza per prevenire

Information Security

"The weakest link in the security chain is the human element"

Kevin Mitnick

Fattore Umano

Fattore Umano

- Curiosità
- Distrazione
- Ignoranza
- Superficialità
- Manipolazione attraverso un attacco di Social Engineering

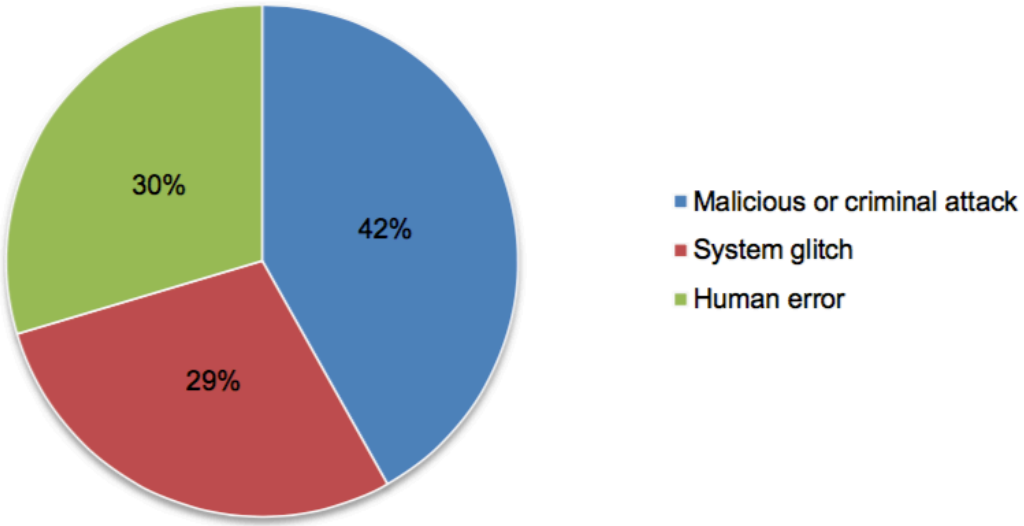
- Sono solo alcuni degli elementi implicati in questo complesso meccanismo e che porta inevitabilmente alla maggiore esposizione al rischio delle informazioni

Quanto conta il fattore umano?

The root causes of data breach

Malicious or criminal attacks are most often the cause of data breach globally.[5] Figure 5 provides a summary of the main root causes of data breach on a consolidated basis for all ten countries represented in the research. Forty-two percent of incidents involved a malicious or criminal attack, 30 percent concerned a negligent employee or contractor (human factor), and 29 percent involved system glitches that includes both IT and business process failures.[6]

Figure 5. Distribution of the benchmark sample by root cause of the data breach
Consolidated view (n=314)



[6] The most common types of malicious or criminal attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection.

Ponemon Institute© Research Report

Fonte: http://www.ibm.com

ISY
Information Security easy²

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology".

Bruce Schneier
(Esperto mondiale di sicurezza informatica)

La sicurezza informatica è costituita da due elementi inscindibili: infrastrutture tecnologiche e comportamenti consapevoli degli operatori.

La nostra proposta è formare il personale che lavora in azienda a partire dalla direzione

Intervenire sul "fattore umano": progetto di formazione

Obiettivo del progetto di formazione è **aiutare le aziende** ad aumentare la **consapevolezza** e la **responsabilità** delle attività svolte quando si trattano le informazioni aziendali e personali.

4 versioni disponibili:

Per lavoratori in generale

Per direzione aziendale

Per studi professionali

Per studenti

A chi è indirizzata la formazione

La formazione è indirizzata a tutti i lavoratori che trattano informazioni verbali, cartacee o attraverso strumenti informatici, e che abbiano necessità di lavorare in **ufficio** o in un **luogo remoto** rispetto all'azienda

Di cosa parliamo

Verranno affrontati argomenti di estrema quotidianità ed attualità per spiegare i possibili problemi nel trattare le informazioni ed **offrire spunti e soluzioni per una loro attenta e consapevole gestione**

Il progetto di **Information Security easY**consiste in una serie di moduli suddivisi per argomenti e viene « vestito su misura » per l'azienda.

Riassumendo

- Le tecnologie sono sempre più numerose e complesse
- Gli attacchi informatici sono sempre più sofisticati, crescenti e mirati
- Il fattore umano è considerato il minimo comun denominatore (distrazione, curiosità, scarsa cultura) per le cause di attacco
- Il gap delle conoscenze necessarie per coadiuvare la prevenzione dei rischi di attacchi informatici aumenta sempre più.

Caratteristiche necessarie al progetto di formazione

- Occorre aiutare il personale d'azienda che tratta informazioni con un progetto di formazione:
  - Diretto, non via e-learning
  - In lingua locale
  - Efficace nel messaggio con esempi chiari e semplici
  - Interattivio nella formazione per chiarire dubbi ed esperienze
  - Raggiunga tutti i livelli aziendali a partire dalla direzione
  - Aggiornato costantemente con le nuove situazioni e rischi più frequenti
  - Reiterato costantemente nel tempo (es 1 volta anno)

@InfoSecEasy

Grazie a tutti per l'attenzione

www.information-security.it

Copyright ©2015 Vito Villa – Tutti i diritti riservati