MOTORE SANITÀ
SICUREZZA E PRIVACY NEL MONDO SANITARIO

Gabriele Faggioli

Milano, 19 giugno 2017

L'emergenza Chiesto un riscatto. A Londra dirottate le ambulanze. In Italia colpita l'università Bicocca

Il grande attacco ai computer

Gli hacker contro ospedali e aziende in 74 Paesi. Il virus rubato agli 007 Usa

Il vertice L'Ocse metterà a punto una proposta entro il 2018

Gli avvertimenti (via Twitter) di Trump all'Fbi

Patto tra ministri del G7 per tassare i giganti web

«Busso al c... eccomi, so...

CONCORDI...

LA SENTENZA

Schettino, ... di condan...

L'EX COMANDANTE

Rapporto CLUSIT 2017

Dall'introduzione

… tale analisi è basata sull'attenta valutazione di tutte le informazioni pubblicamente disponibili in merito a un campione di attacchi "gravi" che, a questo punto, è costituito da **oltre 5.700 incidenti noti avvenuti tra il gennaio 2011 e il dicembre 2016 (dei quali oltre 1.000 nel 2016),** ...

Va sottolineato che le statistiche ed i commenti presentati di **seguito sono relativi a un campione necessariamente limitato**, per quanto ragionevolmente significativo, rispetto al numero degli attacchi informatici gravi effettivamente avvenuti nel periodo in esame.

Questo accade sia perché **la maggior parte delle aggressioni non diventano mai di dominio pubblico**

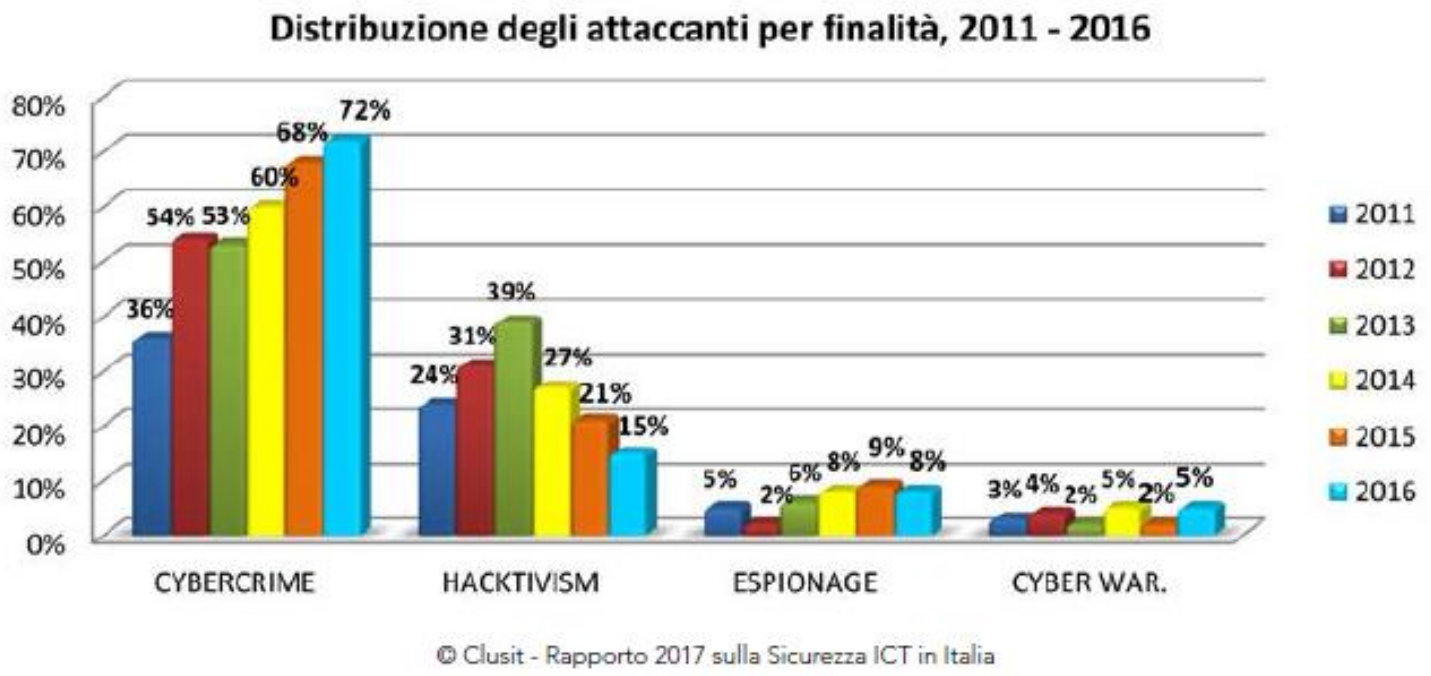
Dalla **edizione 2017** del **Rapporto Clusit**:

- ✓ Il 2016 è stato complessivamente **l'anno peggiore di sempre in termini di evoluzione delle minacce "cyber" e dei relativi impatti, non solo dal punto di vista quantitativo ma anche e soprattutto da quello qualitativo**.
- ✓ la maggior parte delle aggressioni non diventano mai di dominio pubblico
  - **manca ancora una normativa che renda obbligatorio darne notifica**: il GDPR sarà pienamente in vigore solo dal maggio 2018,
  - le **vittime spesso non sono consapevoli di averli subiti**.
- ✓ **Aumento costante della superficie di attacco** complessivamente esposta dalla nostra società digitale:
  - "smart working" sempre più diffuso
  - device IoT, spesso privi delle più elementari misure di sicurezza, non più solo in ambito consumer ma anche in contesti produttivi, (la c.d. Industry 4.0), oppure per applicazioni critiche, (e-health, smart-city, …)

Dalla **edizione 2017** del **Rapporto Clusit**:

- ✓I quadro che emerge dai dati è disastroso e la tendenza generale, se il fenomeno non sarà contrastato con grandissima determinazione, è verso un ulteriore peggioramento.
- ✓**Investimenti in ICT Security che, pur essendo**
  - cresciuti in un anno del 5%
  - sfiorano il miliardo di euro in Italia
- ✓**Investimenti in ICT assolutamente insufficienti**
  - rispetto al valore del mercato di beni e servizi ICT (pari in Italia a 66 miliardi di euro), e soprattutto
  - Rispetto alla percentuale di PIL che oggi viene generato tramite l'applicazione dell'ICT

Rapporto CLUSIT 2017



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Il rischio «cyber» diventa inaccettabile

- ✓ Ciò impone di adottare e attuare dei **piani strategici a livello nazionale**, che coinvolgano l'architettura istituzionale di sicurezza cibernetica;
- ✓ al contrario, negli ultimi tre anni il **divario** tra **percezione** dei **rischi «cyber»** e **realtà**, tra **gravità** di questi **rischi** ed efficacia delle **contromisure** adottate, è **aumentato**;
- ✓ attualmente, dunque, il tema della cybersecurity non è ancora gestito in modo efficace.

Rapporto CLUSIT 2017

Distribuzione delle vittime per tipologia

VITTIME PER TIPOLOGIA	2011	2012	2013	2014	2015	2016	Variazioni 2016 su 2015	Trend 2017
Institutions: Gov - Mil - LEAs - Intel	153	374	402	213	223	220	-1,35%	↘
Other targets	97	194	146	172	51	38	-25,49%	↓
Entertainment / News	76	175	147	77	138	131	-5,07%	↘
Online Services / Cloud	15	136	114	103	187	179	-4,28%	↘
Research - Education	26	104	70	54	82	55	-32,93%	↓
Banking / Finance	17	59	108	50	64	105	64,06%	↑
Software / Hardware Vendor	27	59	46	44	55	56	1,82%	→
Telco	11	19	19	18	18	14	-22,22%	↓
Gov. Contractors / Consulting	18	15	2	13	8	7	-12,50%	↓
Security Industry	17	14	6	2	3	0	-100,00%	↓
Religion	0	14	7	7	5	6	20,00%	↑
Health	10	11	11	32	36	73	102,78%	↑
Chemical / Medical	2	9	1	5	2	0	-100,00%	↓
Critical Infrastructures	-	-	37	13	33	38	15,15%	↑
Automotive	-	-	17	3	5	4	-20,00%	↓
Org / ONG	-	-	19	47	46	13	-71,74%	↓
GDO / Retail	-	-	-	20	17	29	70,59%	↑
Hospitability	-	-	-	-	39	33	-15,38%	↘
Multiple targets (nuova)	-	-	-	-	-	49	-	-

Rispetto al 2015, nel 2016 la crescita percentuale maggiore di attacchi gravi si osserva verso le categorie **“Health” (+102%), “GDO/Retail” (+70%) e “Banking / Finance” (+64%), seguite da “Critical Infrastructures” (+15%).**

L’ampia categoria “Others” risulta in calo, principalmente perché abbiamo dovuto introdurre una nuova categoria, **“Multiple targets”,** per rendere conto del crescente numero di attacchi gravi compiuti in parallelo dallo stesso attaccante contro numerose organizzazioni appartenenti a categorie differenti

Cybersecurity e dati sanitari protetti (PHI)

Le violazioni

La principale causa di violazione è l'**errore umano**.

MODALITA' DI VIOLAZIONE:

- Furto o perdita di dispositivi portatili (es. laptop, tablet e chiavette USB)
- Errore umano (es. invio di un referto medico al destinatario sbagliato)
- Uso improprio di privilegi da parte di un dipendente per accedere a informazioni sensibili

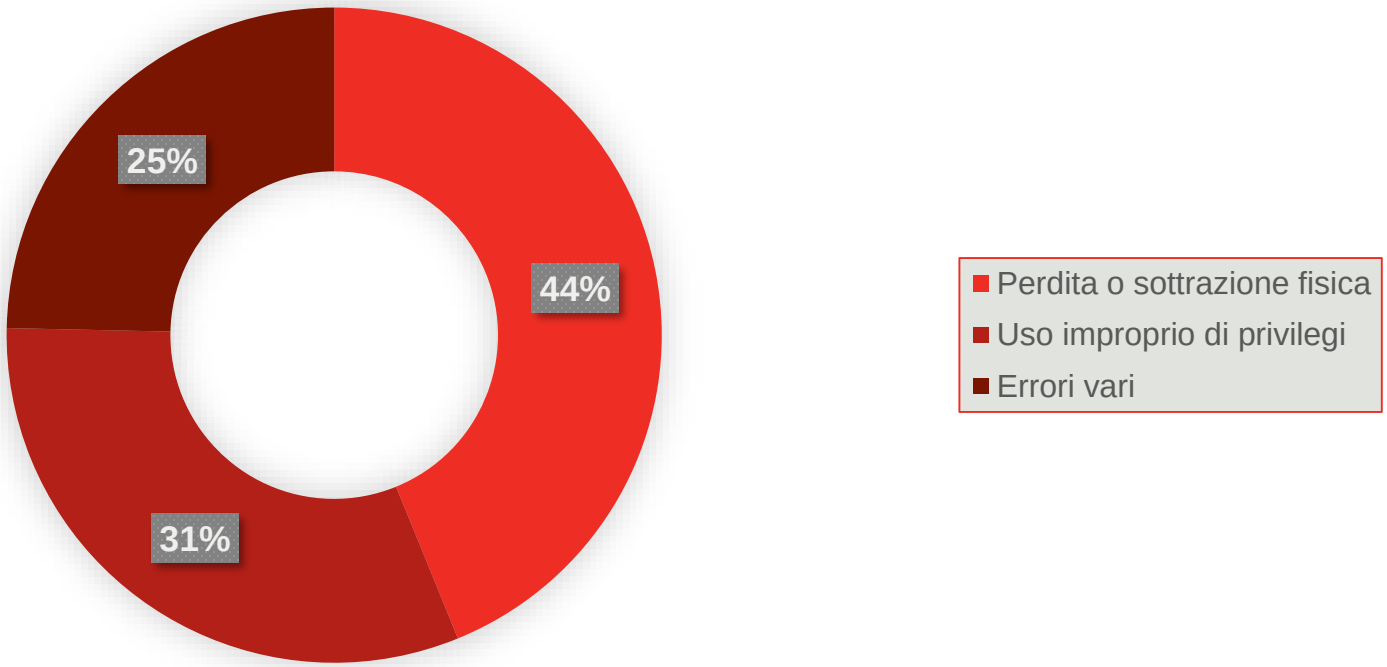
Tali modalità costituiscono l'**86%** delle violazioni di dati sensibili

Fonte: Verizon

Attacchi nel mondo sanitario

Esistono tre differenti **tipologie di attacco** nel mondo sanitario:

Rappresentano il 73% degli attacchi totali, suddiviso in:



Fonte: Verizon Data Breach Investigation Report

Attacchi nel mondo sanitario: malware

All'interno della Pubblica Amministrazione, la Sanità, è stata quella che ha registrato il maggior numero di attacchi ransomware negli ultimi anni.

COME CONTRASTARLI?

Attraverso lo sviluppo di programmi di awareness mirati per gli utilizzatori dei sistemi informativi della PA in aggiunta ad efficaci misure di sicurezza.

AGENZIA DIGITALE ITALIANA

L'AgID ha pubblicato nel 2016 un documento che contiene le "Misure minime di sicurezza ICT per la Pubblica Amministrazione" (parte integrante delle Linee Guida per la Sicurezza).

Come proteggere i dati: raccomandazioni

Alcune raccomandazioni per proteggere al meglio i propri dati:

- Approfondita conoscenza delle comuni tipologie di attacco
- Autenticazione a due fattori
- Applicazione tempestiva delle patch
- Restringere e controllare gli accessi
- Monitorare i log
- Crittografare i dati
- Incrementare la formazione del personale in merito all'argomento

CONOSCERE I DATI – PROTEGGERLI MEGLIO

Fonte: Verizon

Come proteggere i dati: aspetti

Gli interventi non si limitano alla sfera tecnologica, ma si riferiscono ad una **serie di aspetti**:

- Organizzativi
- Culturali
- Tecnologici
- Economici

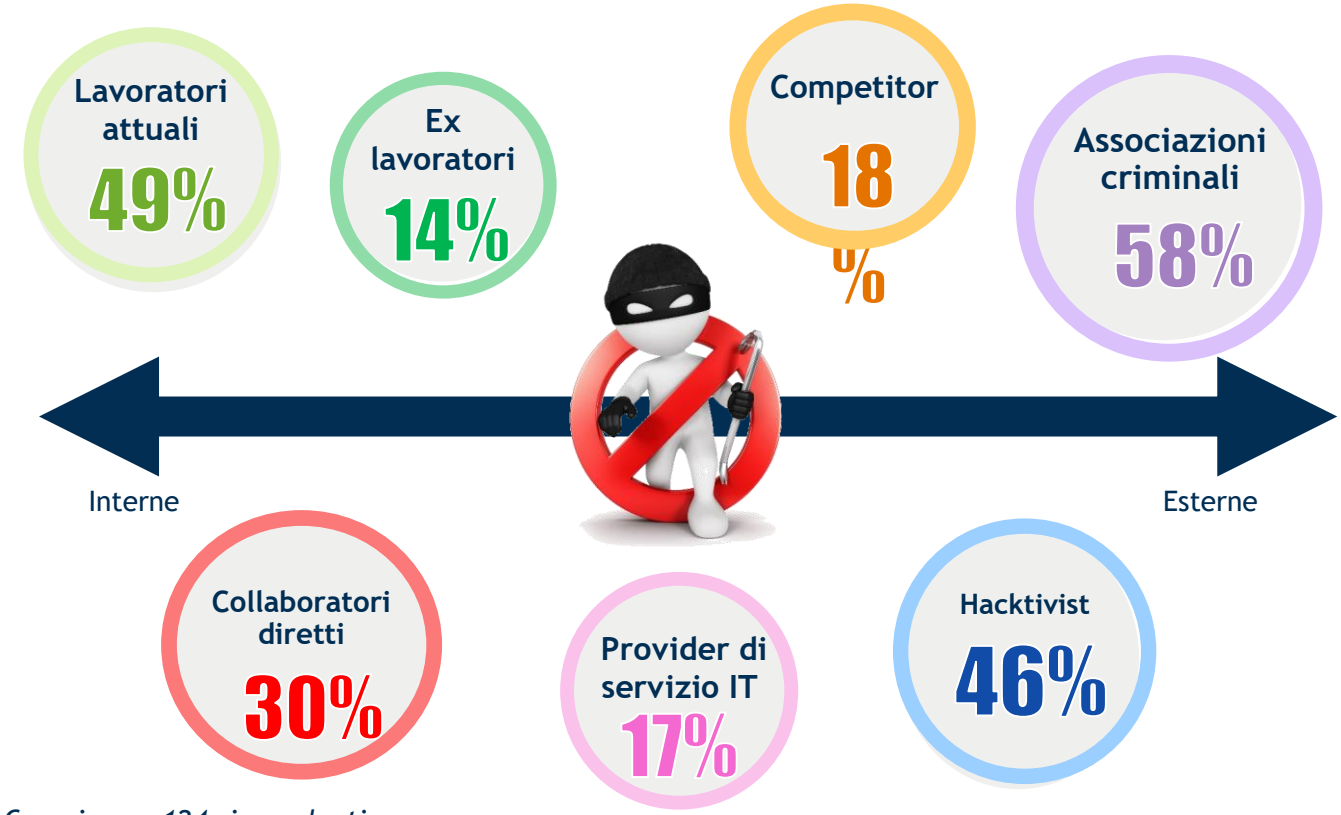
Punto di partenza è la concezione di fondo, per cui

Fonte: Aisis

Osservatorio Sicurezza e Privacy
Politecnico di Milano
Le imprese italiane e la sicurezza

Ricerca del 2016 - *Campione : 124 rispondenti*

Osservatorio Politecnico di Milano



Campione : 124 rispondenti

Osservatorio Politecnico di Milano

78%

Inconsapevolezza rispetto alle policy aziendali

56%

Distrazione delle persone

47%

Accesso in mobilità alle informazioni

33%

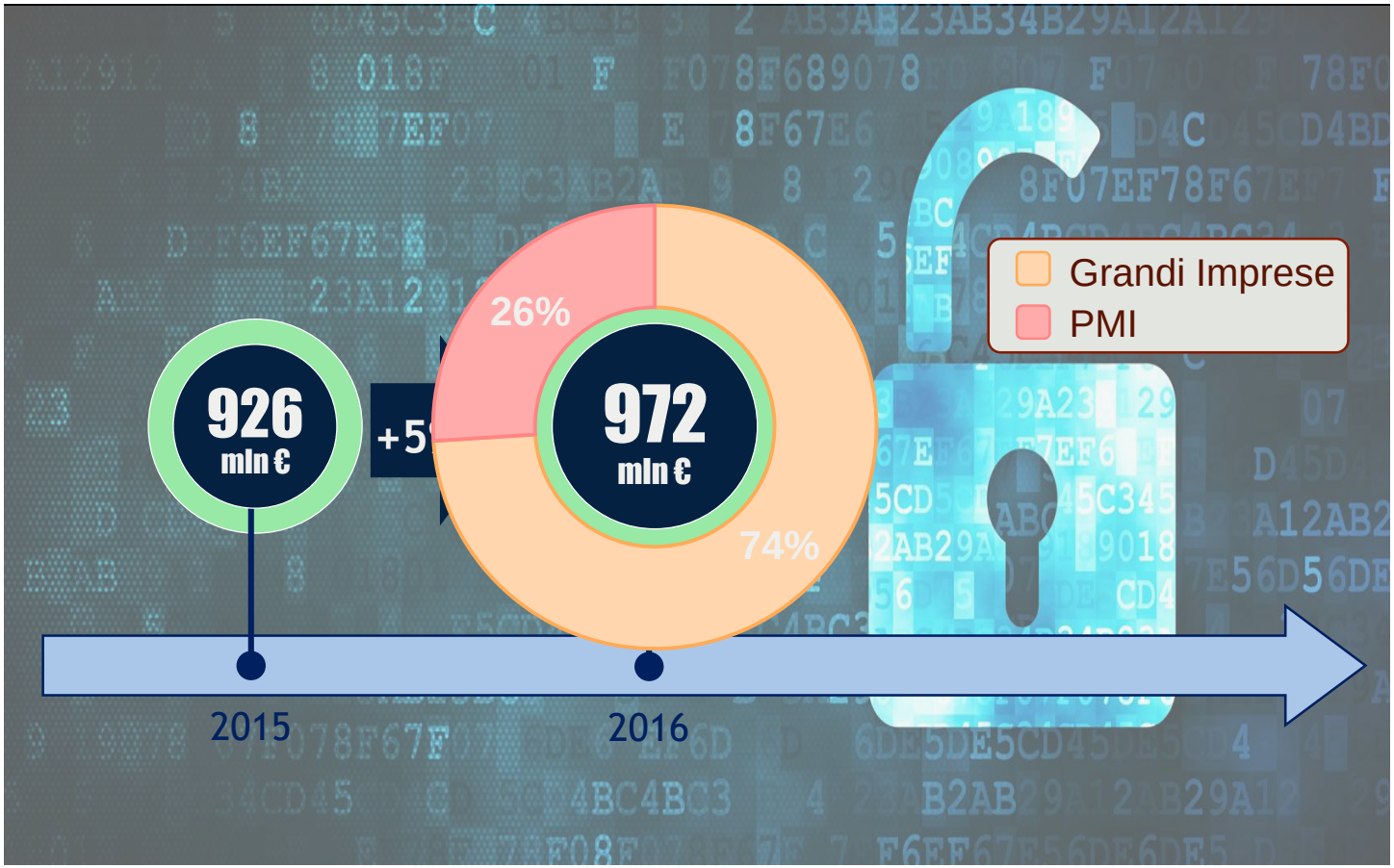
Presenza di device mobile personali (BYOD)

18%

Architettura IT obsoleta

Campione : 125 rispondenti

LA MATURITÀ DELLE IMPRESE E LO SCENARIO DI MERCATO
IL MERCATO DELLA SECURITY: CRESCE PERÒ…



ART. 24: RESPONSABILITÀ DEL TITOLARE

Responsabilità del titolare (Accountability)

Art. 24

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche il **titolare mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare**, che il trattamento è effettuato conformemente alla legge.

Responsabilità di titolare e responsabile

Art. 82 c. 2

Un **titolare** del trattamento coinvolto nel trattamento **risponde** per il **danno** cagionato dal suo trattamento che **violi il presente regolamento**.

Un **responsabile** del trattamento risponde per il danno causato dal trattamento **solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili** del trattamento **o** ha **agito in modo difforme o contrario rispetto alle** legittime **istruzioni del titolare** del trattamento.

Responsabilità solidale di titolari e responsabili

Art. 82 c. 4

Qualora **più titolari del trattamento o responsabili** del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano **coinvolti nello stesso trattamento** e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, **ogni titolare del trattamento o responsabile del trattamento è responsabile in solido** per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

Responsabilità dei contitolari

Art. 26

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi **determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità**.

Grazie!

gabriele.faggioli@p4i.it