Tutti in Difesa!

E si salvi chi può

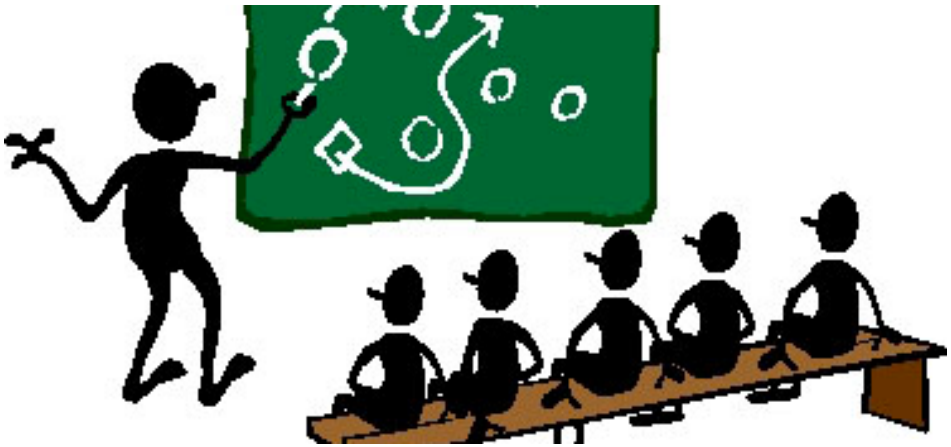
Luca Spalazzi

Dipartimento di Ingegneria dell'Informazione

cini Cyber Security National Lab

Gruppo Ingegneria Informatica @UNIVPM GII

Tuti indrìo e si salvi chi può!
Nereo Rocco



Sommario

- Strumenti di difesa
- Il fattore umano è una delle principali cause di un attacco
  - Situazione nel mondo e in Italia
  - 4 casi embematici

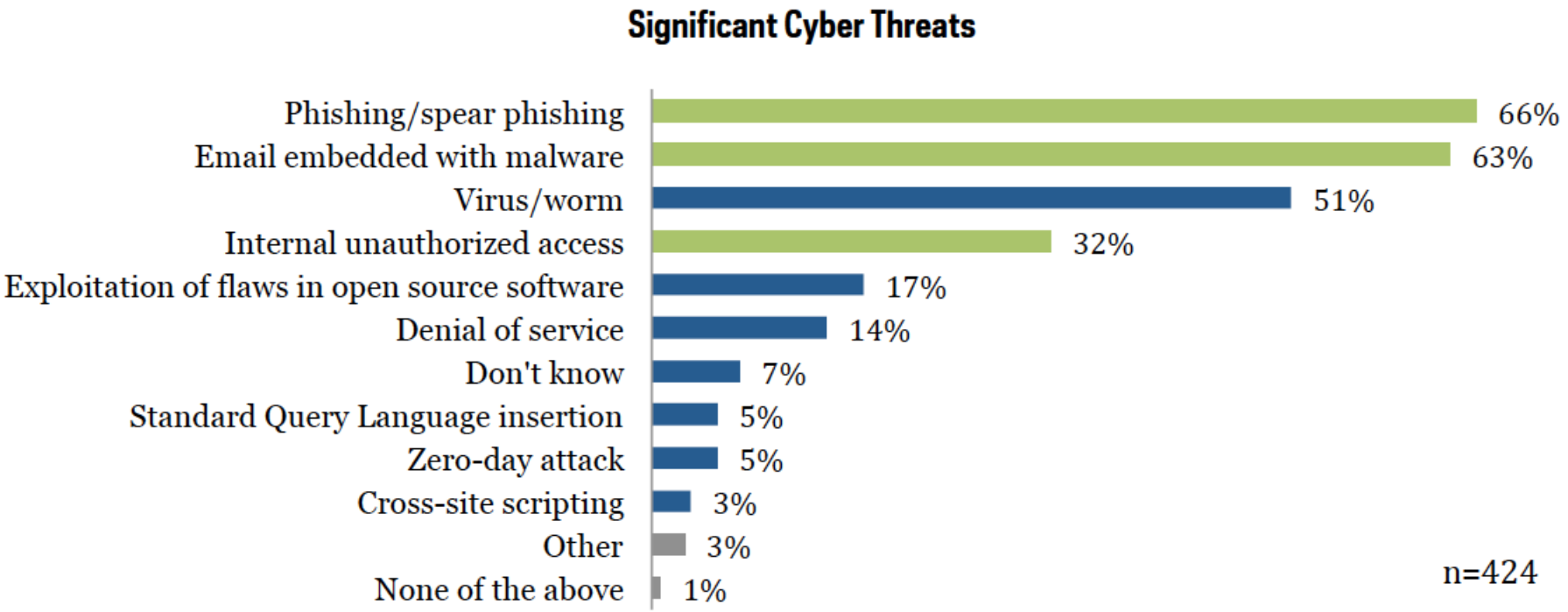
Strumenti di difesa

- Isolamento
  - Impedire ad un programma di accedere alle interfacce associate all'esecuzione di un altro
    - Isolamento fisico, macchine virtuali, …
- Monitoraggio
  - Garantire ad un programma la possibilità di controllare ed eventualmente bloccare l'esecuzione di un certo insieme di operazioni
    - Reference monitor (istruzioni privilegiate, firewall, …) IDS/IPS, antimalware, …
- Offuscamento
  - Informazioni che possono essere comprese solo conoscendo un segreto
    - Crittografia, …

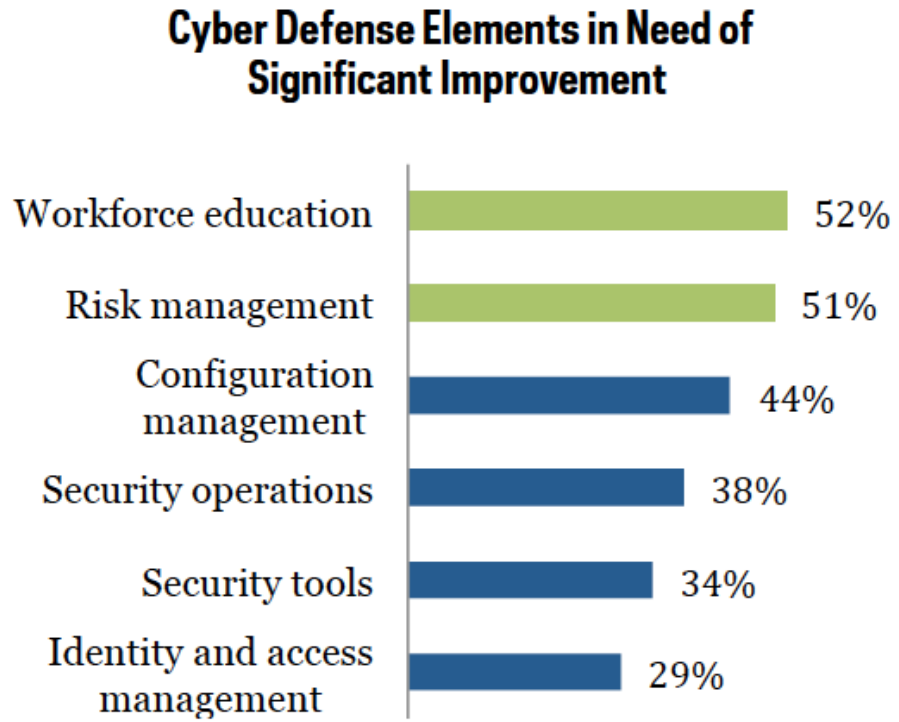
Cause di un attacco

- Difetti di specifica e progettazione
  - Non sono stati considerati tutti i requisiti di sicurezza.
  - Il progetto non è conforme alle specifiche di sicurezza.
- Difetti di realizzazione e configurazione
  - Il sistema non è conforme al progetto.
  - Il sistema è configurato male
- Difetti di utilizzo
  - Il sistema è utilizzato male ➡ Il fattore umano!!!

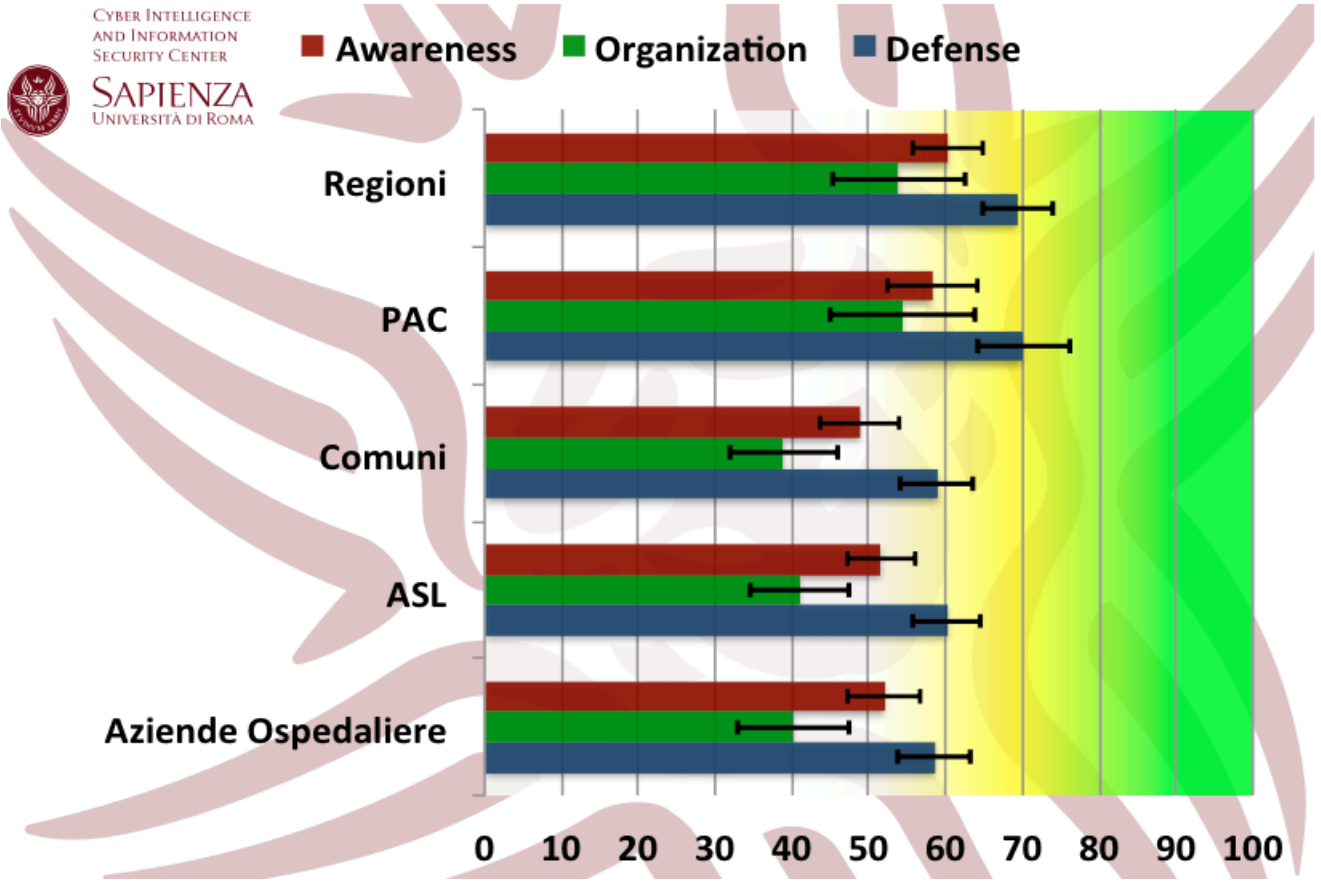
Government Business Council & Dell Software - The human factor at the core of Federal Cybersecurity



Government Business Council & Dell Software - The human factor at the core of Federal Cybersecurity



CIS Sapienza – 2014 Italian Cyber Security Report



CIS Sapienza – 2014 Italian Cyber Security Report

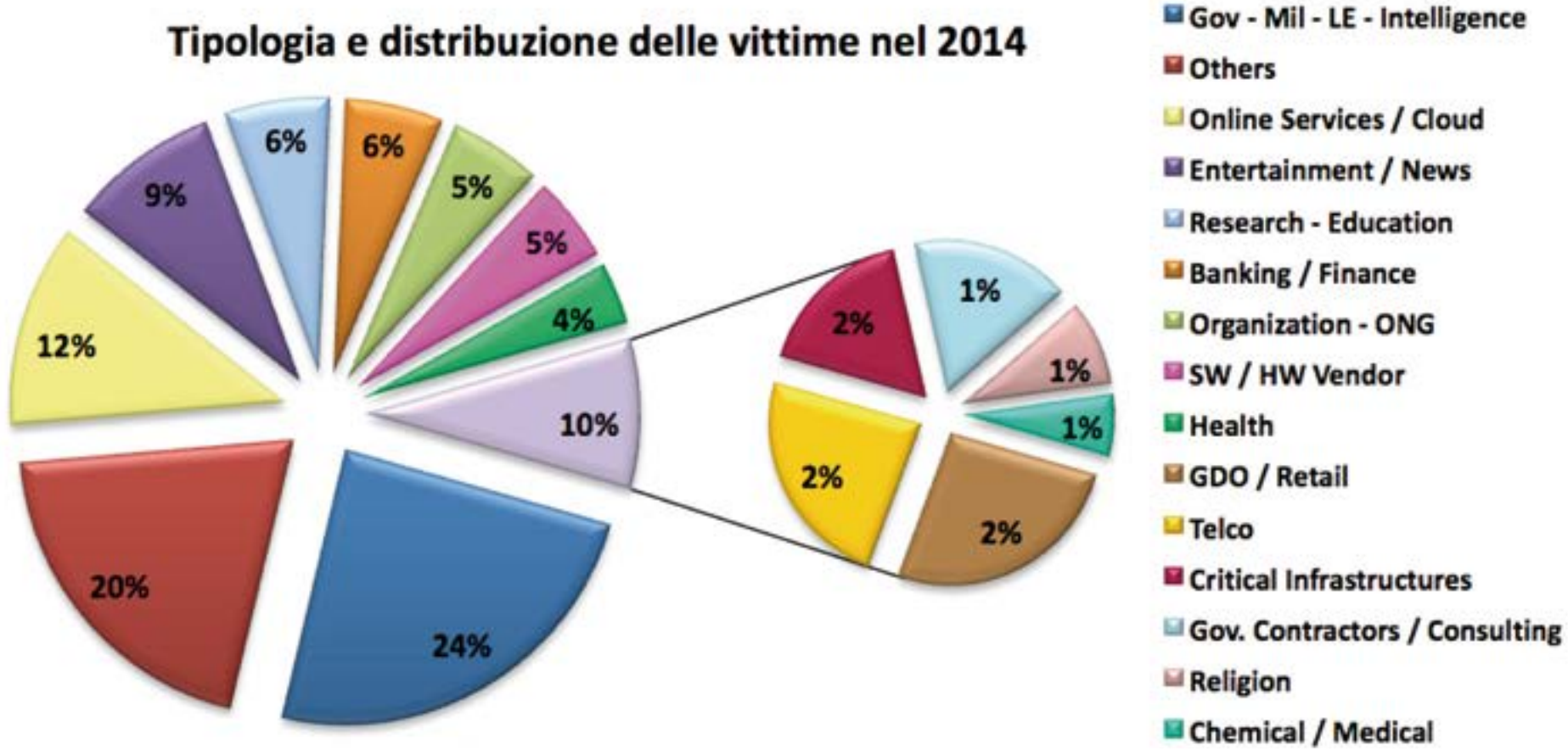
Alcune pratiche comunemente ignorate

- Risk assessment
- Piano di risposta – Piano di sicurezza
- Sistema di gestione della sicurezza delle informazioni (ISMS)
- Sistemi di controllo degli accessi fisici ai locali
- Attività di Penetration Testing, Vulnerability Assessment and Mitigation, verifiche periodiche

Clusit – Rapporto 2015 sulla Sicurezza ICT in Italia

TECNICHE DI ATTACCO	2011	2012	2013	2014	Variazioni 2012 su 2011	Variazioni 2013 su 2012	Variazioni 2014 su 2013	Variazioni 2014 su 2011	Trend 2015
SQL Injection	197	435	217	110	120,81%	-50,11%	-49,31%	-44,16%	↓
Unknown	73	294	239	198	302,74%	-18,71%	-17,15%	171,23%	↑
DDoS	27	165	191	81	511,11%	15,76%	-57,59%	200,00%	→
Vulnerabilità note	107	142	256	195	32,71%	80,28%	-23,83%	82,24%	→
Malware	34	61	57	127	79,41%	-6,56%	122,81%	273,53%	↑
Account Hijacking / Theft	10	41	115	86	310,00%	180,49%	-25,22%	760,00%	↑
Phishing / Social Engineering	10	21	3	4	110,00%	-85,71%	33,33%	-60,00%	→
Multiple Techniques / APT	6	13	71	60	116,67%	446,15%	-15,49%	900,00%	↑
0-day	5	8	3	8	60,00%	-62,50%	166,67%	60,00%	→
Phone Hacking	0	3	0	3	-	-	-	-	↓

Clusit – Rapporto 2015 sulla Sicurezza ICT in Italia



NASA 2008

- Stazione Spaziale Orbitante.
  - Un 'incauto' astronauta avrebbe utilizzato una sua chiavetta USB personale.
  - Conteneva un virus per videogiochi.
  - Per fortuna non ha provocato danni.

JP Morgan Chase

- Nota banca americana
  - Il punto di attacco iniziale è stato un server poco usato e quindi trascurato (vulnerabile) utilizzato come “trampolino di lancio” per portare attacchi a sistemi interni sensibili.
  - Ha causato la sottrazione di circa 79 milioni di record relativi ai propri clienti .

Home Depot

- Grande catena di negozi di bricolage
  - Ha disattivato un sistema di sicurezza.
  - Furto di 56 milioni di carte di credito / debito, per un danno di centinaia di milioni di dollari.

Target

- Catena di supermercati
  - Non ha reagito tempestivamente alla segnalazione di un attacco in corso inviata dal proprio SOC di Bangalore .
  - Sottratti circa 40 milioni di carte di credito dai POS dei punti vendita.
  - Perdite stimate di circa un miliardo di dollari .


UNIVPM
Università Politecnica delle Marche
감사합니다
Natick
شكرا
Grazie
Danke
Ευχαριστίες
Dalu
Obrigado
Thank You
Köszönöm
Tack
Спасибо
Dank
Gracias
Seé
谢谢
Merci
ありがとう