PA digitale e cybersecurity

Un approccio sostenibile per le misure minime di sicurezza nelle Università

SAPIENZA
UNIVERSITÀ DI ROMA

2017 FORUM PA

Leonardo Querzoni
Centro di ricerca in Cyber Intelligence and Information Security

Giuseppe Arrabito
Centro Infosapienza

Il Cyberspazio e la sua evoluzione

Dagli anni ’90 ad oggi il Cyberspazio è evoluto profondamente

- Da semplice rete di interconnessione di computer a mercato economico fondamentale.
- Da semplice rete di computer a medium di comunicazione globale

Proteggere il cyberspazio è oggi una priorità globale ed una responsabilità di ogni singola nazione

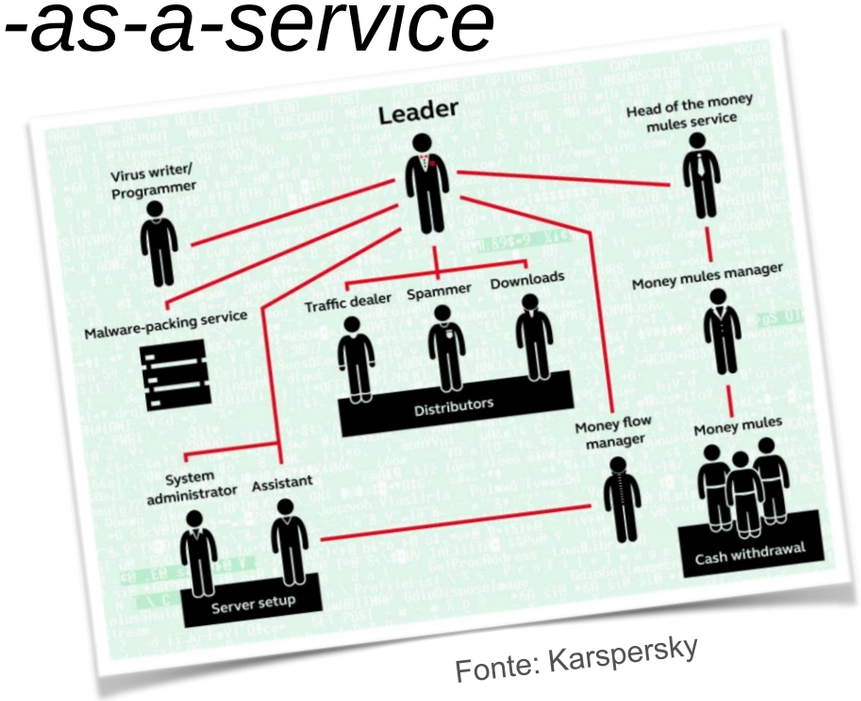
Più opportunità = Più minacce

Di pari passo anche le attività criminali su internet si sono evolute

- 1990: attacchi dimostrativi, esperimenti, danni spesso limitati
- 2000: internet boom e prima monetizzazione degli attacchi
- 2010: strutture criminali organizzate e specializzate

Oggi si realizza la visione del *Crime-as-a-service*

- Servizi accessibili e ben strutturati
- Maggiore concorrenza = costi ridotti
- Organizzazioni trans-nazionali



Fonte: Karspersky

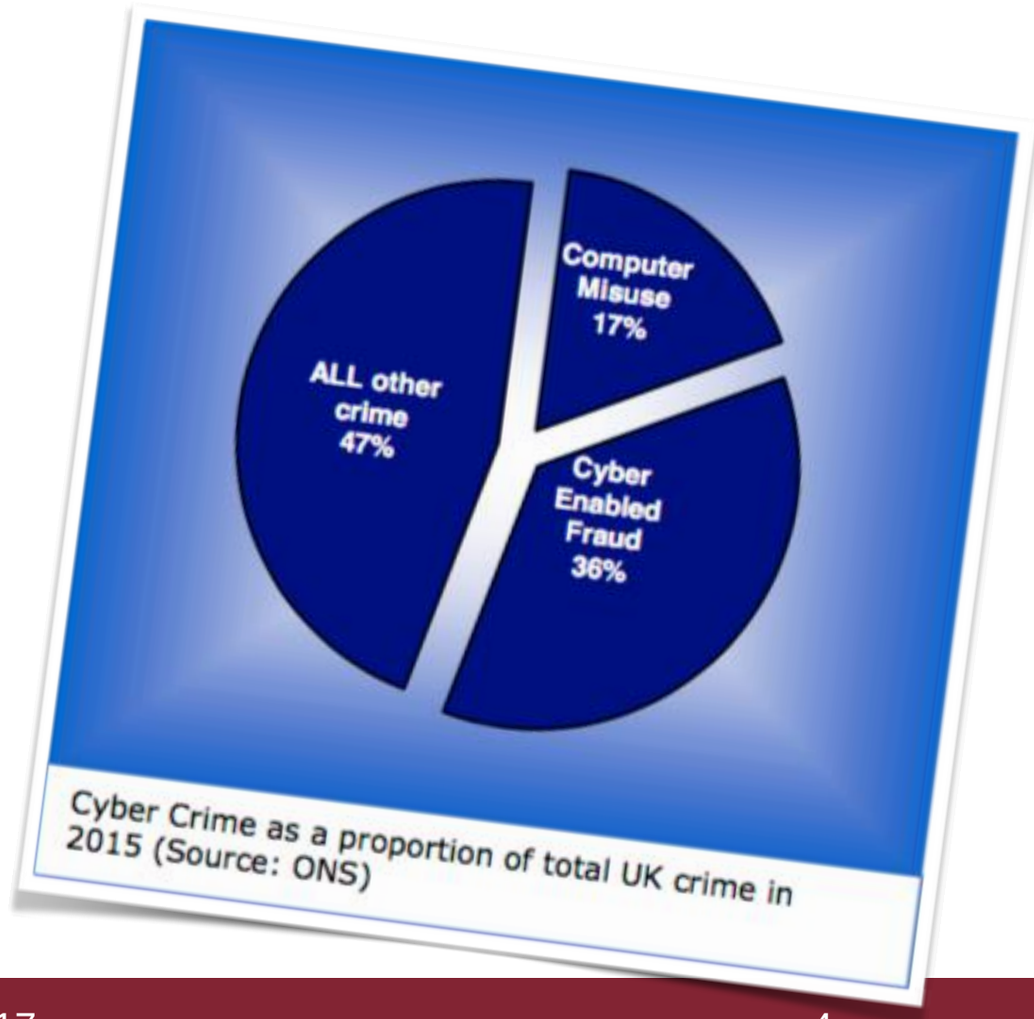
Più opportunità = Più minacce

Di pari passo anche le attività criminali su internet si sono evolute

- In UK nel 2015 il numero di crimini legati al cyberspazio ha superato i crimini avvenuti nel mondo fisico (fonte: *National Crime Agency*, Luglio 2016)

La barriera di ingresso per diventare cybercriminali è bassa

Prima erano necessarie le competenze, oggi è sufficiente il denaro



Sicurezza, attacchi ed asimmetria

Quante probabilità ci sono che un ladro usi un carro armato per rubare qualche soldo da una villetta?

Nel cyberspazio software malevolo di incredibile complessità è alla portata del singolo criminale con sufficienti risorse

- Costo per l'uso di un exploit kit (es. Angler) per un mese: ~5.000$
- Uso esclusivo di un exploit 0-day: 10.000$ - 700.000$
- Costo per l'uso di tecnologia dell'NSA: 0$ (!!!)

Il Centro di ricerca CIS

CIS - Centro di ricerca in cyber intelligence ed information security

- Nasce nel 2012 come polo di aggregazione delle competenze in ambito cyber
  - Economia, Legge, Ingegneria, Informatica, Statistica
  - Più di 60 docenti, centinaia tra studenti di dottorato e post-doc
- Centro multidisciplinare per la ricerca su:
  - cyber security
  - cyber intelligence
  - sicurezza delle infrastrutture critiche
  - smart systems e IoT

Il Centro di ricerca CIS

Dipartimento
Informazioni per
la sicurezza

IBM

sogei

LEONARDO

TELECOM

MEF
Ministero
dell'Economia
e delle Finanze

enel

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

eni

Agenzia per l'Italia Digitale
Gestione ex-DigitPA

VITROCISET

acea

Microsoft

CISCO

MBDA

Laboratorio Nazionale di Cyber Security

Laboratorio Nazionale di Cyber Security - CINI

- Istituito nel 2014 dal Consorzio Interuniversitario Nazionale per l'Informatica
- Obiettivi
  - Diventare attore del processo di implementazione della strategia nazionale per la Cyber Security
  - Supportare le organizzazioni diffuse sul territorio nazionale perché diventino maggiormente resilienti rispetto al rischio cyber
  - Definizione di standard e metodologie nazionali
  - Rappresentare il punto di riferimento nazionale per l'implementazione di progetti allo stato dell'arte nell'ambito della cyber security
- 250 docenti afferenti a 34 Università e centri di ricerca sparsi su tutto il territorio

cini
Cyber Security National Lab

Laboratorio Nazionale di Cyber Security

Framework Nazionale - Vision

Big Data

Smart Cities

IoT

Industry 4.0

Robotica

Moneta elettronica

Agricoltura 4.0

Droni

Framework Nazionale - Vision

Economia

Cyberspace

La protezione del cyberspace è condizione necessaria per la prosperità economica di una nazione

Framework Nazionale - Vision

Economia

Cyberspace

La protezione del cyberspace non è soltanto un problema tecnico

Framework Nazionale - Obiettivi

1 — Portare il **rischio cyber** sui tavoli dei consigli di amministrazione

2 — Approcciare il rischio cyber come un **rischio economico**

3 — Creare un framework adatto al **contesto italiano**

4 — Conforme con altri **standard internazionali**

Dal NIST al Framework Nazionale

Framework core
- Function
- Categories
- Subcategories

Profili

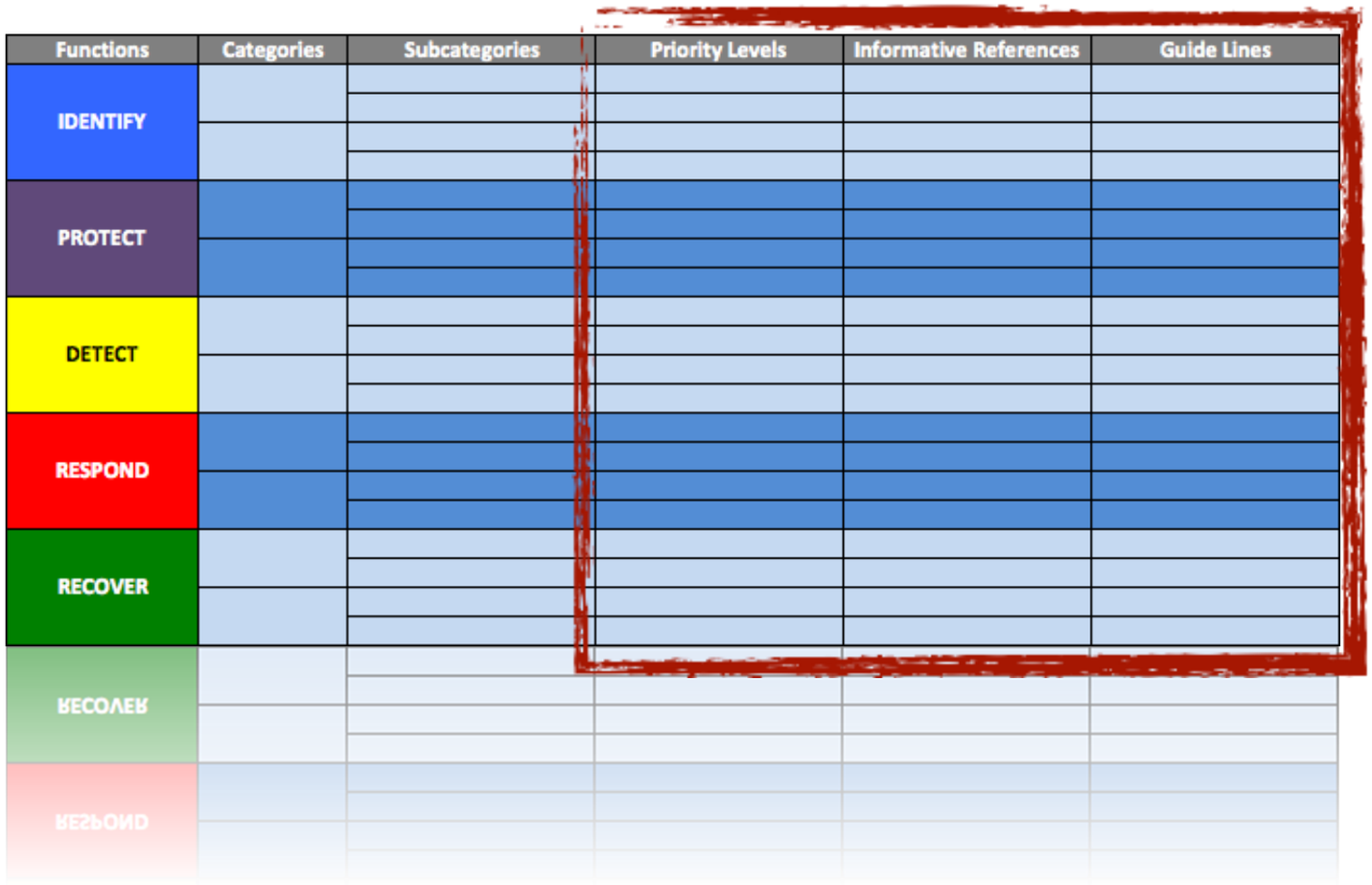
Implementation tiers

Livelli di priorità

Livelli di maturità

Riferimenti normativi

Linee guida per l'implementazione



Vantaggi per la nazione

Fornire un linguaggio comune a diversi soggetti per poter emanare regole in maniera coerente (es.: Garante Privacy, AGID, PCM, ecc.)

Facilita la *due diligence* internazionale

Abilita una valutazione complessiva dell'esposizione nazionale al rischio cyber

Il framework può rappresentare un "linguaggio" comune
a tutta la nazione nel dominio della cyber security

E le pubbliche amministrazioni?

La PA è un obiettivo privilegiato da parte di diversi tipi di criminali

- 2014 - attacco ransomware ai comuni italiani (phishing)
- 2015 - 21 milioni di record associati a dipendenti delle pubbliche amministrazioni USA vengono trafugati dall'Office of Personnel Management (state attack?)
- 2015 - 700.000 cartelle fiscali di cittadini americani vengono trafugati (cattiva progettazione del software)

E le pubbliche amministrazioni?

Il framework nazionale viene mappato con le recenti **Misure minime di sicurezza informatica per le PA** pubblicate il 26/9/2016

(fonte: sito web AgID)

Nella terza colonna, "FNSC" (Fra
l'identificatore della Subcategory d
Security, proposto con il 2015 Italia
scorso 4 febbraio 2016, al quale il
contestualizzazione del Framework,
tanti ed efficaci azioni che questo g
ed il differente obiettivo che i due
l'accento sopra gli aspetti di prevenz

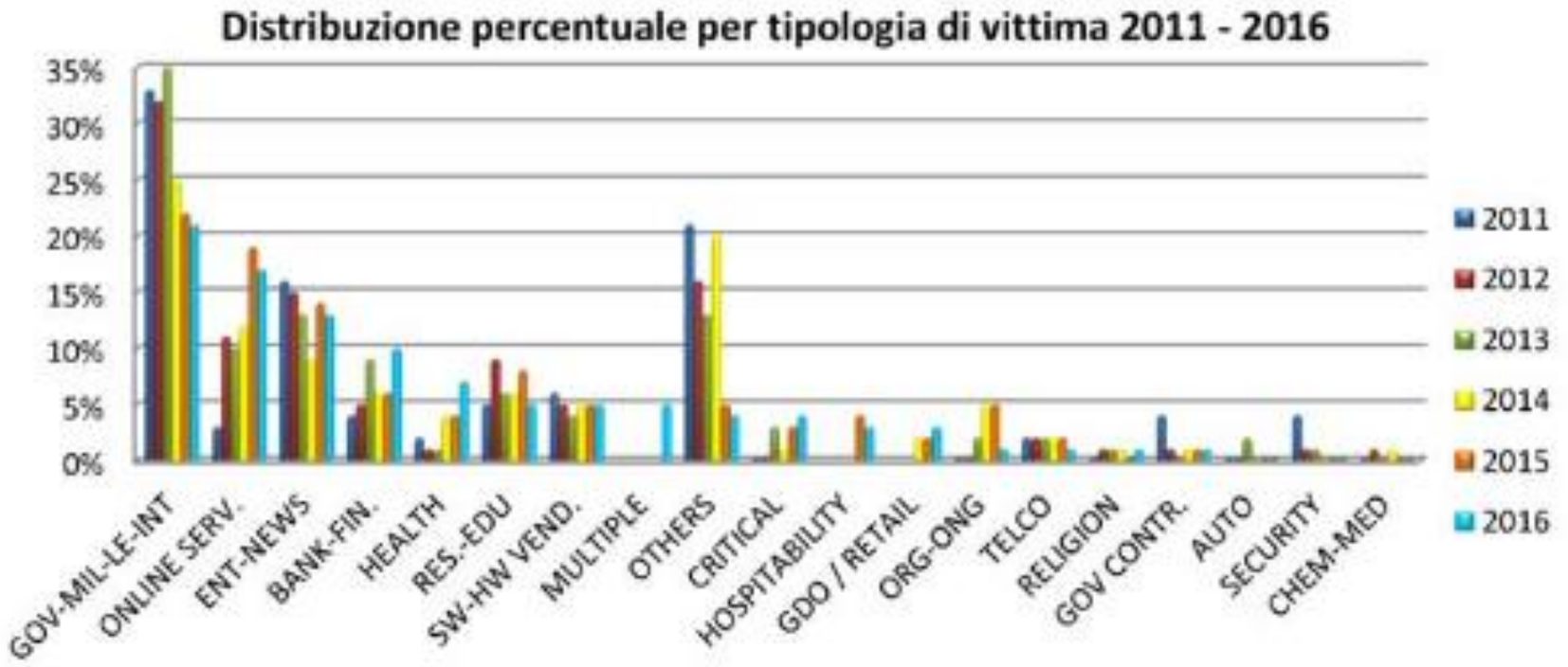
ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
3	1	1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	PR.IP-1	X	X	X
		2	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	PR.IP-1		X	X
		3	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	PR.IP-2 RC.IM-1			X
	2	1	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	PR.IP-1	X	X	X
		2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	PR.IP-2 RC.RP-1	X	X	X
		3	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	PR.IP-3		X	X
	3	1	Le immagini d'installazione devono essere memorizzate offline.	PR.IP-2	X	X	X
		2	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	PR.DS-2 PR.IP-2		X	X
	4	1	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	PR.AC-3 PR.MA-2	X	X	X

Lo scenario attuale

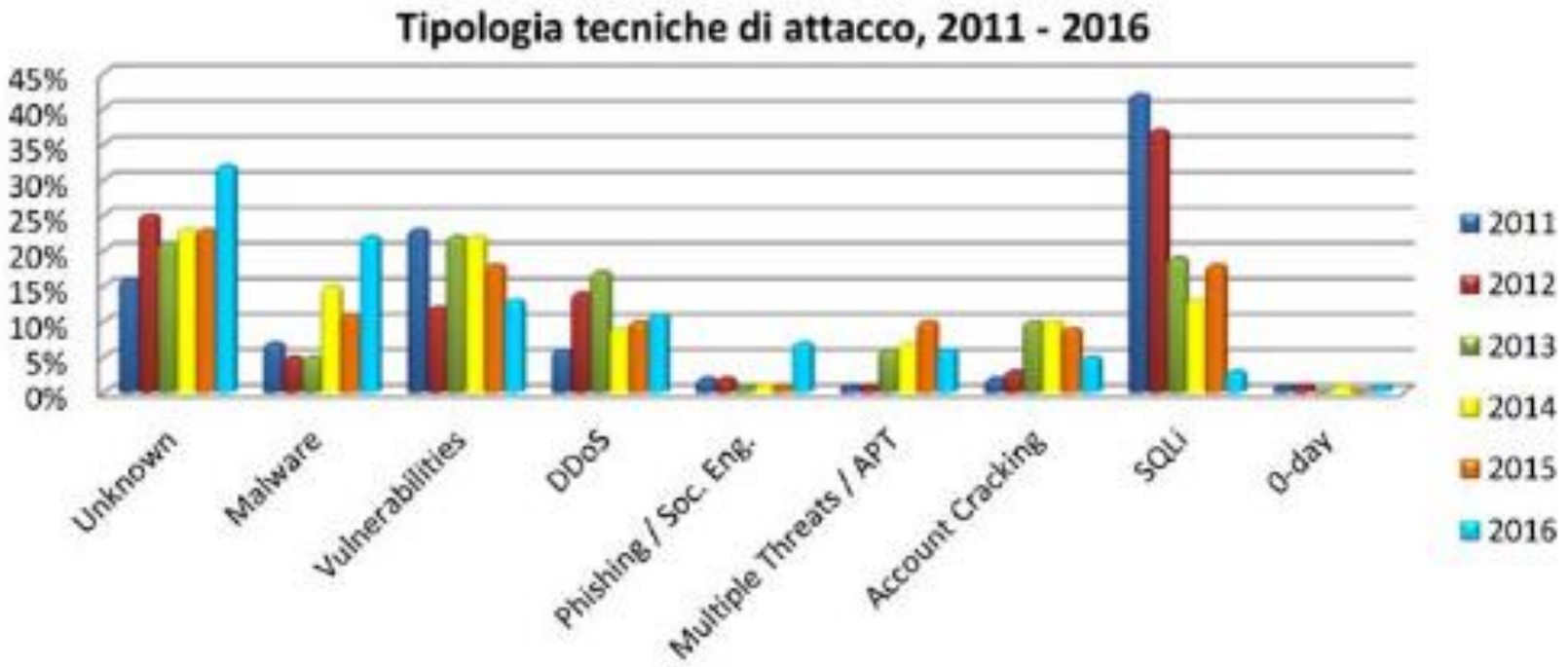
2016 l'anno peggiore di sempre in termini di evoluzione delle minacce "cyber"



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Lo scenario attuale

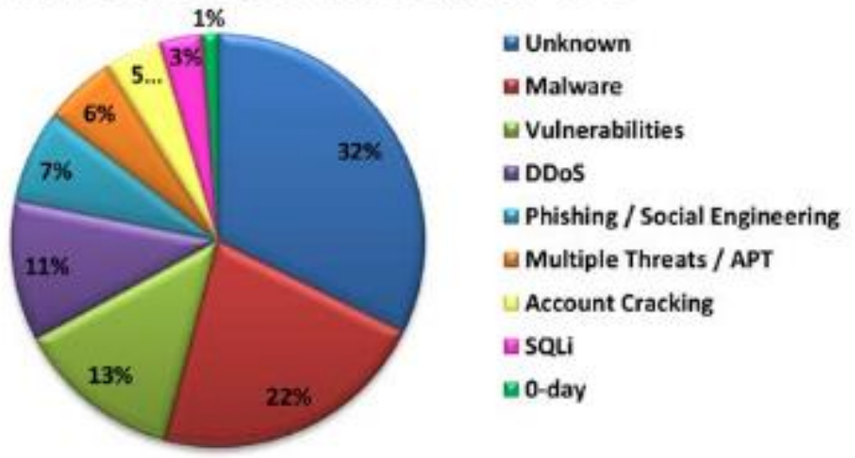
2016 l'anno peggiore di sempre in termini di evoluzione delle minacce "cyber"



Lo scenario attuale: le vittime illustri

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	-	-

Tipologia e distribuzione delle tecniche d'attacco - 2016



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Il quadro normativo per la PA

Con l'avvenuta pubblicazione in Gazzetta Ufficiale (Serie Generale n.103 del 5-5-2017) della Circolare 18 aprile 2017, n. 2/2017, recante «**Misure minime di sicurezza ICT per le pubbliche amministrazioni**. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)», le Misure minime sono ora divenute di obbligatoria adozione per tutte le Amministrazioni.
Scadenza 31/12/2017

AGID Misure minime di sicurezza

Il **regolamento generale sulla protezione dei dati** (GDPR, *General Data Protection Regulation-Regolamento UE 2016/679)* è un Regolamento con il quale la Commissione europea intende rafforzare e unificare la protezione dei dati personali entro i confini dell'Unione europea). **Applicabile dal 24/05/2018**

GDPR

Il nuovo CAD. Con la pubblicazione sulla Gazzetta Ufficiale n. 214 del **13 settembre 2016**, il decreto legislativo 26 agosto 2016, n. 179 recante *Modifiche ed integrazioni al Codice dell'amministrazione digitale, in materia di riorganizzazione delle amministrazioni pubbliche*, entra in vigore oggi, 14 settembre 2016

Codice Amministrazione Digitale

DPCM 17 febbraio 2017
Decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017
Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali
(pubblicato sulla GU n. 87 del 13/4/2017)

Strategia nazionale e piano di cybersecurity

I possibili rischi per l’Ateneo

- Rischio di perdita di disponibilità, integrità e confidenzialità delle informazioni e dei dati: violazioni informatiche
- Rischio di sanzioni amministrative e penali: perdite economiche
- Rischio reputazionale: danno all’immagine
- Perdita di fiducia degli utenti nell’utilizzo delle tecnologie informatiche e nell’innovazione digitale: possibile calo di nuove iscrizioni

IL DANNO DI IMMAGINE

«…consiste nella considerazione e nella credibilità di cui il soggetto gode nella società e ne costituisce il primo driver di valore….»
[Corradini, Nardelli 2013]

Le misure minime di sicurezza - AGID

CIRCOLARE 17 marzo 2017, n. 1/2017
Misure minime di sicurezza ICT per le pubbliche amministrazioni. *(Direttiva del PDCM 1/08/2015). (17A02399)* *(GU Serie Generale n.79 del 04-04-2017)*

Obiettivo della presente circolare è indicare alle pubbliche amministrazioni **le misure minime per la sicurezza ICT che debbono essere adottare al fine di contrastare le minacce più comuni** e frequenti cui sono soggetti i loro sistemi informativi.

Ai sensi dell'art. 3 della Circolare citata, "**il responsabile dei sistemi informativi** di cui all'art. 10 del decreto legislativo 12 febbraio 1993, n. 39, ovvero, in sua assenza, il **dirigente allo scopo designato**, ha la responsabilità della attuazione delle misure minime di cui all'art. 1".

Obbligo per le pubbliche amministrazioni, in ossequio a quanto previsto al successivo art. 5 della Circolare, entro il **31 dicembre 2017** dovranno attuare gli adempimenti necessari ed uniformarsi.

Le misure minime di sicurezza - AGID

- Tali misure, il cui rispetto è richiesto a tutte le PA, prevedono **tre livelli di attuazione: minimo, standard e alto:**

I livelli successivi rappresentano situazioni evolutive in grado di fornire livelli di protezione più completi, e dovrebbero essere adottati fin da subito dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati) ma anche visti come obiettivi di miglioramento da parte di tutte le altre organizzazioni.

- Fra le misure minime è previsto anche che le pubbliche amministrazioni accedano sistematicamente a **servizi di early warning** che consentano loro di rimanere aggiornate sulle nuove vulnerabilità di sicurezza. A tal proposito il CERT-PA fornisce servizi proattivi ed informativi a tutte le amministrazioni accreditate.

- Le misure minime di sicurezza ICT- che costituiscono parte integrante del più ampio disegno delle Regole Tecniche per la sicurezza informatica della Pubblica Amministrazione di futura emanazione

Le misure minime di sicurezza – i controlli

AgID Basic Security Control(s) (ABSC) sono un estratto di 5 dei 20 Critical Security Check (CSC) del SANS Institute

Tipologia	Descrizione
ABSC1 (CSC1)	INVENTARIO DEI DISPOSITIVI AUTORIZZATI
ABSC2 (CSC2)	INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI
ABSC3 (CSC3)	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER
ABSC4 (CSC4)	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ
ABSC5 (CSC5)	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE
ABSC8 (CSC8)	DIFESE CONTRO I MALWARE
ABSC10 (CSC10)	COPIE DI SICUREZZA
ABSC13 (CSC13)	PROTEZIONE DEI DATI

Le misure minime di sicurezza: le criticità per le Università

- Pubblicazione e periodo di applicabilità
- Criticità legate al contesto accademico
- Sostenibilità delle contromisure: budget di previsione già redatti
- Gruppo di lavoro CODAU per consultazione con AGID
- Dubbi riguardanti alcune definizioni (risorse attive, dispositivi informatici, etc)
- Applicabilità e sostenibilità interna
- Mancanza di un processo di verifica di quanto dichiarato
- Obbligo senza un sistema sanzionatorio: solo attività preventiva?

Sicurezza per InfoSapienza: obiettivi

- Analizzare e quantificare il livello di sicurezza rispetto a standard comuni
- Accrescere il livello di sicurezza dei servizi e sistemi informatici
- Raggiungere la conformità normativa alle leggi specifiche
- Definire un sistema di gestione della sicurezza delle informazioni
- Sviluppare piani di rimedio a mitigazione delle criticità e vulnerabilità rilevate
- Ottenere livelli di sicurezza adeguati rispetto alle nuove minacce
- Ottimizzare gli investimenti in sicurezza delle informazioni

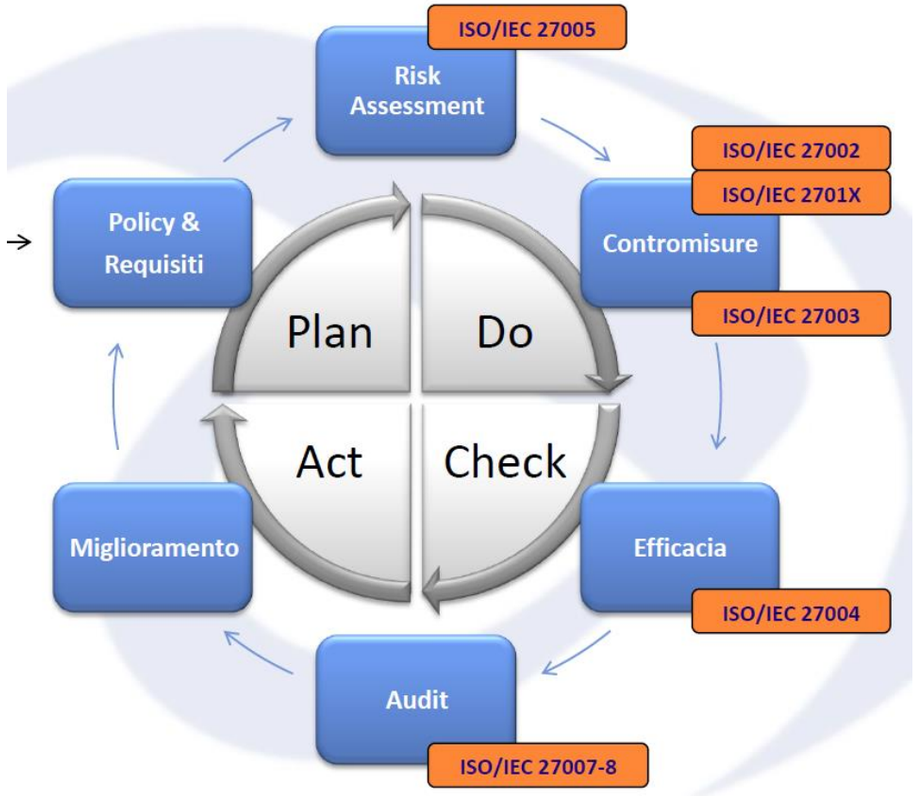
Infosapienza: il processo di gestione della sicurezza

CULTURALE

ORGANIZZATIVO

TECNICO

COMUNICATIVO



Il percorso di InfoSapienza

ORGANIZZATIVO

- Acquisizione di competenze in tema di information security
- Collaborazione con il CIS
  - Analisi delle vulnerabilità dei siti web delle strutture
  - Supporto in casi di incidenti di rilevanza mediatica
  - Organizzazione dell'evento Cyber Security Forum
- Definizione di un budget dedicato alla sicurezza informatica
- Restrizione della navigazione web per l'Amm. Centrale
- Incremento della percezione del rischio informatico
- Formazione ai referenti informatici
- Compliance alla normativa sulla privacy: il GDPR

Il percorso di InfoSapienza

TECNICO

- Analisi delle vulnerabilità delle web aplication: piani di rimedio
- Rafforzamento delle connessioni https (TLS)
- Restrizione della navigazione web per l'Amm. Centrale
- Definizione di un processo di protezione dei dati: patch management, backup, continuità operativa dei servizi
- Diminuzione della superficie di attacco: hosting dei siti web delle strutture periferiche
- Definizione di un processo di incident management: il SIEM
- Gap Analisys: analisi dallo scostamento dei livelli di sicurezza rispetto allo standard ISO 27001

Gap Analisys

Information Security Management System

Analisi AS-IS

Gap Analysis & Remediation Plan

Security Roadmap

Standard ISO/IEC 27001:2013

Leggi e regolamenti (196:2003, amministratori di sistema, GDPR)

Perimetro Infosapienza: sede, datacenter, servizi core, servizi di supporto

Gestione efficace degli incidenti

#EyePyramid

Infezione di un malware del tipo Remote Control adibito a compromettere i sistemi delle vittime ed esflitrare un gran quantitativo di informazioni riservate.

- Supporto congiunto CIS ed Infosapienza
- Analisi e verifica dell'infezione
- Nessun caso riscontrato sui dispostivi dell'Amm. Centrale

#WannaCry

Infezione virale di un malware del tipo ransomware che ha colpito circa 99 paesi con più di 200.000 infezioni.

- Attivazione del team Infosapienza
- Analisi del worm e successive contromisure
- Emanazione di linee guida preventive e correttive
- Nessun caso riscontrato nell'amministrazione Centrale
- 6 casi isolati all'interno di strutture dipartimentali

Conclusioni generali

- ✓ Necessità di un approccio integrato della sicurezza: tecnico, organizzativo e gestionale.
- ✓ Superamento della dicotomia libertà vs sicurezza: libertà **e** sicurezza
- ✓ Occorre una visione della sicurezza condivisa e partecipata
- ✓ Necessità di una politica di sicurezza delle informazioni per l'Ateneo: definizione della funzione security
- ✓ Accrescere la consapevolezza degli utenti: l'elemento più vulnerabile del processo è l'uomo
- ✓ Inserire gli aspetti di sicurezza in ogni processo riguardante le informazioni e i dati
- ✓ InfoSapienza riferimento dei processi di sicurezza della Sapienza con mansioni di supporto alle varie strutture dipartimentali
- ✓ Creare sinergie proattive tra i dipartimenti, centri di ricerca e InfoSapienza

PA digitale e cybersecurity

Un approccio sostenibile per le misure minime di sicurezza nelle Università

SAPIENZA
UNIVERSITÀ DI ROMA

2017 FORUM PA

Leonardo Querzoni
Dip. Ing. Automatica e Gestionale

Giuseppe Arrabito
Centro Infosapienza