Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

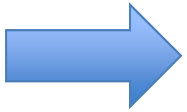
La strategia e le azioni AgID per la gestione della sicurezza informatica delle PA

Agostino Ragosa

Roma, 10 luglio 2013

Il contesto

- L'economia digitale consente di registrare un forte impatto diretto sul PIL e di supportare indirettamente lo sviluppo di tutti i settori della società.
- Le pubbliche amministrazioni partecipano a questo processo in modi nuovi:
  - Fornendo servizi su canali differenziati
  - Aprendo i loro sistemi alla collaborazione con altre PA anche estere e con i privati
  - Aprendo i loro bacini informativi
  - Fornendo servizi sempre più integrati e di valore



- I sistemi informativi delle PA sono una risorsa critica, preziosa e da proteggere, anche allo scopo di aumentare la fiducia nei servizi digitali.
- Occorre garantire l'accesso alle risorse solamente ai soggetti che legittimamente devono avere tale accesso e tutelare la privacy.
- Le azioni devono essere corali e sincronizzate.

Cosa devono fare le Pubbliche Amministrazioni

Da Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i.

Art. 51 - Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni.

2. *I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta.*

Una qualunque rappresentazione di informazioni con strumenti e su supporti informatici

L’incontro di oggi e l’agenda

1. La normativa sulla sicurezza informatica
2. I risultati della rilevazione presso le PAC
3. I rischi di sicurezza
4. Le azioni AgID

L’incontro di oggi e l’agenda

1. La normativa sulla sicurezza informatica
2. I risultati della rilevazione presso le PAC
3. I rischi di sicurezza
4. Le azioni AgID

Le normative in materia di sicurezza informatica /1

- Codice in materia di protezione dei dati personali L n. 196/2003

→ L'Allegato B) costituisce il disciplinare tecnico relativo alle misure minime di sicurezza

- art. 51 del CAD. «Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni «

→ Con le regole tecniche adottate ai sensi dell'articolo 71 sono individuate le modalità che garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture

- Art. 21 DPCM regole tecniche SPC (1 aprile 2008)

→ L' architettura di sicurezza del SPC è volta a consentire:

a. lo sviluppo del SPC come dominio affidabile (trusted), costituito da una federazione di domini di sicurezza in cui diversi soggetti si impegnano reciprocamente ad adottare le misure minime definite nell'ambito del SPC, atte a garantire i livelli di sicurezza necessari all'intero sistema;

La Commissione SPC , sulla base dell'analisi dei rischi cui sono soggetti il patrimonio informativo ed i dati della pubblica amministrazione, emana le linee guida riguardanti le misure di sicurezza e gli standard da adottare

Le normative in materia di sicurezza informatica /2

- Art. 20, comma 3, lett b) DL 83/2012

→L'Agenzia detta indirizzi, regole tecniche e linee guida in materia di sicurezza informatica, …

- Decreto crescita 2.0: DL 18 ottobre 2012 n. 179 convertito nella legge 17 dicembre 2012 n. 221 Art. 33-septies, comma 1, Consolidamento e razionalizzazione dei siti e delle infrastrutture digitali del Paese.

→ L'Agenzia per l'Italia digitale, con l'obiettivo di razionalizzare le risorse e favorire il consolidamento delle infrastrutture digitali delle pubbliche amministrazioni, avvalendosi dei principali soggetti pubblici titolari di banche dati, effettua il censimento dei Centri per l'elaborazione delle informazioni (CED) della pubblica amministrazione, come definiti al comma 2, ed elabora le linee guida, basate sulle principali metriche di efficienza internazionalmente riconosciute, finalizzate alla definizione di un piano triennale di razionalizzazione dei CED delle amministrazioni pubbliche che dovrà portare alla diffusione di standard comuni di interoperabilità, a crescenti livelli di efficienza, **di sicurezza** e di rapidità nell'erogazione dei servizi ai cittadini e alle imprese.

Le normative in materia di sicurezza informatica /3

- DPCM 24 gennaio 2013 GU n.66 del 19-3-2013 recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale .

→ interagire con le corrispondenti autorità estere (UE, NATO) ;

→ Architettura su tre distinti livelli d'intervento:

  - indirizzo politico e coordinamento strategico, cui affidare l'individuazione degli obiettivi funzionali a garantire la protezione cibernetica e la sicurezza informatica nazionali,
  - di supporto, a carattere permanente, con funzioni di raccordo nei confronti di tutte le Amministrazioni ed enti competenti,
  - di gestione delle crisi, con il compito di curare e coordinare le attività di risposta e di ripristino della funzionalità dei sistemi, avvalendosi di tutte le componenti interessate;

Scopo del decreto indirizzi per la protezione cibernetica e la sicurezza informatica nazionale

- Il decreto definisce, in un contesto unitario e integrato, l'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, indicando a tal fine i compiti affidati a ciascuna componente ed i meccanismi e le procedure da seguire ai fini della riduzione della vulnerabilità, della prevenzione dei rischi, della risposta tempestiva alle aggressioni e del ripristino immediato della funzionalità dei sistemi in caso di crisi.
- I soggetti compresi nell'architettura istituzionale operano nel rispetto delle competenze già attribuite dalla legge a ciascuno di essi.
- Il modello organizzativo-funzionale delineato con il decreto persegue la piena integrazione con le attività di competenza del Ministero dello sviluppo economico e dell'Agenzia per l'Italia digitale, nonché con quelle espletate dalle strutture del Ministero della difesa dedicate alla protezione delle proprie reti e sistemi nonché alla condotta di operazioni militari nello spazio cibernetico, dalle strutture del Ministero dell'interno, dedicate alla prevenzione e al contrasto del crimine informatico e alla difesa civile, e quelle della protezione civile.

Contesto internazionale

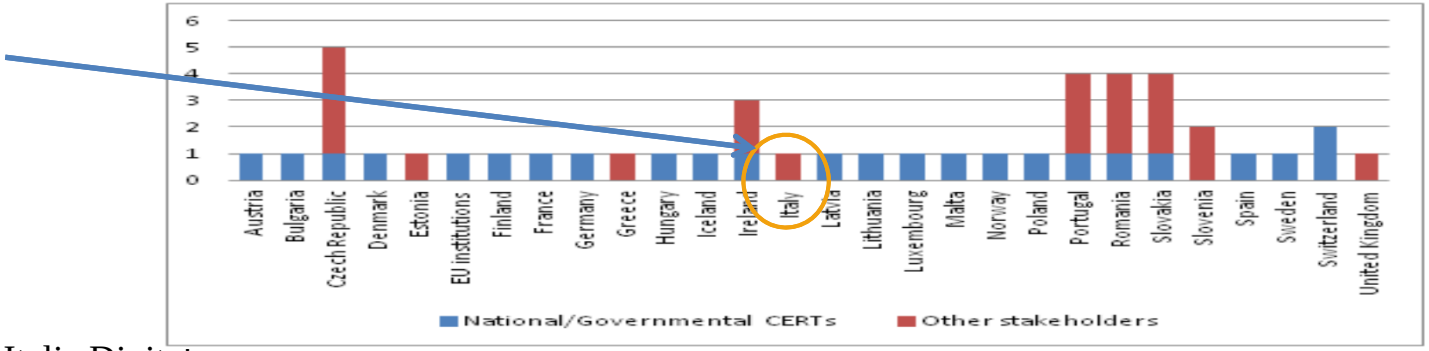
Agenda digitale europea

- Prevede un pillar (nr. 3) dedicato a “trust and security”

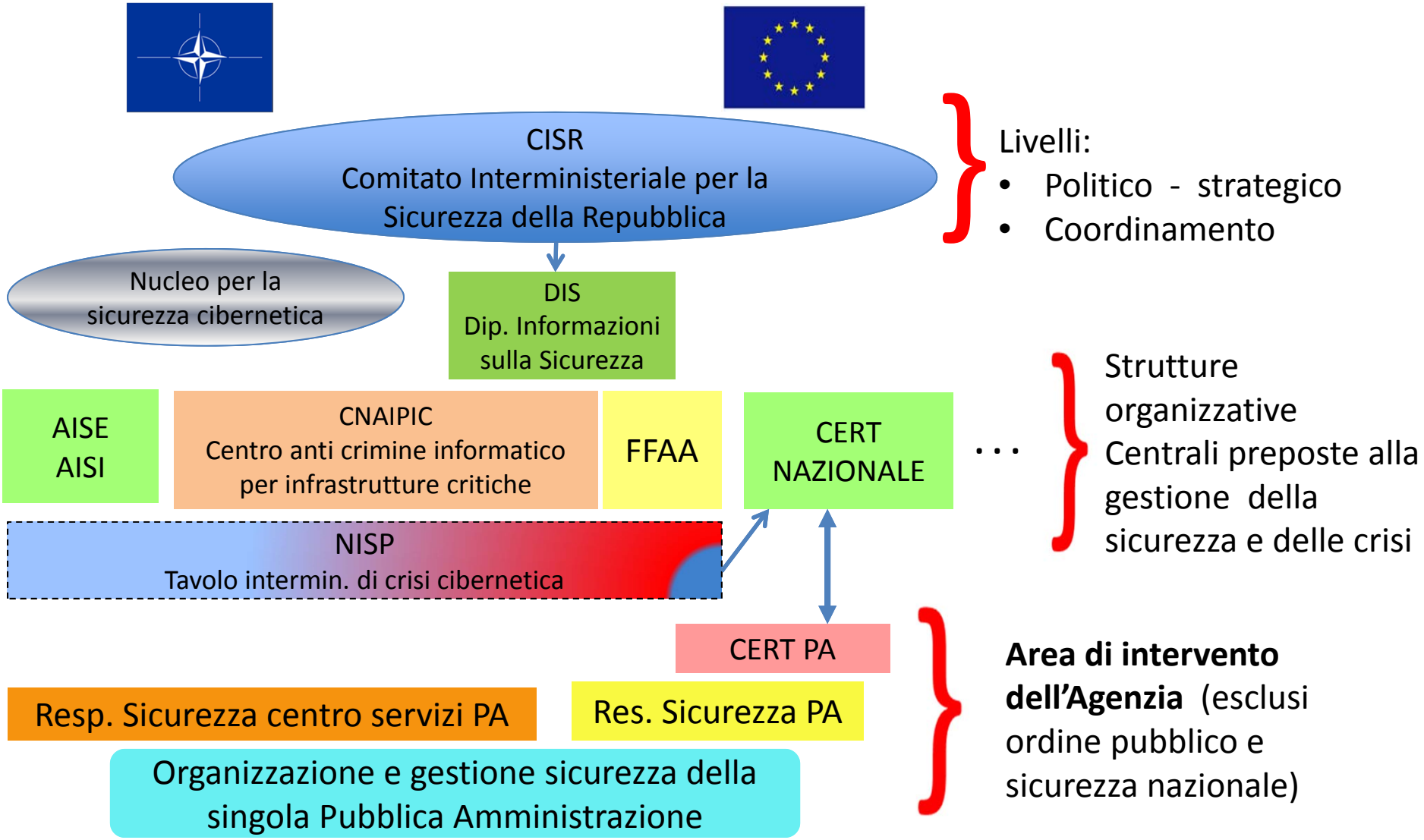
  - ✓ Action 29 – combattere cyber attack contro sistemi critici
  - ✓ Action 38 – creazione di reti di CERT
  - ✓ Action 41 – adattare piattaforme nazionali di allerta di attacchi per combattere cyber attack anche cross-border

- Altri aspetti di sicurezza sono ad es. previsti nel **Pillar 7**,
  - ✓ Action 83 – gli stati membri definiscono piattaforme per assicurare il riconoscimento reciproco di meccanismi di identificazione e autorizzazione digitale anche transfrontaliera

Le actions della Digital Agenda for e-Europe riguardano la Commissione e gli stati membri e vengono monitorate attraverso «scoreboard»



L'organizzazione della sicurezza informatica



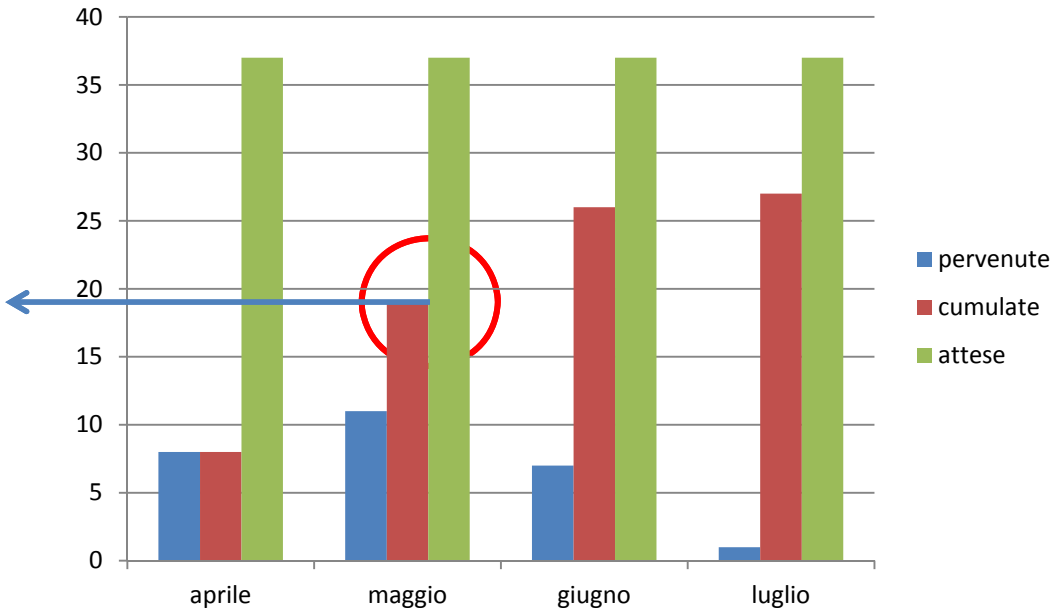
L’incontro di oggi e l’agenda

1. La normativa sulla sicurezza informatica
2. I risultati della rilevazione presso le PAC
3. I rischi di sicurezza
4. Le azioni AgID

Il questionario

- Con lo scopo di definire un punto di partenza, a fine marzo 2013 , è stato inviato un questionario a 37 amministrazioni centrali
- Sono pervenute 27 schede pari al 73% delle PA interpellate

Dopo 2 mesi avevano risposto il 50% delle PA



Il questionario/2

		SI	NO	Note
1	Esiste un responsabile della sicurezza informatica?	78%	22%	
2	E' stato formalmente definito ed approvato il piano della sicurezza informatica?	56%	44%	
3	Esiste un nucleo di riferimento per la sicurezza informatica?	89%	11%	
4	Esiste un gruppo di gestione degli incidenti informatici?	82% (*)	18%	(*) 52% no formale
5	E' stata istituita l'ULS dell'Amministrazione?	78%	22%	
6	Modalità di colloquio della ULS con il provider SPC	27%	73%	
7	Sono raccolte statistiche sulla sicurezza informatica?	73%	27%	
8	Se esistono contratti di outsourcing, i contratti prevedono verifiche dell'Amministrazione sulla gestione della sicurezza informatica?	74%	26%	
9	Esiste una previsione di spesa dedicata specificatamente alla sicurezza informatica?	48%	52%	
10	Sono state prese iniziative per informazione/formazione sulla sicurezza informatica rivolte al personale dell'Amministrazione ?	78%	22%	

L’incontro di oggi e l’agenda

1. La normativa sulla sicurezza informatica
2. I risultati della rilevazione presso le PAC
3. I rischi di sicurezza
4. Le azioni AgID

Rischi e attacchi

Quali rischi?

- Informazioni: possono essere sottratte, alterate e distrutte
- Servizi: possono essere degradati, alterati e bloccati
- Fonti: possono essere confuse, alterate
- I livelli autoritativi: possono essere alterati
- Le autorizzazioni: possono essere alterate
- I sistemi di controllo e monitoraggio: possono essere manomessi o distrutti

Come ?

→ Contagio da malware (virus, phishing, botnet)

→ Attacchi cyber (activisms, cybercrime, cyberwar)

→ Furto di credenziali/identità (impersonificazione di un soggetto/ organizzazione o servizio

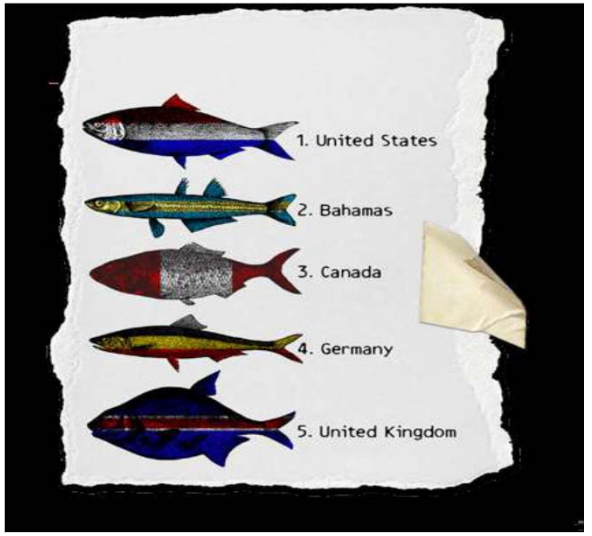
→ Degrado/interruzione e distruzione di servizio (denial of services, oscuramento siti)

Attraverso software malizioso, vulnerabilità dei sistemi, scarsa applicazione di regole, disattenzione

Alcuni dati relativi alle minacce

- Sfruttando le potenzialità di Internet la criminalità informatica ha costruito, nel corso degli ultimi anni, una efficiente rete finalizzata allo scambio di informazioni e alla commercializzazione di “prodotti/servizi” funzionali al compimento di atti criminosi.
- La possibilità di ricorrere ad un mercato globale in grado di gestire una crescente offerta di “armi informatiche” e di “mercenari informatici”, estende lo scenario del cyber-crime a qualsiasi tipologia di organizzazione criminale o terroristica che intenda avvalersi delle tecniche informatiche per il compimento dei propri scopi.

- URL «malicious» crescono del 600% anno
- Tra i paesi che “ospitano” malware vi sono anche quelli occidentali (i primi 5 sono USA, Russia, Germania, Cina, Moldavia)
- Il phishing diventa sempre più sofisticato e mirato



Alcuni dati sui principali incidenti internazionali noti del 2012

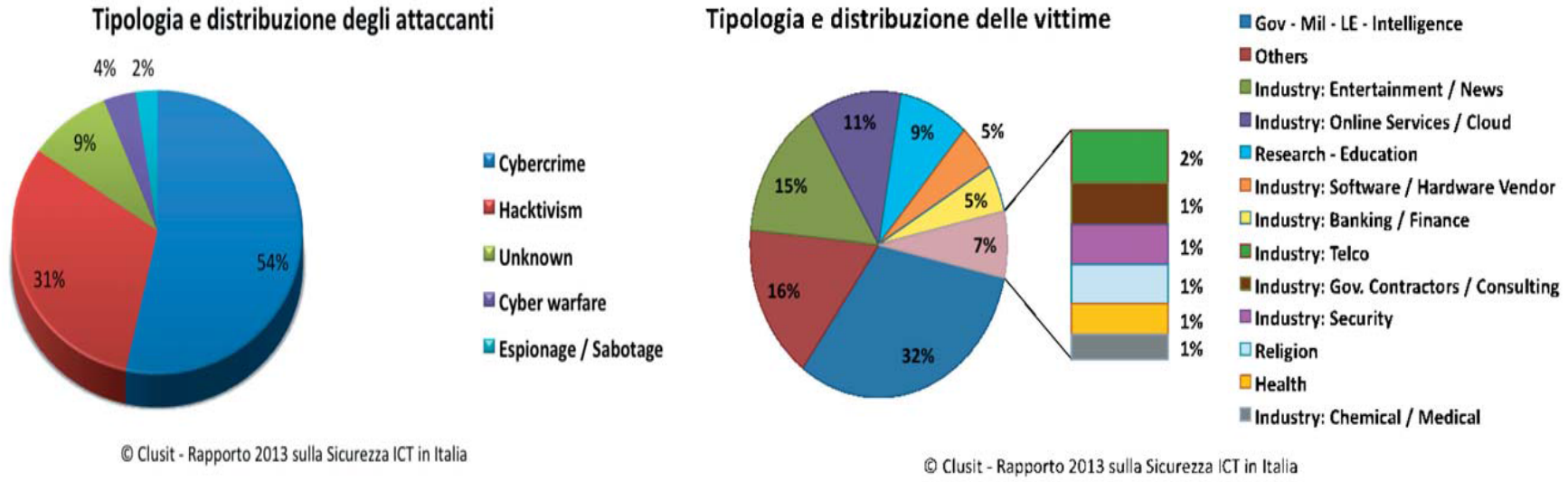
ATTACCANTI PER TIPOLOGIA	2011	2012	Totale	Incremento
Cybercrime	170	633	803	372,35%
Unknown	148	110	258	-25,68%
Hacktivism	114	368	482	322,81%
Espionage / Sabotage	23	29	52	126,09%
Cyber warfare	14	43	57	307,14%
TOTALE	**469**	**1.183**	**1.652**	**252,24%**

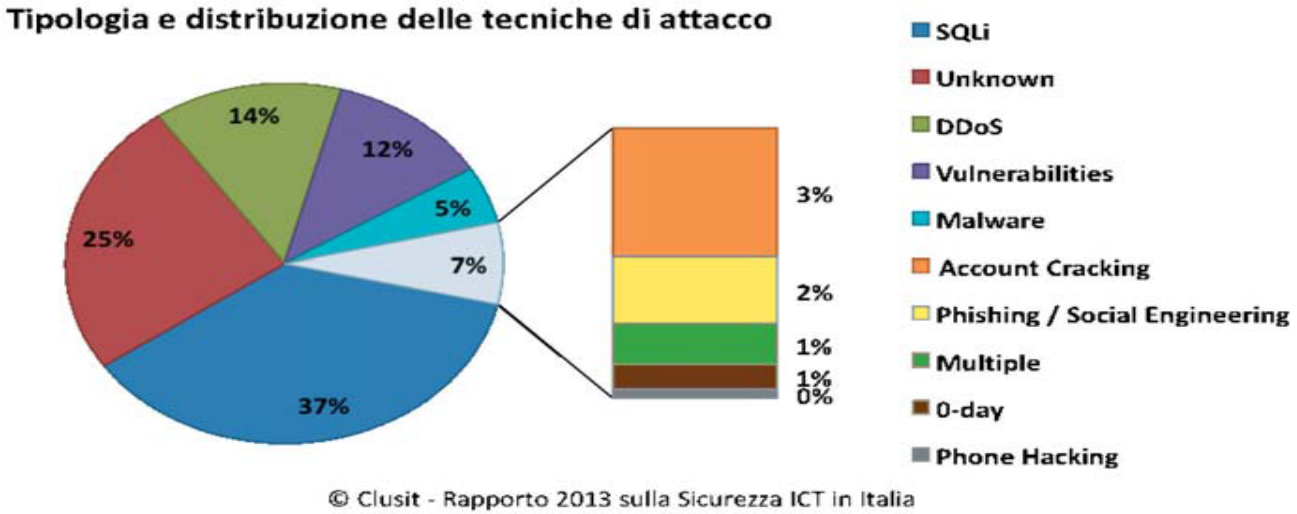
VITTIME PER TIPOLOGIA	2011	2012	Totale	Incremento
Institutions: Gov - Mil - LEAs - Intelligence	153	374	527	244,44%
Others	97	194	291	200,00%
Industry: Entertainment / News	76	175	251	230,26%
Industry: Online Services / Cloud	15	136	151	906,67%
Institutions: Research - Education	26	104	130	400,00%
Industry: 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**

TECNICHE DI ATTACCO PER TIPOLOGIA	2011	2012	Totale	Incremento
SQL Injection[38]	197	435	632	220,81%
Unknown / APT	73	294	367	402,74%
DDoS[39]	27	165	192	611,11%
Known Vulnerabilities / Misconfigurations	107	142	249	132,71%
Malware	34	61	95	179,41%
Account Cracking	10	41	51	410,00%
Phishing / Social Engineering	10	21	31	210,00%
Multiple Techniques	6	13	19	216,67%
0-day[40]	5	8	13	160,00%
Phone Hacking	0	3	3	300,00%
TOTALE	**469**	**1.183**	**1.652**	**252,24%**

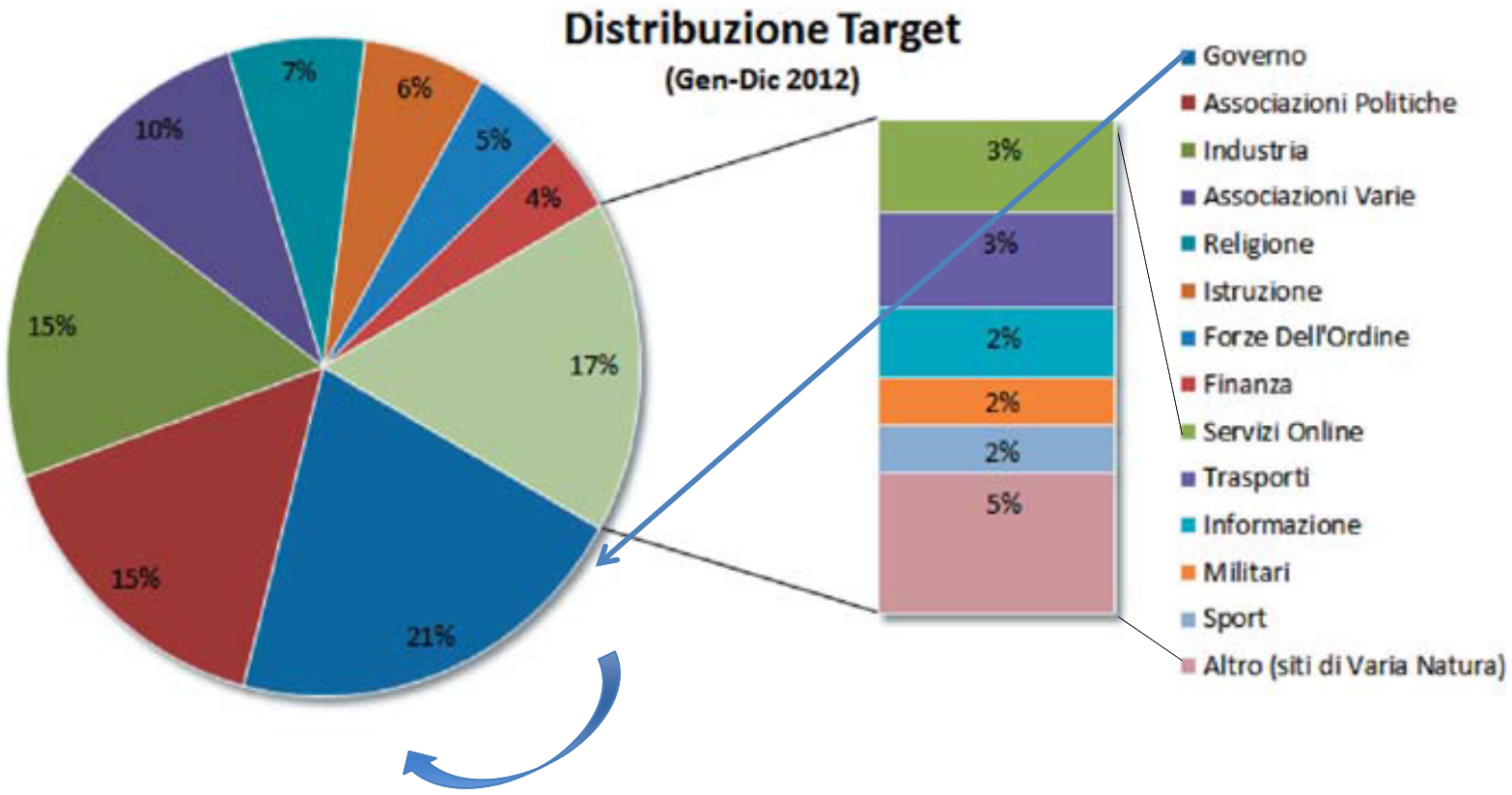
© Clusit - Rapporto 2013 sulla Sicurezza ICT in Italia

Alcuni dati sui principali incidenti internazionali noti del 2012





La distribuzione degli attacchi in Italia nel 2012



La situazione delle principali minacce secondo Enisa

Top Threats	Current Trends	Top 10 Emerging Trends					
		Mobile Computing	Social Technology	Critical Infrastr.	Trust Infrastr.	Cloud	Big Data
1. Drive-by exploits	↑	↑	↑	↑		↑	↑
2. Worms/Trojans	↑	↑	↑	↑		→	↑
3. Code Injection	↑	→		↑		↑	
4. Exploit Kits	↑	↑	→	↑			↑
5. Botnets	↑	↑		→		→	
6. Denial of Service	→			→	↑	→	
7. Phishing	→	↑	↑	→			→
8. Compromising Confidential Information	↑	↑		↑	→	↑	↑
9. Rogueware/ Scareware	→		→				
10. Spam	↓		→				→
11. Targeted Attacks	↑		↑	↑	→	↑	→
12. Physical Theft/Loss/Damage	↑	↑	↑	↑	→	→	
13. Identity Theft	↑	↑	↑		→	↑	↑
14. Abuse of Information Leakage	↑	→	↑		→	↑	↑
15. Search Engine Poisoning	→						
16. Rogue Certificates	↑				↑		

Legend: ↓ Declining, → Stable, ↑ Increasing

Necessità operative

- Definire scenari di valutazione del rischio, coinvolgendo le strutture adeguate
- Definire piani di difesa
- Attivare strumenti tecnici ed organizzativi su tutta la filiera
- Coordinare le azioni con «alleati» esterni
- Monitorare e aggiornare costantemente procedure, prassi e strumenti
- Sensibilizzare sulla necessità di skill e strumenti multidisciplinari
- Attivare piani di informazione e formazione

L’incontro di oggi e l’agenda

1. La normativa sulla sicurezza informatica
2. I risultati della rilevazione presso le PAC
3. I rischi di sicurezza
4. Le azioni AgID

Cosa deve fare l'Agenzia

L'Agenzia per l'Italia Digitale è chiamata a dettare raccomandazioni, strategie, norme tecniche in tema di:

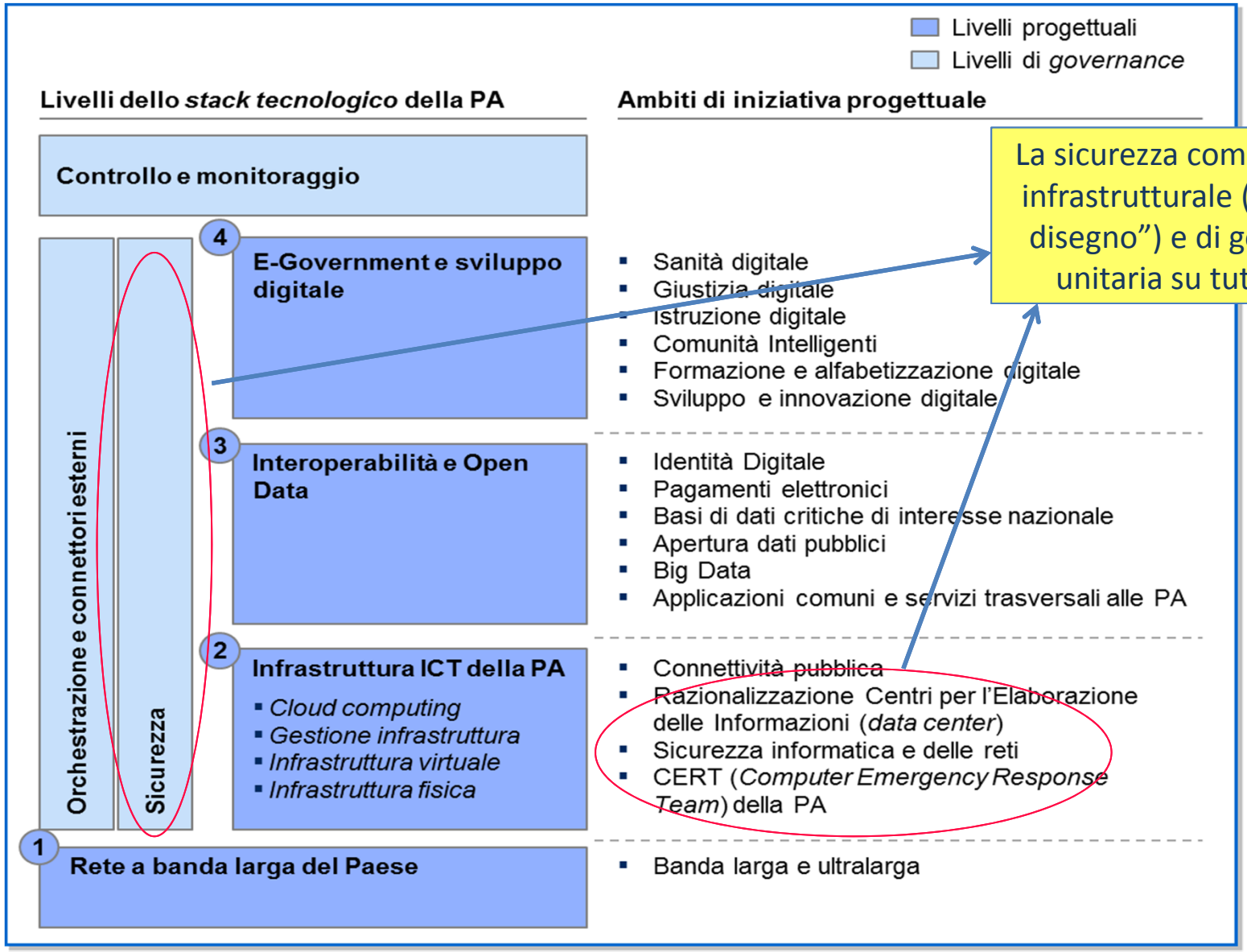
1. sensibilizzazione e alfabetizzazione del personale in materia di sicurezza informatica e di relative emergenze,
2. metodologia di rilevazione ed analisi dei rischi connessi all'impiego di tecnologie evolute,
3. valutazione dell'impatto - nel quadro della riservatezza e della sicurezza – dell'avvio di iniziative di automazione,
4. esame e stima delle misure di protezione poste in essere e delle eventuali attività di misurazione delle prestazioni

L'Agenzia d'intesa e con la partecipazione delle amministrazioni interessate, provvede inoltre a:

1. promuovere progetti coerenti con gli obiettivi di cui sopra
2. accertare periodicamente, il livello di sicurezza e riservatezza dei sistemi informatici e delle reti telematiche geografiche e locali utilizzate dalle amministrazioni stesse
3. proporre interventi correttivi e suggerire rimedi alle eventuali carenze tecniche, procedurali e organizzative rilevate in sede di riscontro periodico.

L'Agenzia è impegnata ad avviare gestire ed evolvere il CERT della PA, in un quadro di coordinamento strategico con altri CERT e di creare una community preparata, aggiornata e che condivida politiche ed azioni in materia di Cybercrime e di coordinamento delle politiche di sicurezza informatica in tale settore.

Dalla strategia all'attuazione



Ambito di azione e strumenti dell'AgID per la sicurezza informatica

Strumenti normativi:
- art. 51 del CAD
- Art. 20, co 3, lett b) e g) DL 83
- DPCM regole SPC
- LG Commissione SPC

Strumenti di indirizzo:
- Linee guida x org. Sicurezza PA
- Requisiti mandatory x gare

CERT PA

Strumenti di governance:
- CERT PA
- Cruscotti
- Assessment
- Network resp. Sicurezza
- Commissione SPC

Resp. Sicurezza centro servizi PA

Res. Sicurezza PA

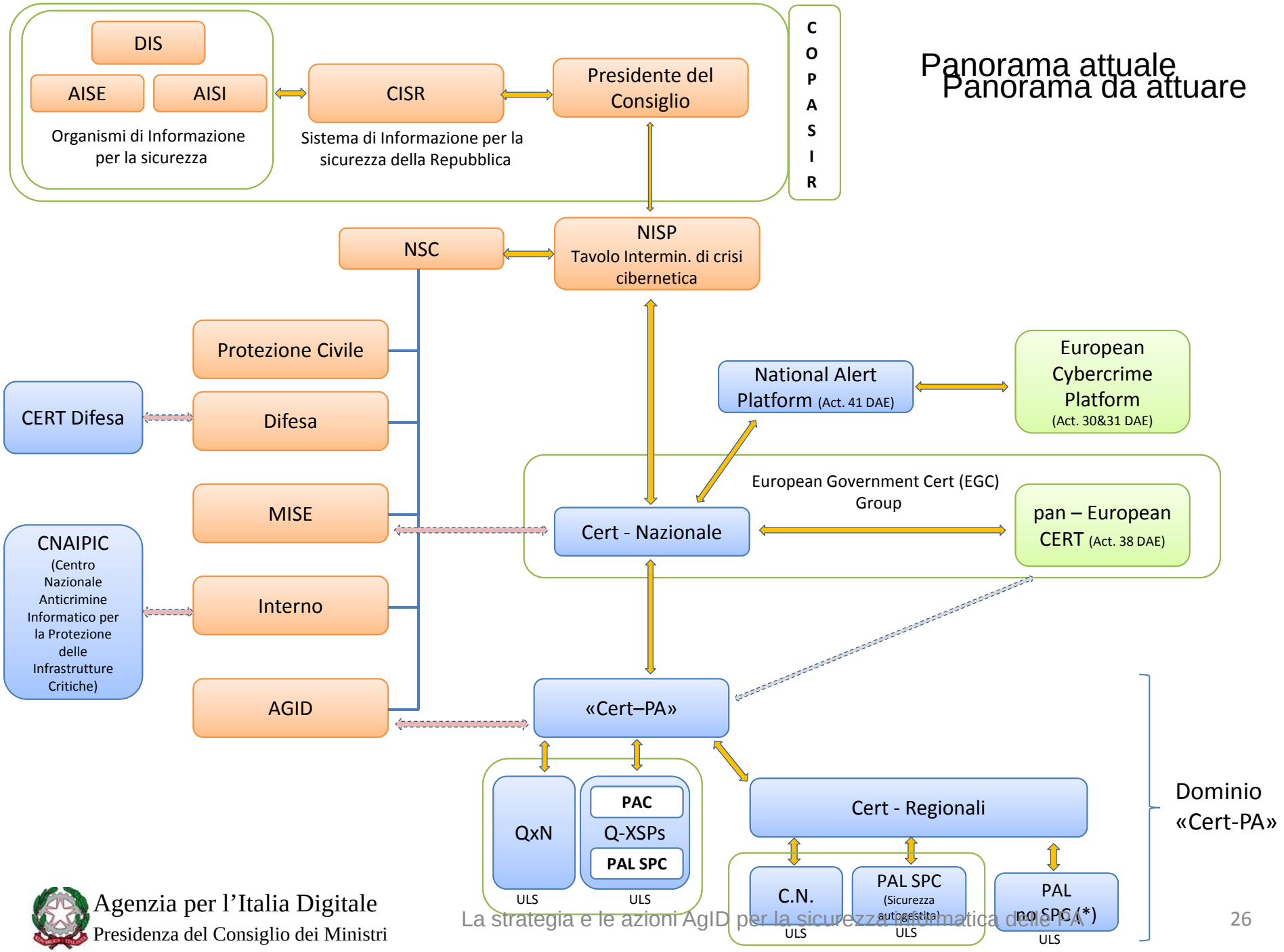
Organizzazione e gestione sicurezza della singola Pubblica amministrazione

Pac

Regioni

ASL

Strumenti di sussidiarietà x le PA:
- Strumenti tecnici
- Servizi di consulenza
- Servizi di assessment
- Servizi di gestione
- Servizi di formazione
- Diffusione bulletin


Panorama attuale
Panorama da attuare
DIS
AISE
AISI
Organismi di Informazione per la sicurezza
CISR
Sistema di Informazione per la sicurezza della Repubblica
Presidente del Consiglio
COPASIR
NSC
NISP
Tavolo Intermin. di crisi cibernetica
Protezione Civile
CERT Difesa
Difesa
MISE
CNAIPIC
(Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche)
Interno
AGID
National Alert Platform (Act. 41 DAE)
European Cybercrime Platform
(Act. 30&31 DAE)
European Government Cert (EGC) Group
Cert - Nazionale
pan – European CERT (Act. 38 DAE)
«Cert–PA»
QxN
PAC
Q-XSPs
PAL SPC
ULS
ULS
Cert - Regionali
C.N.
ULS
PAL SPC
(Sicurezza autogestita)
ULS
PAL no SPC (*)
ULS
Dominio «Cert-PA»

I servizi del CERT PA e i tempi

- Messa a punto del modello e delle linee guida (ottobre 2013)
- Avvio dalla RIPA e con le PA presenti per provare il set iniziale di servizi (dicembre 2013)
  - Servizi di analisi e indirizzamento (definizione di metodologie e metriche, definizione dei processi interni ed esterni)
  - Servizi proattivi (raccolta dati, emanazione di bollettini, costruzione di basi informative
  - Servizi reattivi (gestione allarmi e supporto ai processi di gestione e risoluzione degli incidenti
  - Servizi di assurance (monitoraggio piani , verifica applicazione di linee guida e best practices, sviluppo della mappa dei rischi)
  - Servizi di formazione e comunicazione
- Estensione ad altre PA e a qualche Regione (marzo 2014)
- Definizione dello scenario a regime (giugno 2014)

Le indicazioni per la sicurezza IT delle PA: struttura del documento

RIFERIMENTO ARCHITETTURALE PER LA SICUREZZA

Architetture ITC di riferimento
Politica della sicurezza
Il Sistema di Gestione della sicurezza ICT (SGSI)
Organizzazione del SGSI
CERT-PA (dal punto di vista del sistema sicurezza IT delle PA)

INDICAZIONI PER L'OPERATIVITÀ E LA GESTIONE DELLA SICUREZZA

Sicurezza fisica
Progettazione di sistemi e applicazioni e requisiti di accettazione
Gestione operativa dei sistemi e delle reti
Monitoraggio della sicurezza
Controllo degli accessi
Gestione degli incidenti relativi alla sicurezza
Conformità e audit
Politiche di formazione e informazione
CERT-PA (dal punto di vista operativo)

APPENDICI

Appendice A: Rischi informatici
Appendice B: Gestione dei documenti della sicurezza
Appendice C: La sicurezza delle reti NGN
Appendice D: Cenni alla Continuità Operativa

Verrà sottoposto ad una consultazione per la finalizzazione prima dell'emissione entro l'autunno 2013

Stato attuazione art. 33-septies: il censimento dei CED della PA

La norma dispone tre compiti per AGID:
- l'effettuazione del censimento dei CED della PA;
- la predisposizione delle linee guida per la razionalizzazione dei CED della PA;
- la predisposizione della proposta di piano triennale per la razionalizzazione dei CED della PA

E' stata avviata la stesura del documento

Il censimento è realizzato mediante la compilazione di un questionario di 65 domande che le PAC, le Regioni, le ASL e le AO, le Province, i Comuni sopra i 10.000 abitanti sono chiamate a fare.

10 domande sono relative ad aspetti di sicurezza e continuità operativa dei CED.

Il censimento è cominciato ai primi di giugno 2013 e proseguirà sino al 15 luglio.

Alla data, lo stato della compilazione è il seguente:

AMMINISTRAZIONI	QUESTIONARI COMPLETATI
PAC	23
Regioni	19
ASL/AO	50
Province	72
Comuni	251
Unioni Comuni	7
Altre	2
TOTALI	**424**

Servizi SPC per la sicurezza

Gara Connettività:

- Servizi di sicurezza perimetrale di rete
- Servizi di consulenza specialistici sulle problematiche di sicurezza

Gara Infrastrutture:

- creazione di un repository funzionale alle esigenze del Cert-SPC

Gara applicativa:

- Servizi di assessment della sicurezza
- Servizi per l'organizzazione della sicurezza
- Servizi per la valutazione delle vulnerabilità
- Servizi per la gestione delle emergenze
- Servizi di formazione sulle problematiche di sicurezza

→ vincoli di SOC x tutti i fornitori SPC ed i centri servizi collegati ad SPC

Prossimi passi

Entro ottobre 2013

- Costituzione della Community dei security manager delle PA centrali
- Coinvolgimento delle Regioni
- Avvio del CERT PA (con successiva pianificazione del coinvolgimento delle PA)
- Finalizzazione delle Linee guida sulla sicurezza informatica
- Definizione di percorsi formativi, anche in via telematica, indirizzati alle PA in materia di prevenzione e gestione di incidenti di sicurezza informatica

Le suddette attività verranno realizzate con fondi AgID, riprogrammando attività progettuali e obiettivi

G r a z i e !