La gestione dell'Information Security e la normativa di riferimento degli Enti Locali

MODULO 1 - I RISCHI E LO SCENARIO ATTUALE DELLA SICUREZZA NEGLI ENTI LOCALI

Davide Grassano, KPMG
Andrea Zapparoli Manzoni, KPMG

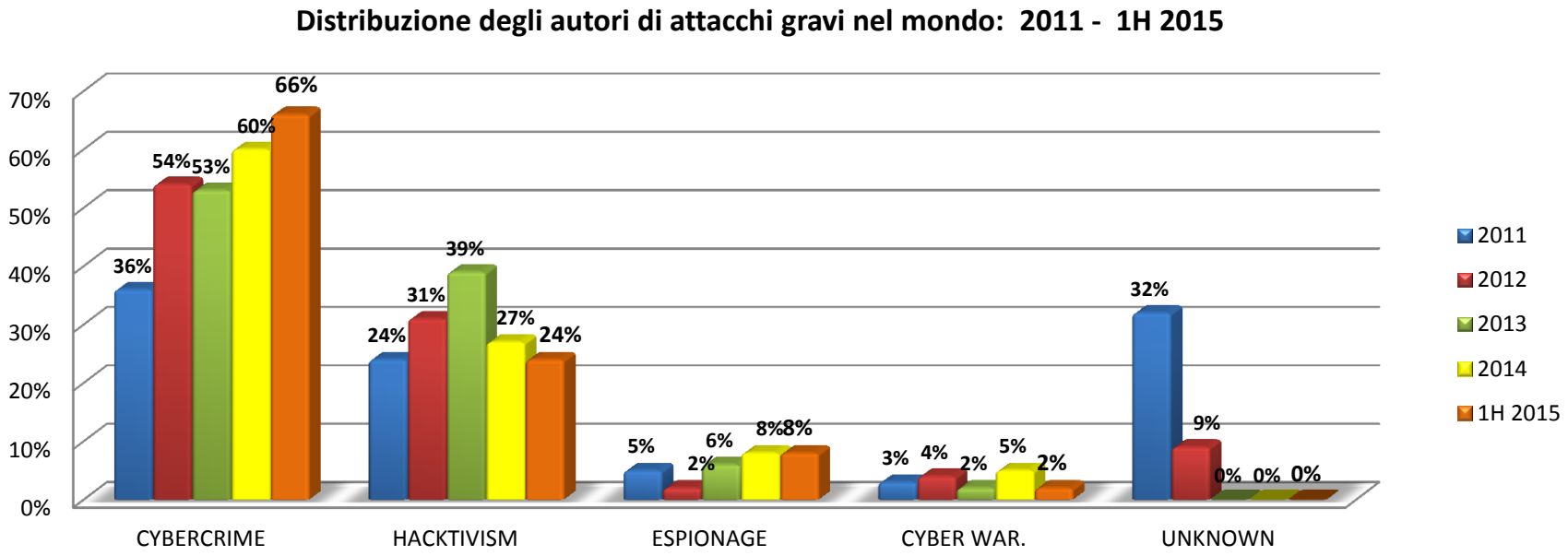
Agenda

- Analisi concreta dello scenario dei rischi (globale e nazionale)
- Sicurezza della PA nello scenario attuale – principali trend di attenzione
- Information security e ruoli nella definizione della sicurezza:
  - Sicurezza perimetrale e servizi di gestione reattiva e prospettive sul modello dei servizi: Esempi pratici
  - La sicurezza degli applicativi e la gestione dei ruoli e dei profili: Esempi pratici
  - Sicurezza nella gestione di outsurcer e fornitori e requisiti di sicurezza nell'ambito delle gare della PA locale: Esempi pratici
  - Sicurezza dei dispositivi individuali PC, Mobile,App : Esempi pratici
- La gestione del cambiamento e le aspettative sulla sicurezza dei servizi offerti dalla PA a cittadino e stakeholders

Analisi concreta degli scenari di rischio

DATI GLOBALI E NAZIONALI

Scenario globale dei rischi

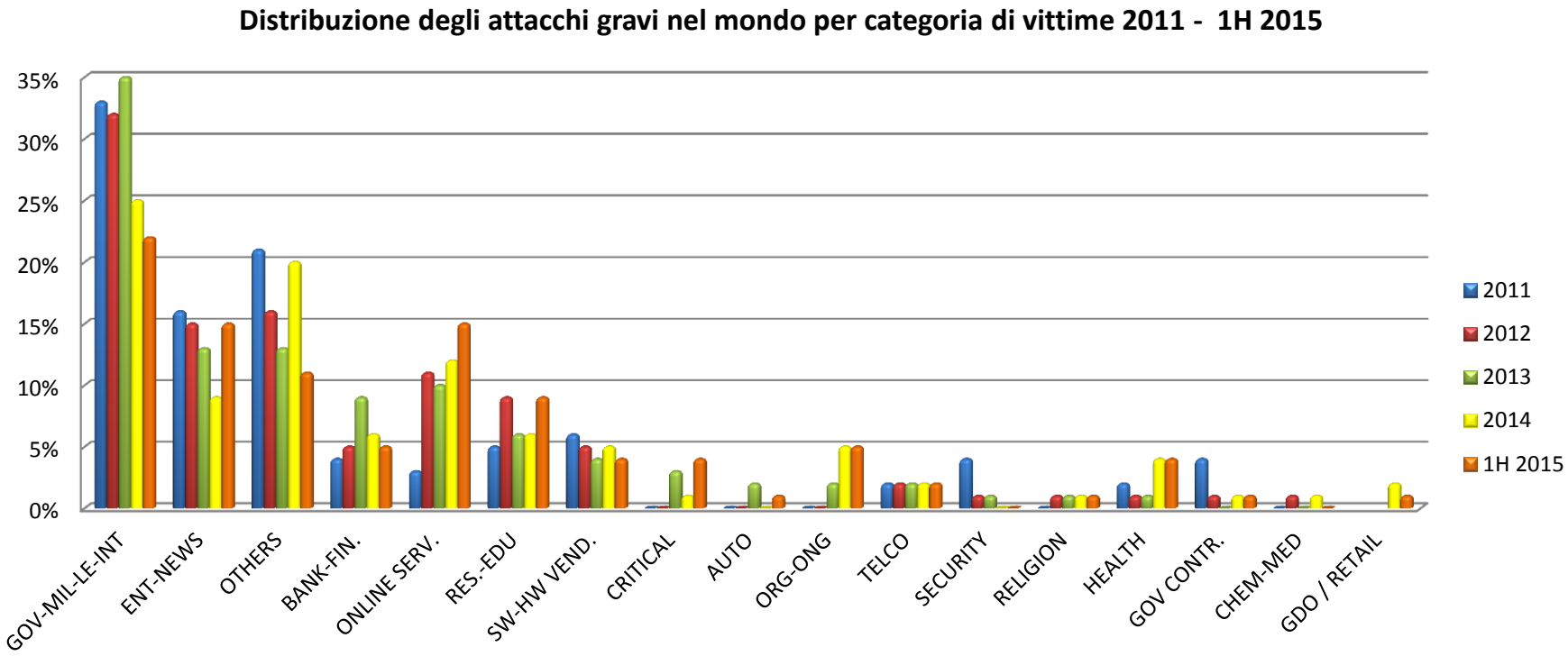


© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2015

Negli ultimi 5 anni si assiste ad un **aumento esponenziale degli attacchi informatici**, non solo contro privati cittadini ma anche contro aziende ed Enti pubblici.

Tra le diverse tipologie di attaccanti, quella che cresce più rapidamente (sia in termini numerici che di impatto economico) è il **Cyber Crime** (crimine organizzato che opera tramite strumenti informatici). I danni diretti ed indiretti stimati a livello globale nel 2014 sono **450 miliardi** di USD.

Scenario globale dei rischi

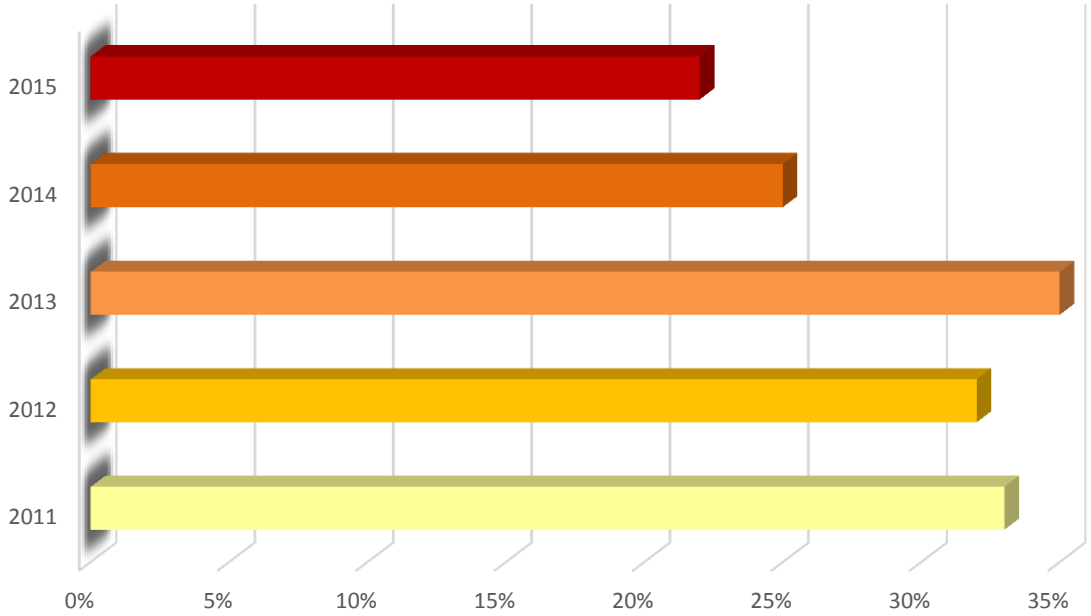


Il singolo settore più colpito da attacchi informatici gravi è quello Governativo.
Le ragioni sono molte, tra queste:

- Queste organizzazioni sono bersagli per attività di Information Warfare e di Hacktivism
- Dispongono di grandi quantità di dati relativamente ai cittadini ed alle imprese, utili per finalità di spionaggio economico (Espionage)
- Hanno livelli di sicurezza mediamente inferiori rispetto ad altri settori (Cyber Crime)

Scenario globale dei rischi

Percentuale di attacchi gravi al settore Gov su totale - 2011 - 1H 2015

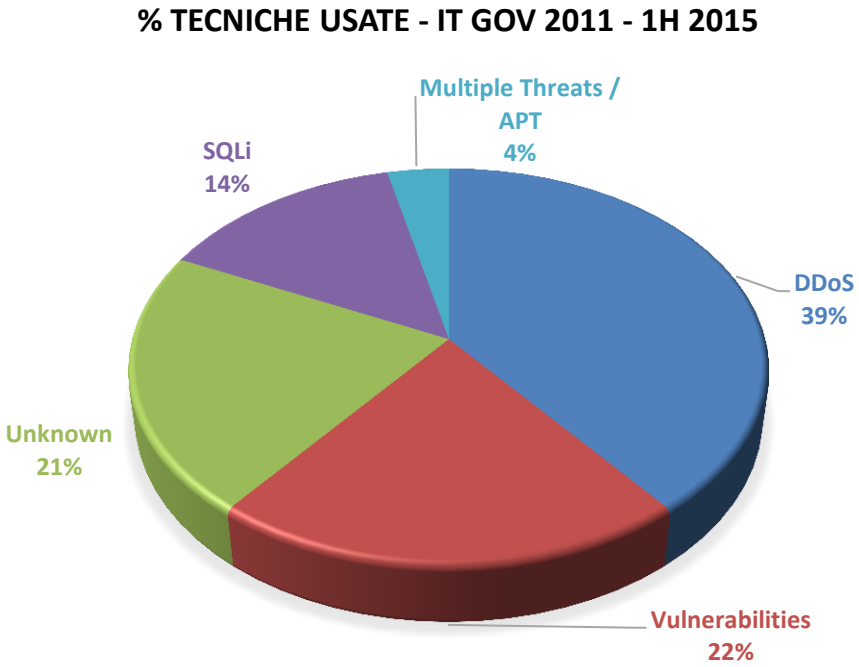


© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2015

Negli ultimi 5 anni, per quanto l'incidenza percentuale sul totale degli attacchi gravi registrati a livello globale sia in diminuzione (da un massimo del 34% nel 2013 al 22% del primo semestre 2015), il numero assoluto di attacchi gravi verso il settore Governativo **è in aumento**.

Si assiste inoltre ad un **cambiamento nella tipologia degli attaccanti** (meno Hacktivism, più Espionage e Cyber Crime), il che rappresenta un **aumento dei rischi**.

Scenario nazionale dei rischi



© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2015

Anche in Italia, **il singolo settore più colpito è quello della PA centrale e locale**, per le stesse ragioni.

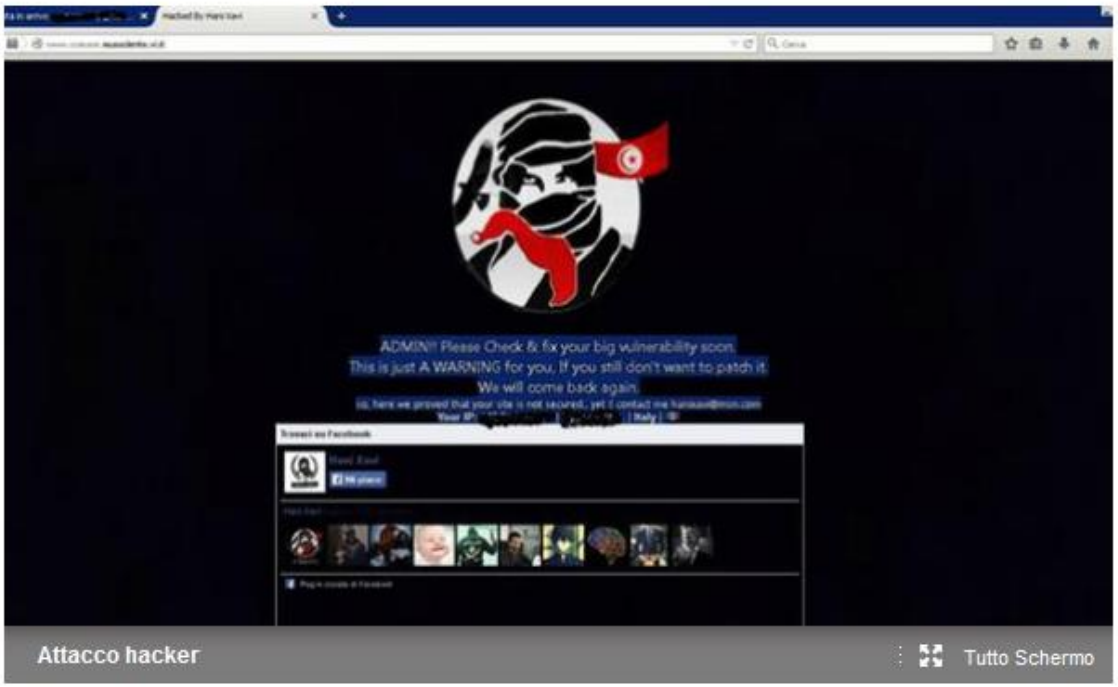
Internet rende il mondo "piatto", di conseguenza **lo stesso genere di minacce** grava ormai sulle organizzazioni di ogni Paese, in particolare di quelli avanzati.

In particolare negli ultimi 3 anni le nostre amministrazioni pubbliche (centrali e locali) hanno subito crescenti attacchi informatici, alcuni gravi (vedi esempi successivi). Il **75%** di questi è stato compiuto utilizzando **tecniche di attacco "banali"** (DDoS, Vulnerabilità note, SQLinjection).

Esempi recenti: Information Warfare

27.02.2015

Attacco hacker filoislamista al sito del Comune



Aumenta
Diminuisci
Stampa

Un gruppo di hacker filo islamisti ha attaccato ieri mattina il sito web del Comune di Mussolente. Il sito è stato messo completamente fuori uso e per circa due ore non è stato possibile accedere ai servizi online.

Esempi recenti: Hacktivism

HACKER | 09 febbraio 2014

Anonymous Italia all'attacco del sito del Ministero della Salute

COMMENTI (0)

0 Tweet G+1 0

LinkedIn 0 Pinterest 0 Email

Come è questa notizia?

Homepage del sito del Ministero della Salute

Roma - Dopo aver hackerato in passato il sito del Ministero dell'Interno e di altre istituzioni, **Anonymous Italia** colpisce il sito del Ministero della Salute .

L'attacco è legato alla manifestazione antiproibizionista e per la legalizzazione della cannabis che si è tenuta ieri a Roma (fotogallery).

ARTICOLI CORRELATI

E Anonymous "spegne" Grillo

Milano, attacco hacker al sito del tribunale

Esempi recenti: Espionage

Condividi:

Commenti: 12

Attacco informatico all'Italia. Rubate le e-mail della Difesa

L'assalto cibernetico degli hacker prosegue da un mese. Nel mirino anche le conversazioni delle Forze armate. Vertice a Palazzo Chigi. ***La mappa interattiva degli attacchi hacker***

Giuseppe Marino - Mer, 20/05/2015 - 12:01

commenta G+1 1 Mi piace 747

Roma - Da un mese il ministero della Difesa e le Forze armate italiane sono sotto attacco informatico. Nel mirino è il «C4i»: suona come il personaggio di Guerre stellari , ma è il termine con cui viene indicato il «sistema di comando, controllo, telecomunicazioni e informatica» della Difesa italiana.

Esempi recenti: Cyber Crime (contro gli Enti)

Ransomware, Comuni italiani sotto attacco

21 ottobre 2014 By Redazione 0 comments

Ransomware, è allarme per i sistemi informatici dei Comuni italiani.

Dopo mesi trascorsi a scrivere, e a leggere, di minacce più o meno fantomatiche che avrebbero potuto colpire le infrastrutture It della Pa, Pc e archivi delle amministrazioni locali sono stati infine colpiti. E nella maniera più impensata e beffarda che si potesse credere.

Di ritorno dalla pausa del fine settimana migliaia di responsabili informatici dei Comuni nazionali hanno trovato infatti i documenti dei cittadini, salvati in vario formato, inservibili: a fronte dell'impossibilità di aprire i file, un messaggio: "Pagate un riscatto di 400 euro e i vostri documenti saranno sbloccati. In caso contrario, trascorsi tre giorni la cifra necessaria a eliminare il virus che vi è stato inviato sarà raddoppiata".

Esempi recenti: Cyber Crime (contro gli utenti)

13
Feb

Avviso su malware o codice maligno

Data pubblicazione: 13/02/2015

Si informa che è in corso una campagna di diffusione di malware (programma malvagio o codice maligno/nocivo) tramite email apparentemente inviate dall'INPS (da supporto@inps.gov.it), relative alle certificazioni DURC, e riportanti in allegato un file .ZIP contenente il file con l'infezione virale.
L'Istituto informa che le comunicazioni relative alle certificazioni DURC vengono inviate esclusivamente tramite la casella PEC (Posta Elettronica Certificata) che ha indirizzi @postacert.inps.gov.it e che riportano in allegato solo documenti PDF e non file ZIP come le email fraudolente identificate.
Si invita dunque a non aprire l'allegato riportato in tali email e a verificare che l'email ricevuta abbia tutti gli elementi di autenticità di una PEC.

Domanda di Accesso al Bando VFP1 del 2015

Tutti coloro che sono interessati al nuovo **Bando dell'Esercito Italiano del 2015** dovranno presentare la Domanda solo ed esclusivamente per via Telematica attraverso il portale web dedicato ai concorsi online del Ministero della Difesa:

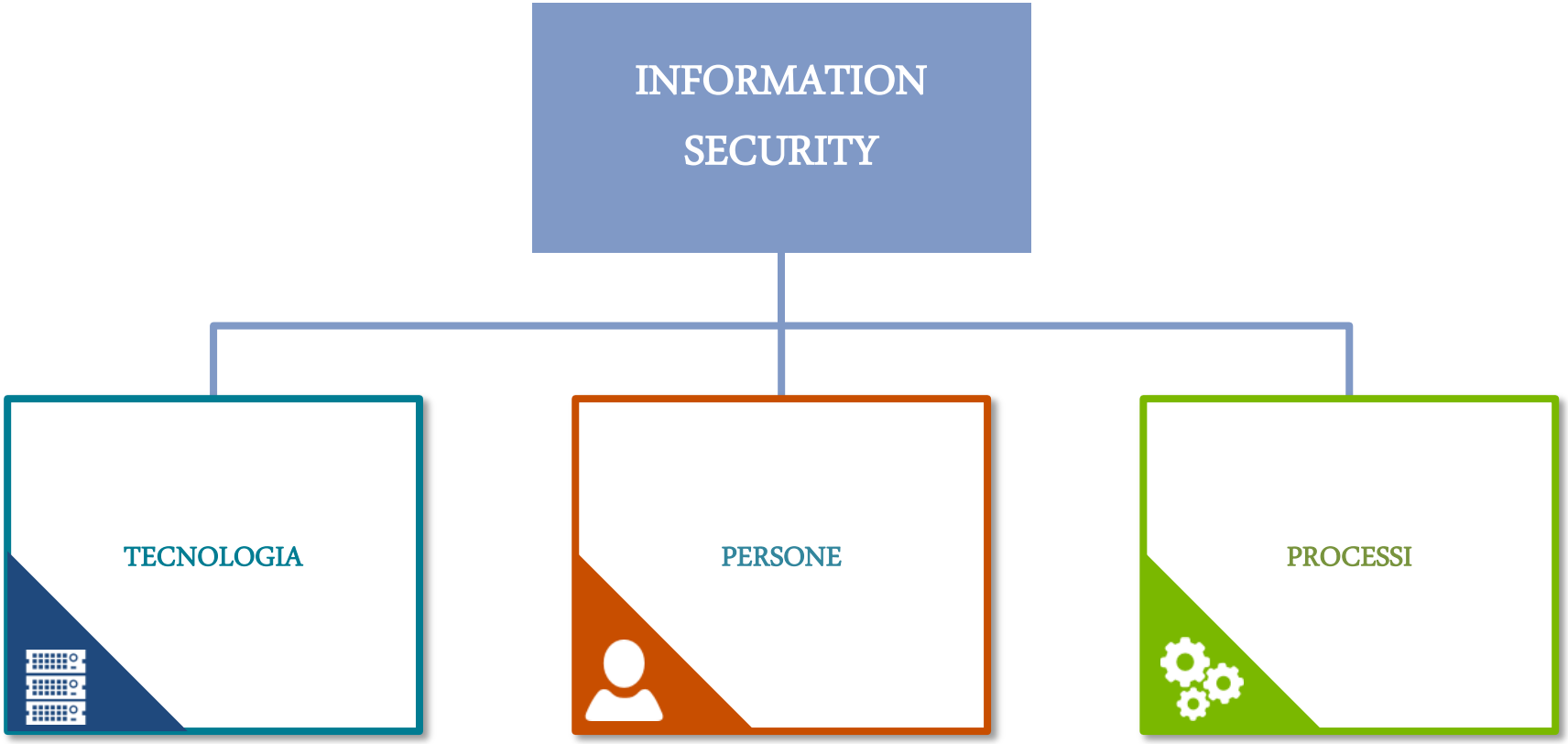
https://concorsi.difesa.it/default.aspx

Sicurezza della PA nello scenario attuale

PRINCIPALI TREND DI ATTENZIONE

La sicurezza delle informazioni

Nel seguito si rappresentano gli ambiti di applicazione della Sicurezza delle Informazioni.



Che cosa è la Cyber Security

I termini quali **cyber crime**, inteso come azioni a scopo di lucro da parte di organizzazioni criminali attuate attraverso il cosiddetto cyberspazio, oppure **cyber attack**, ovvero attacchi condotti da stati, organizzazioni o individui con scopi ostili, o ancora di **cyber warfare**, alludendo ad attacchi strutturati attuati con caratteristiche e mezzi simili a quelli del mondo militare.

Per **NIST** (National Institute of Standards and Technology) la Cyber Security va intesa come un processo finalizzato alla **protezione delle informazioni** attraverso attività di prevenzione, rilevazione e risposta ad attacchi provenienti dal cyberspazio.

Il concetto di cyberspazio viene inteso come un insieme di **infrastrutture tecnologiche interconnesse** tra di loro che include la rete **Internet**, ma si estende a tutti gli **apparati tecnologici** (sistemi di telecomunicazione, computer e loro componenti, ecc.) in grado di connettersi tra loro.

La Cyber Security focalizza la propria attenzione quindi sulle modalità più efficaci per **proteggere il patrimonio informativo ed i processi aziendali** che generano ed utilizzano tale patrimonio, al fine di preservare tutto ciò che è dipendente, e quindi vulnerabile ed a rischio, dall'ICT.

La Cyber Security si configura come un **processo** e non come una soluzione tecnologica ad un problema puramente tecnologico: i cosiddetti framework di Cyber Security, ovvero i modelli che guidano le aziende nella gestione di questa tematica complessa, sono un insieme di **attività, ruoli e responsabilità, approcci e metodologie, ed anche tecnologie**, che aiutano ogni organizzazione a definire, implementare e migliorare costantemente una **strategia di protezione adeguata** al proprio contesto.

Sicurezza della PA nello scenario attuale

Piano Nazionale…

Individua un insieme molto ampio ed articolato di interventi e linee di azione che dovranno essere realizzati coinvolgendo un elevato numero di attori secondo una logica incrementale.

Il modello per la PA

I riferimenti

- CERT Nazionale
- CERT Pubblica Amministrazione
- CERT territoriale

OGGI…

Cosa fare

- Valutazione dei rischi
- Adeguatezza dei presidi
- Piano incrementale

"Obiettivi selezionati"

Azioni e misure da attuare

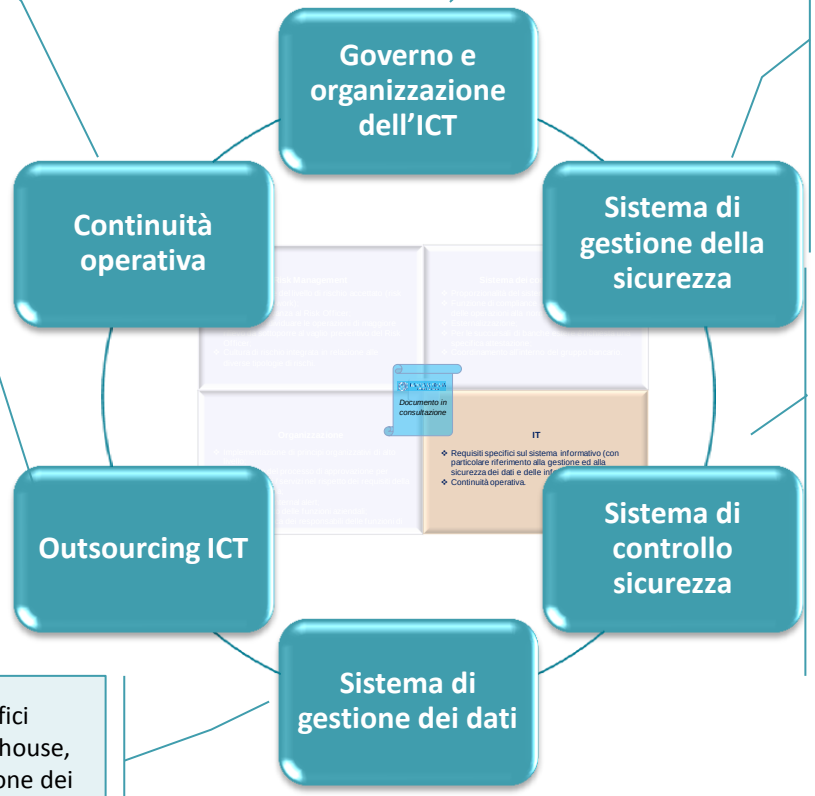
- Consapevolezza e formazione
- Prevenzione e protezione
- Reazione e contrasto

Implementare la Sicurezza delle Informazioni nella PA

Di seguito si riportano sinteticamente cosa gli Enti devono indirizzare per la **Sicurezza delle Informazioni e la continuità operativa:**

SOC e Incident Management: identificazione e comunicazione degli incidenti e dei fattori anomali rilevanti alle strutture preposte

Organizzazione della funzione di **Information and communications technology** secondo i principi generali indicati



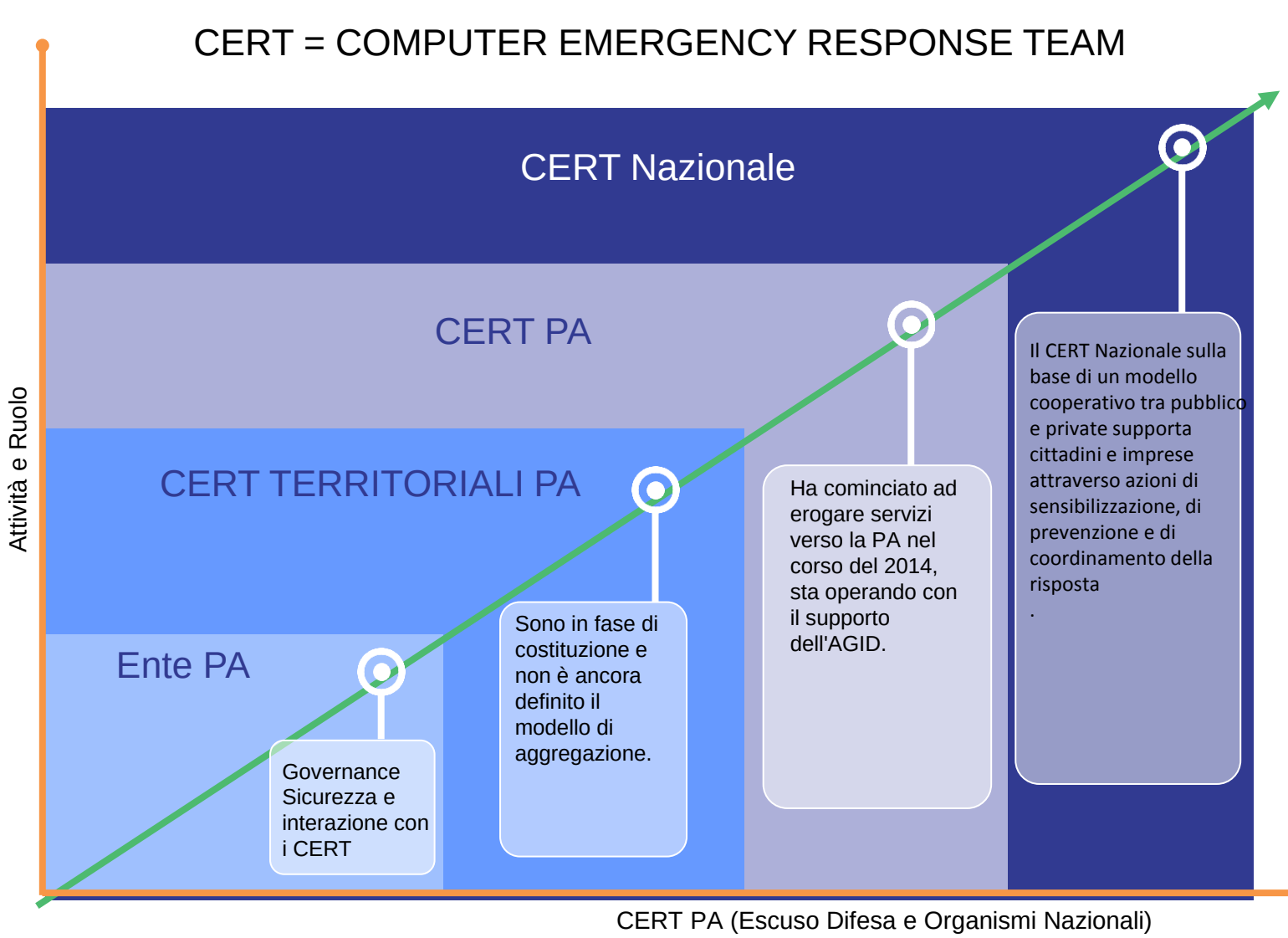
- Valutazione e gestione del rischio cui sono soggette le risorse
- Individuazione del modello organizzativo e formazione
- gestione dei cambiamenti

- Applicazione della politica di **esternalizzazione**
- Disposizione di specifiche indicazioni
- Valutazioni dei rischi connessi al *cloud computing*
- *Verifica dell'applicazione delle normative e regolamenti*

1. **Gestione sicurezza**
   Policy e strategie omunicate a tutto il personale e terze parti
2. Misure in materia di servizi offerti
3. Definizione e **controllo degli accessi** (presidi fisici, accessi logici, autenticazione, monitoraggio, tracciamento, ecc.)
4. Sicurezza dei processi

La gestione dei dati deve soddisfare specifici requisiti (es.: data governance, data warehouse, documentazione delle procedure di gestione dei dati, ecc. ...)

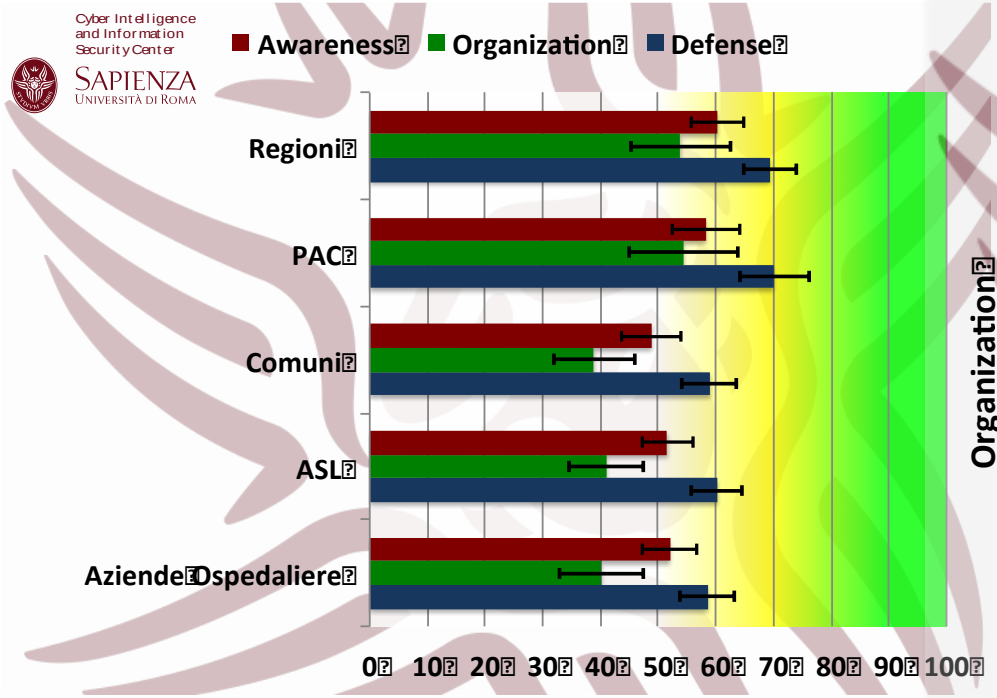
Approccio previsto dal Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico

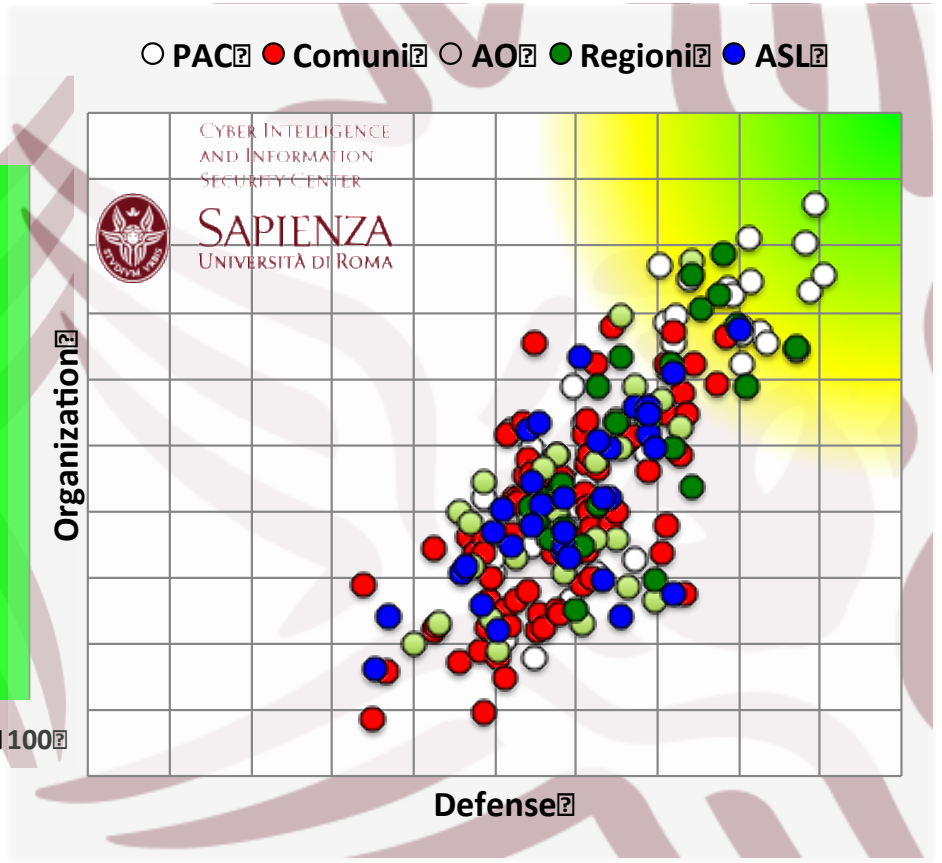


Vengono Individuate un insieme molto ampio ed articolato di interventi e linee di azione che dovranno essere realizzati coinvolgendo un elevato numero di attori secondo una logica incrementale.

Il rapporto sulla consapevolezza della minaccia e capacità difensiva della PA Italiana

A valle della pubblicazione della strategia nazionale nel 2014 intervista oltre 230 Pubbliche Amministrazioni: Regioni, Asl e Aziende Ospedaliere e altre PA locali





I principali trend che richiedono attenzione

I principali "punti di non ritorno" rappresentati possono essere raggruppati come segue:

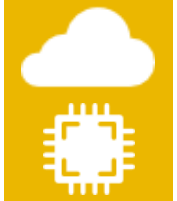
PERSONE ED INTERNET

Come le persone si connettono tra di loro, anche il il mondo attorno alla PA viene trasformato dalla tecnologia. Le tecnologie miglioreranno la "presenza digitale" e trasformeranno i servizi della PA, permettendo di interagire in modi nuovi.

ANALYTICS E BIG DATA

La digitalizzazione crea in modo esponenziale più dati – relativi a tutto e a tutti. In parallelo stanno aumentando la difficoltà dei problemi che i SW possono indirizzare in autonomia e la capacità dei SW di autoapprendimento.

ELABORAZIONE E ARCHIVIAZIONE



Oluzione delle dimensioni e del costo delle tecnologie sta guidando una crescita esponenziale del potenziale di accesso ad internet. La disponibilità di datied informazioni è sostenuta da infrastrutture che saranno consolidate offerte in modalità di servizio.

SMART CITIES

Internet sta guidando il passaggio verso modelli economici e sociali basati sulla rete che riguardano il cittadino e i servizi della PA. Gli asset creati possono essere condivisi, creando efficienza e nuovi servizi a valore.

IOT – Internet Of Things

Vengono introdotti sensori sempre più piccoli, più economici e più intelligenti - in case, abiti e accessori, in città, nelle reti dei trasporti e dell'energia, così come nei processi della PA.

DIGITALIZZAZIONE DEI PROCESSI

Gli oggetti e le informazioni fisiche vengono "sostituiti da oggetti e informazioni digitalizzati i: la trasformazione digitale oltre a creare un adeguamento delle competenze richiede un adeguamento del sistema di controllo dei rischi.

(*) dati World Economic Forum - Deep Shift Technology Tipping Points and Societal Impact - sett.2015

- **Information security e ruoli nella definizione della sicurezza**

CASI PRATICI

Sicurezza perimetrale e servizi di gestione reattiva

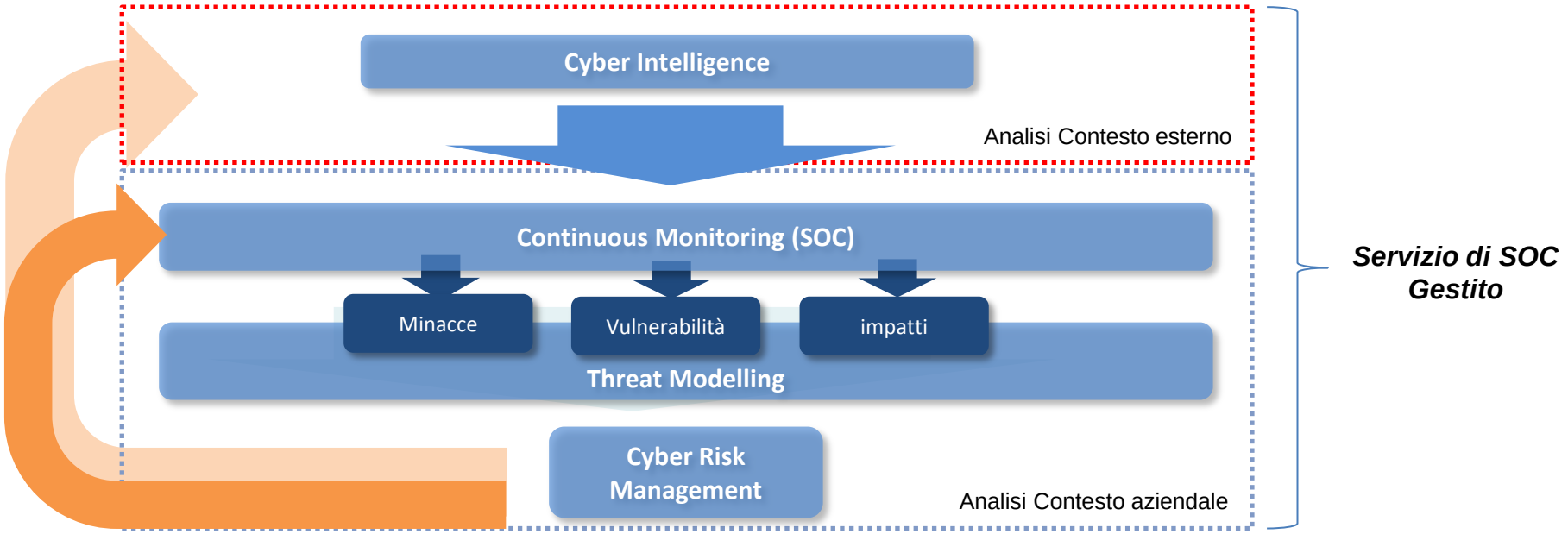
Al fine di garantire la sicurezza delle informazioni e dei sistemi informatici, sono istituiti opportuni presidi fisici di protezione con relative procedure di autorizzazione e controllo per l'accesso fisico ai sistemi informatici e alle informazioni. Queste misure sono attuate per prevenire:

- l'accesso fisico non autorizzato alle sedi, alle aree ed ai locali che ospitano asset informatici
- i danneggiamenti, la distruzione e il furto degli asset.

La protezione fisica è garantita tramite l'adozione di adeguate misure tecniche, organizzative e procedurali:

- Le aree maggiormente critiche, dette "aree sicure", sono protette mediante appropriati controlli di accesso sia in ingresso sia in uscita
- L'accesso alle "aree sicure" è consentito al personale esterno solo se strettamente necessario e deve essere autorizzato e monitorato
- I diritti di accesso alle aree sicure devono essere periodicamente riesaminati ed eventualmente revocati
- Le apparecchiature informatiche sono custodite ed adeguatamente protette da minacce fisiche e ambientali

Sicurezza perimetrale e servizi di gestione reattiva



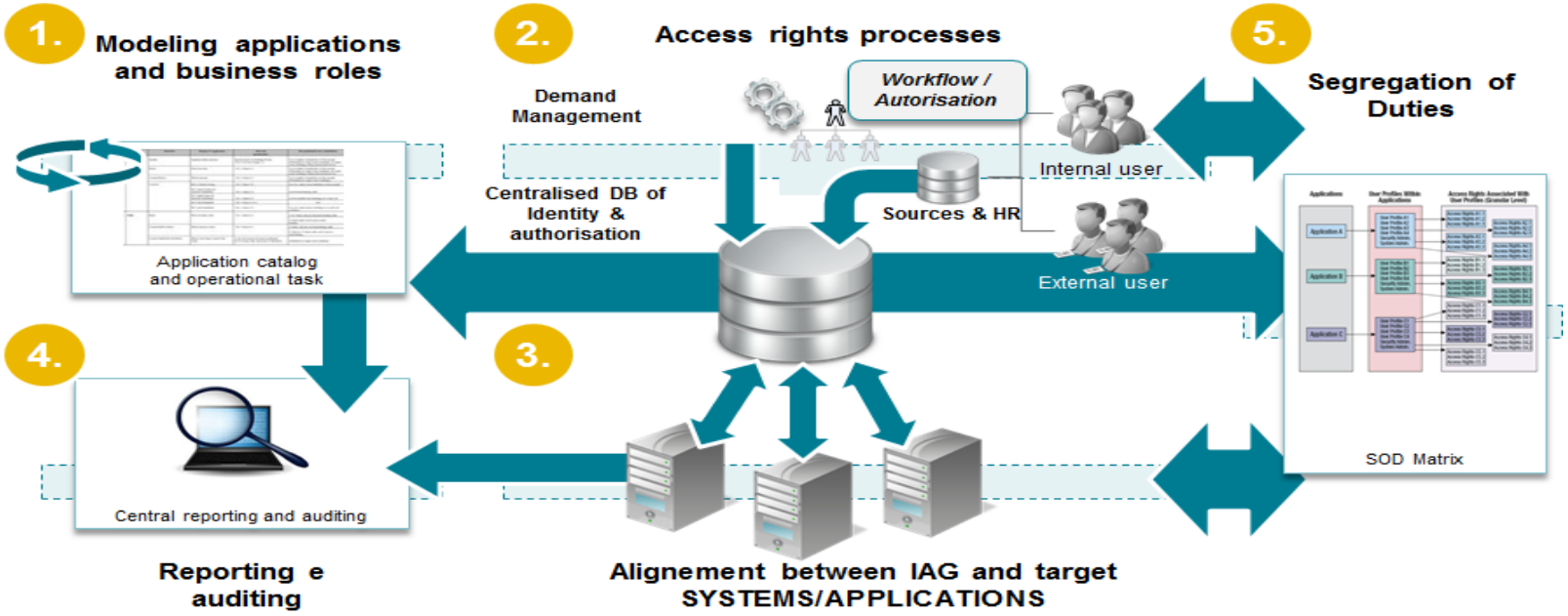
Un modello avanzato di gestione reattiva della sicurezza perimetrale (ed eventualmente anche di quella interna) si compone di:

- Un processo di Cyber Intelligence che monitora costantemente l'esterno, consentendo all'Ente di reagire con grande rapidità e di prevenire le minacce;
- Un processo di Threat Modeling che si aggiorna costantemente, il che ha importanti ricadute sia per la gestione del rischio "cyber", sia per la gestione delle vulnerabilità e della pianificazione delle azioni correttive.

La sicurezza degli applicativi e la gestione dei ruoli e dei profili

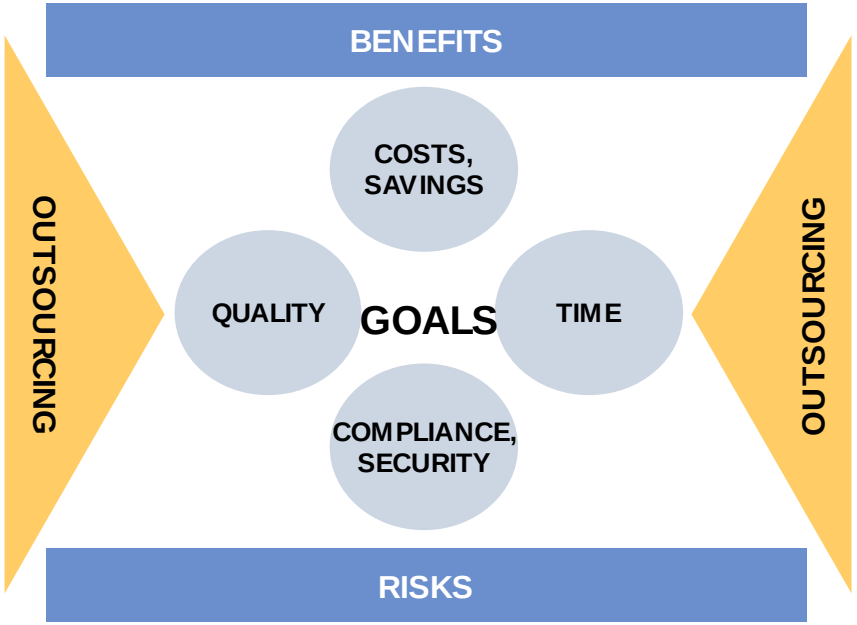
Per il governo degli accessi è necessario definire adeguati processi e regole per garantire che:

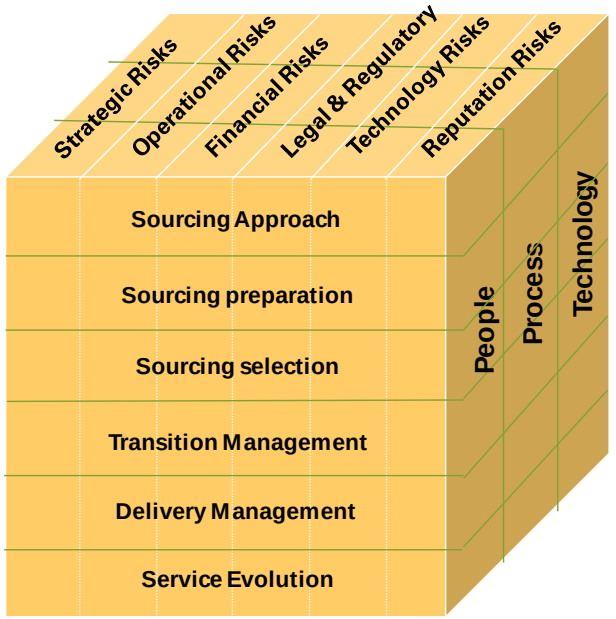
- Le abilitazioni di accesso siano nel tempo commisurate alle mansioni di chi opera
- Ogni richiesta di accesso sia monitorata in termini di chi, quando, ciò che è stato richiesto, chi ha approvato e cosa è stato concesso e di coerenza con i regolamenti e normative.
- Tutte le identità e i diritti di accesso associati siano pienamente verificabili.
- I conflitti di attività siano completamente identificati e gestiti.



Sicurezza nella gestione di outsurcer e fornitori

- Definizione dei requisiti di sicurezza e affidabilità
- Selezione del fornitore
- Gestione della transizione
- Definizione dei livelli di servizio
- Monitoraggio dei livelli di servizio e assurance dei processi
- Evoluzione dei servizi



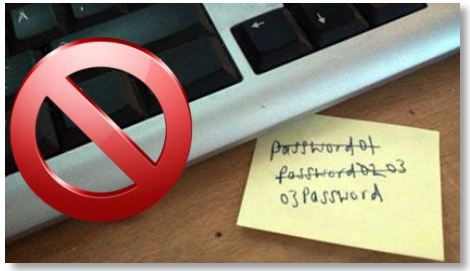


Sicurezza dei dispositivi individuali PC, Mobile,App

Spesso le informazioni sono lasciate indifese davanti a rischi di sicurezza senza neppure rendersene conto. Un atteggiamento noncurante può portare a serie conseguenze se degli estranei accedono alle nostre informazioni.

Semplici passi come scegliere password più complicate, effettuare sempre il log-out, non scriverle e lasciarle in posti di facile accesso, sono comportamenti semplici che possono davvero fare la differenza nella sicurezza.

Le password costituiscono la **PRIMA LINEA DI DIFESA** contro i criminali informatici. È fondamentale dunque che gli utenti proteggano le loro password seguendo i consigli e gli obblighi dettati in materia di sicurezza dalla normativa interna



Sicurezza dei dispositivi individuali PC, Mobile,App

La sempre più ampia diffusione dei dispositivi di mobile computing (laptop, tablet, smartphone) quali strumenti di lavoro e di accesso alle risorse informatiche aziendali, pone all'attenzione della sicurezza informatica specifici rischi connessi con l'utilizzo di tali dispositivi, richiedendo in particolare:

- l'adozione di **PARTICOLARI MISURE PER LA PROTEZIONE** dei dati memorizzati (utilizzo di crittografia, politica di password, protezione da data leakage)
- la disciplina delle **MODALITÀ DI COLLEGAMENTO** alla rete aziendale da ambienti non protetti, richiedendo la certificazione del dispositivo e delle app installate
- il ricorso, laddove fattibile, a **REGOLARI PROCEDURE CENTRALIZZATE** di aggiornamento del software installato
- l'implementazione, laddove disponibili, di funzionalità di **RIMOZIONE DEI CONTENUTI DA REMOTO** (remote wipe) da utilizzare in caso di furto o perdita del dispositivo
- l'abilitazione, a seguito di valutazioni tecniche, delle **FUNZIONALITÀ DI CIFRATURA** della memoria dei dispostivi
- la definizione di specifiche **MODALITÀ DI GESTIONE E TRATTAMENTO** degli incidenti di sicurezza informatica.

- **La gestione del cambiamento e le aspettative sulla sicurezza dei servizi offerti dalla PA a cittadino e stakeholders**

La gestione del cambiamento nella PA

Aspettative sulla Sicurezza dei servizi offerti

La sostanziale evoluzione dei servizi offerti comporta anche maggiore cooperazione tra diversi soggetti per una maggiore disponibilità di servizi a valore dove migliora la qualità e la quantità di dati e informazioni.

La protezione delle informazioni e la sicurezza del territorio è un cardine della tutela dei diritti di cittadini e stakeholder e pone alla PA una forte enfasi al tema della sicurezza .

Guardando al panorama italiano, sicuramente c'è molta strada da fare per garantire le aspettative; per accelerare questo percorso si possono dare alcune priorotà:

- il personale deve essere sensibilizzato per comprendere come il tema della Security rappresenti un rischio da indirizzare e non un problema confinato all'interno del mondo IT;
- a seconda dello specifico contesto di in cui opera l'ente, è prioritario analizzare tutte le implicazioni di sicurezza legati ai requisiti con cui disegnare e integrare i processi e le interazioni con terzi nel rispetto della normativa;
- Occorre definire una strategia per gestire i rischi con un adeguato sistema di controlli e con aggiornamenti periodici su sull'evoluzione nella gestione di tale tipologia di rischi; a cui va aggiunto un monitoraggio continuo del contesto di riferimento, vista la complessità e la dinamicità del tema.