REGIONE PIEMONTE

La gestione di un attacco cyber: l'incident response plan e la notifica di data breach

Torino 25 Maggio 2022 | 10:00 - 11:30

Cyber Exposure

Nel 2022 gli attacchi nel mondo sono **in costante aumento**, e sono sempre più gravi.
Le nuove modalità di attacco dimostrano che i cyber criminali sono sempre più sofisticati e in grado di fare rete con la criminalità organizzata (Clusit Report 2022)

Gli attacchi crescono in **quantità e in "qualità"** e dipendono anche da situazioni Geopolitiche come dimostrano i recenti accadimenti legati al conflitto Russia-Ukraina.

AGENZIA CYBERSECURITY

Minacce cyber all'Italia, allerta del Governo per possibili attacchi sofisticati

13 Mag 2022

CYBER GUERRA

Attacco cyber dalla Russia all'Italia: down siti Senato, Difesa, perché è evento grave

11 Mag 2022

CIRCOLARE AGENZIA CYBER

Diversificare prodotti e servizi tecnologici russi: implicazioni per la PA

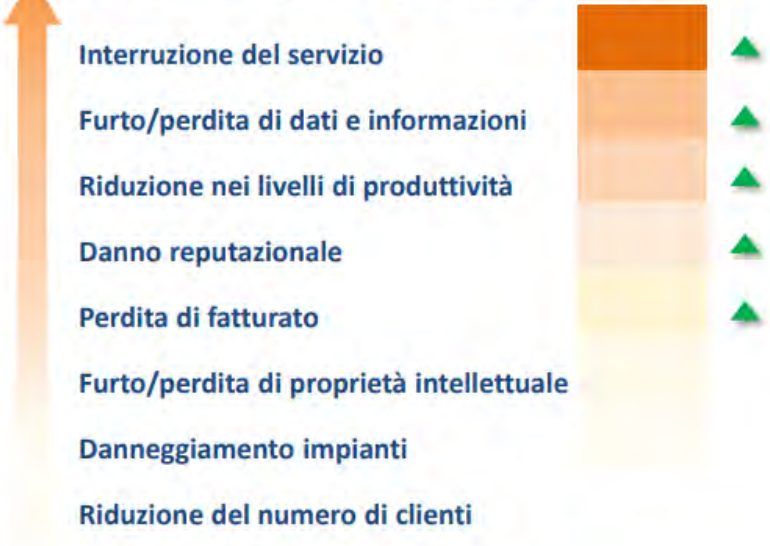
28 Apr 2022

CYBERSECURITY360

Cyber Exposure

Quali sono stati i principali impatti degli attacchi portati a termine con successo?

da = nessun impatto a = impatto molto rilevante



Fonte: NetConsulting cube, Barometro Cybersecurity 2021

PA, Difesa e Sanità i settori più colpiti e con un trend in aumento rispetto allo scorso anno

I ransomware sono cresciuti del +422% tra febbraio 2020 e maggio 2021, l'Italia risulta 4°paese europeo colpito da questa tipologia di attacchi

Ultimi dodici mesi in incremento di attacchi veicolati tramite l'abuso della supply chain

dal 1° agosto 2020 al 31 luglio 2021, oltre 10 volte il numero rilevato per lo stesso periodo l'anno precedente.

Fonte: Viminale

La sicurezza al centro dei processi

Centralità nei processi: la Sicurezza informatica deve divenire parte integrante dei processi, a partire dalle fase iniziali di progettazione e di sviluppo di nuovi sistemi o servizi.

Ridisegnare il modello operativo, la struttura organizzativa e i processi critici: l'organizzazione deve prevedere l'inserimento nei diversi Team di risorse esperte in materia di Sicurezza informatica, in grado di supportare i nuovi progetti sin dalle fasi di disegno.

Security by Design & by Operation: l'inserimento di competenze specifiche a supporto delle diverse strutture garantirà non solo il rispetto dei principi della Security by Design (***fase preliminare***), ma anche il mantenimento degli stessi a livello operativo nelle successive fasi (***fase operativa***).

Gli interventi PNRR sulla cybersicurezza

Il PNRR prevede interventi sulla sicurezza per oltre **600 milioni** (M1C1.1.5), ma interamente declinati **a livello nazionale**:

- Realizzazione di servizi nazionali di cybersecurity (rilevamento, gestione e mitigazione del rischio a livello nazionale)
- Rafforzamento delle capacità nazionali di scrutinio e certificazione tecnologica di beni, sistemi e servizi ICT (Centro di Valutazione e Certificazione Nazionale)
- Potenziamento delle capacità cyber della Pubblica Amministrazione per la messa in sicurezza dei dati e dei servizi dei cittadini

Avviati i primi avvisi per la realizzazione di interventi di potenziamento della resilienza cyber (riservati agli **organi costituzionali**, alle **agenzie fiscali** ed alle **PAC** facenti parte del Nucleo per la cybersicurezza)

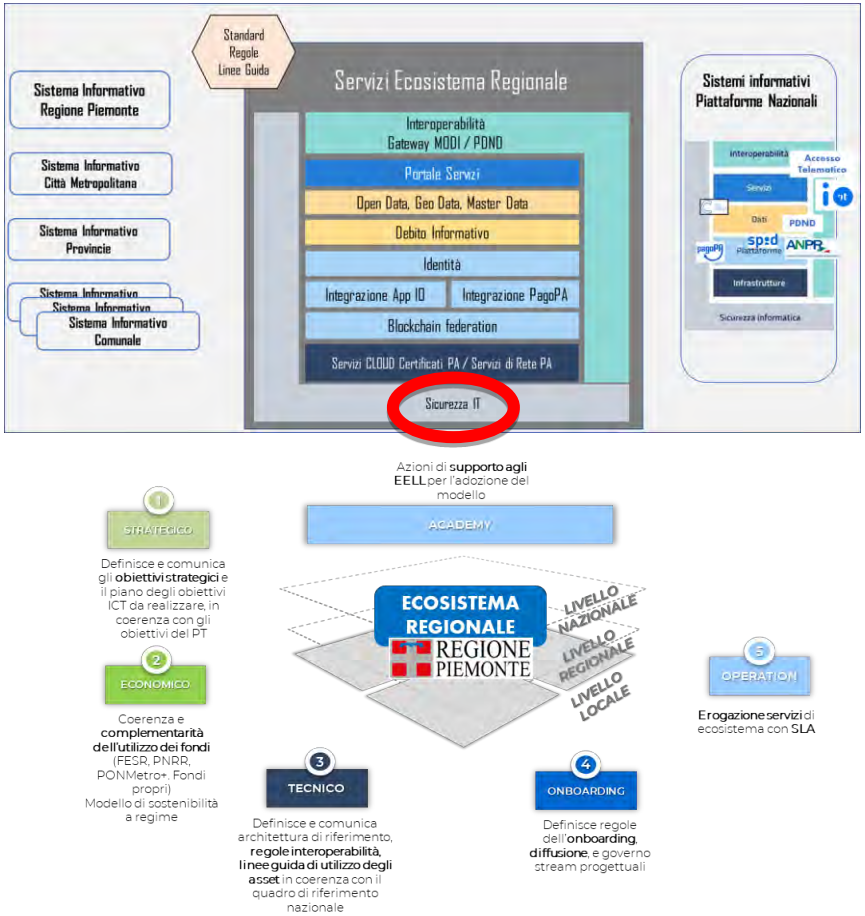
Non sono previsti interventi specifici per il rafforzamento della sicurezza cibernetica a livello di Regioni ed EE. LL. (coerentemente con il fatto che i dati della PAL non sono classificati come «strategici» o «critici»)

Spazio per rendere più sicuri i SI degli EE. LL. attraverso una attenta progettazione degli **investimenti dei «voucher»**, in particolare

- 1.2 Transizione al cloud: modello di **cloud security** precedentemente descritto, ma anche reingegnerizzazione e/o sostituzione di applicativi vulnerabili con soluzioni adeguate ed aggiornate anche dal punto di vista della sicurezza
- 1.4.4 Adozione di SPID/CIE: con l'adozione di strumenti di identità digitale sicuri si possono ridurre le minacce legate a vulnerabilità o phishing

Sicurezza ed ecosistema digitale regionale

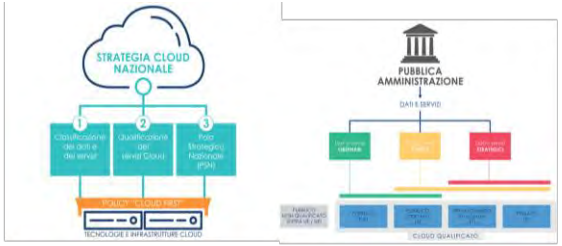
- Le piattaforme regionali disponibili per gli EE. LL. garantiscono già oggi **elevati standard di sicurezza**
- Attraverso i finanziamenti del **PNRR** e del **FESR** 21-27 se ne prevede l'ulteriore **rafforzamento ed evoluzione** a favore del sistema degli EE. LL.
- Trasformazione progressiva in un vero e proprio **ecosistema digitale regionale** partecipato da Regione ed EE. LL.
- **Standard e regole di adesione** dell'ecosistema garantiscono la **sicurezza collettiva** dei soggetti partecipanti



Strategia Cloud Italia

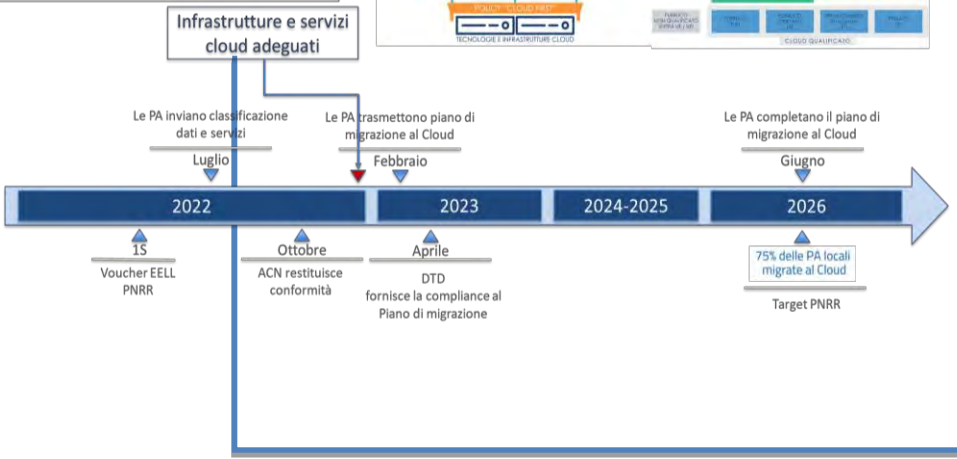
Obiettivi Strategia Cloud

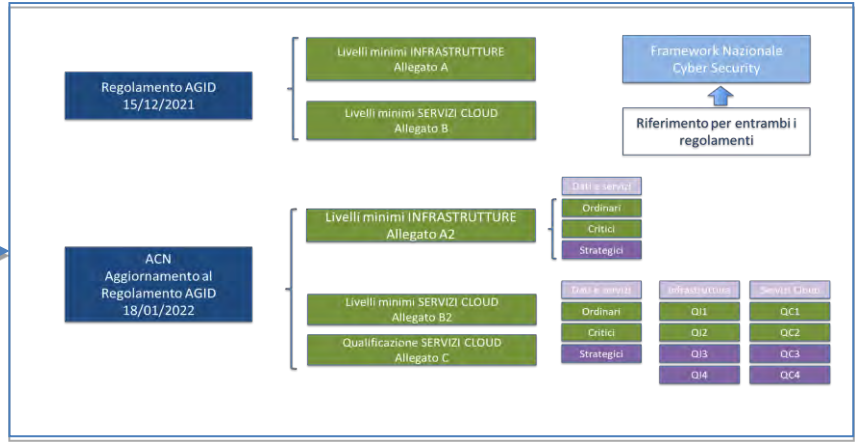
- Dismissione DC Gruppo B
- Adeguamento livelli minimi Infrastrutture Gruppo A
- PSN: migrazione DC gruppo B PA centrale + 80ASL
- Censimento dati e servizi della PA
- Qualificazione CSP secondo criteri ACN in linea con la classiificazione dati e servizi



AGENZIA PER LA CYBERSICUREZZA NAZIONALE

AGID | Agenzia per l'Italia digitale
www.agid.gov.it





Adempimenti minimi per servizi Ordinari e Critici

La classificazione dei dati e dei servizi: il contesto di riferimento

- Nel corso degli ultimi anni le Regioni e Province Autonome hanno effettuato **investimenti consistenti per consolidare le infrastrutture** dedicate ad ospitare i sistemi e i servizi essenziali per l'azione amministrativa degli Enti
- **Tali infrastrutture rappresentano un asset rilevante** nei territori sui quali insistono e, alla luce dei nuovi regolamenti ACN, devono essere adeguate ai requisiti per il trattamento di dati e servizi critici ed ordinari
- Il **Decreto dell'ACN del 18 Gennaio 2022** e relative circolari, concernente la qualificazione dei servizi e delle infrastrutture cloud della Pubblica Amministrazione, hanno profondamente rivisto il quadro di classificazione delle infrastrutture digitali richiedendo di conseguenza importanti interventi tecnici ed organizzativi alle singole amministrazioni

La classificazione di dati e servizi è propedeutica alla partecipazione agli avvisi pubblici dedicati al cloud per beneficiare delle risorse del PNRR e **fissa al 18 luglio la scadenza per l'azione di classificazione dei dati**

La classificazione dei dati e dei servizi: l'azione di Regione Piemonte

- **Regione Piemonte, congiuntamente con Regione Emilia-Romagna e Regione Toscana**, ha formalizzato una richiesta alla Commissione per l'Innovazione tecnologica e la Digitalizzazione per **l'attivazione di un tavolo tecnico e di co-progettazione** finalizzato alla definizione di un percorso condiviso fra le Agenzie nazionali (ACN in primis), il Dipartimento stesso e le Regioni/Prov. Autonome, **con l'obiettivo di mettere queste ultime nelle condizioni di poter evolvere i rispettivi sistemi cloud** in linea con le aspettative e le indicazioni di elevata sicurezza ed affidabilità definite dall'ACN a Gennaio 2022

- il suddetto tavolo tecnico dovrebbe inoltre **integrare la strategia nazionale per il cloud** in modo che sia prevista ed abilitata, per i soli dati ordinari e critici, la presenza di un numero limitato di infrastrutture cloud territoriali regionali che fungano da un lato da aggregatori di enti di piccole e medie dimensioni

- il percorso dovrebbe prevedere una **tempistica sostenibile ed una scadenza coerente** per l'adeguamento dei sistemi regionali al fine di garantire la **continuità dei servizi digitali** essenziali attualmente erogati dai sistemi regionali a cittadini, imprese ed altri enti territoriali, ed al contempo garantire una **coerenza con i finanziamenti europei e locali** che ne hanno sostenuto fin qui il consolidamento

- Lo stesso percorso sarebbe ancora più utile per **affrontare ambiti** particolarmente **delicati**, come quello sanitario, su cui la discussione è tutt'ora aperta.