Liguria Digitale

Gestione incidenti cyber
Punto di vista di Liguria Digitale
Incontro CSI – 22 aprile 2024

Ing. Sandro Pellerano

Liguria Digitale

LIGURIA DIGITALE

Liguria Digitale è la società ICT ***in-house*** che sviluppa la **strategia digitale** della Regione Liguria e degli enti soci.

Garantisce **soluzioni** e **infrastrutture tecnologiche** all'avanguardia e **servizi digitali** efficaci, integrati e facilmente accessibili per **cittadini, imprese, enti.**

DATA CENTER

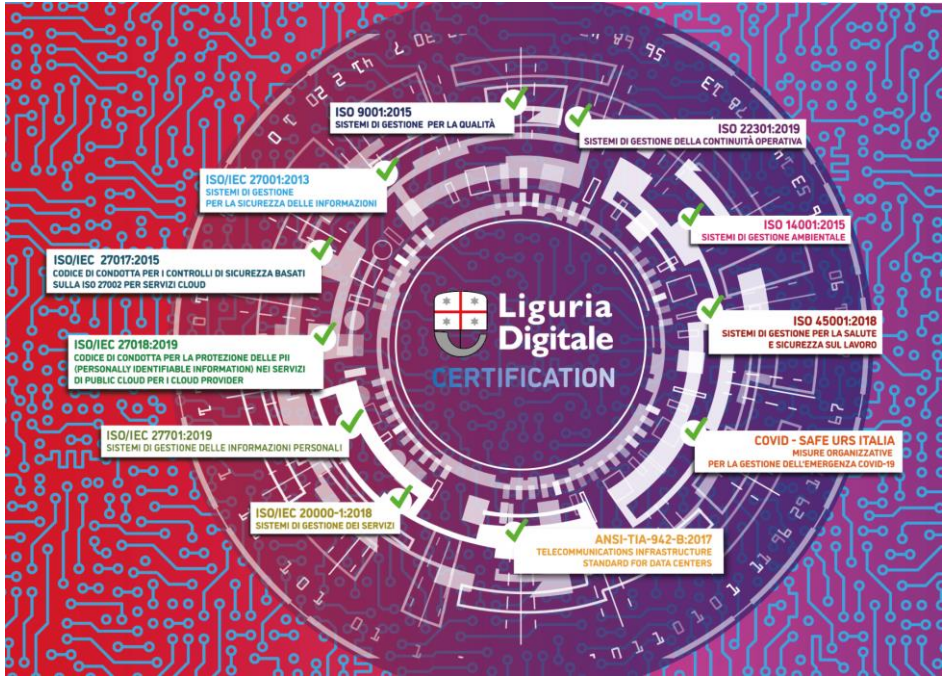
Il **Data Center** di Liguria Digitale è il luogo fisico che ospita i **server** che raccolgono i **dati** di gran parte della **pubblica amministrazione ligure**.

Si tratta di **un'infrastruttura** che si estende per circa **2000m²** e ospita oltre **4000 server** (tra fisici e virtuali), più di **100 km di cavi** in fibra e rame, oltre **8000 TB di storage**.

CERTIFICAZIONI DEL SISTEMA DI GESTIONE INTEGRATO

Il Data Center di Liguria Digitale è dotato di un **Sistema di Gestione Integrato** certificato in conformità a diverse norme, tra cui:

- **ISO/IEC 27001:2013** Sistema di gestione della sicurezza delle informazioni.
- **ISO/IEC 27017:2015 - 27018:2019** sicurezza delle informazioni e protezione dei dati personali per i servizi in cloud
- **ISO/IEC 20000-1:2018** Sistema di gestione dei servizi
- **ISO 22301** Sistema di gestione della continuità operativa



SECURITY OPERATION CENTER (SOC)

Il SOC di Liguria Digitale è operativo dal 2018 presso la sede di Erzelli in un'area dove sono state **centralizzate** le tecnologie e le informazioni sullo **stato di sicurezza** dell'infrastruttura informatica.

Attualmente è formato da un team di persone specializzate e dedicate alle attività di:

- **Gestione tecnologie** di sicurezza;
- **Monitoraggio**, alerting e information sharing;
- **Analisi** minacce e **risposta agli incidenti** di sicurezza informatica.

I SISTEMI DI SICUREZZA:

- Raccolgono più di **1 milione** di eventi di sicurezza al giorno da **4 mila** device
- Monitorano **30 mila** postazioni, da più di **30** enti
- Bloccano più di **5 mila** email di spam/phishing

GLI ANALISTI DEL SOC:

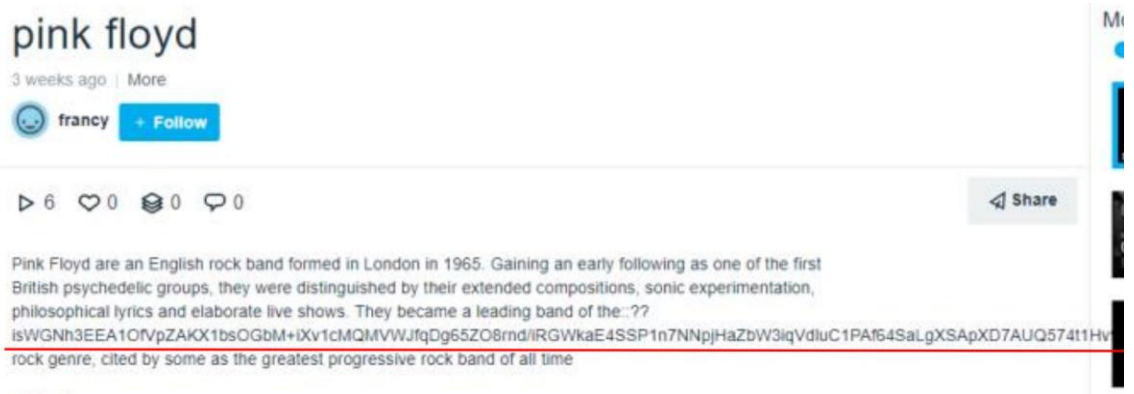
- Gestiscono mediamente **2 incidenti** di sicurezza rilevanti al giorno
- Analizzano e gestiscono **decine** di alert e segnalazioni derivanti dai sistemi
- Condividono regolarmente IoC con le autorità

La nostra gestione incidenti

- Compliance con norme e standard (ISO27001, CSA Star, linee guida…)
- Attivazione CSIRT ad-hoc
- Coinvolgimento di molteplici parti:
  - Dirigenza
  - Comunicazione
  - Gestori Data Center
  - Gruppo privacy e DPO
  - Autorità competenti
  - Etc… tutte le azioni coordinate dal CISO
- Flusso ben delineato INPUT-OUTPUT → prevedere le varie casistiche tipiche di *in-house.*

TIPO 1: «vimeo hack»

- Scatta un alert da **USB** sui nostri sistemi nel 2021 → probabile estensione su tutto il territorio.
- Analisi malware condivisa con PP e ACN.
- Comunicazione con tutti gli enti.



Un anno dopo articolo Mandiant!

TIPO 2: Attacchi DDoS NoName057

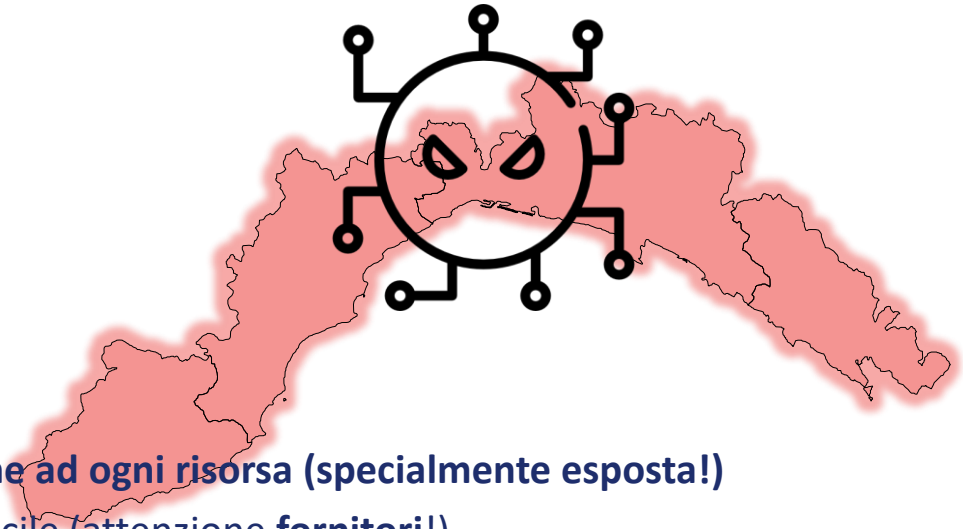
- Sistema di ricezione delle segnalazioni/threat intelligence
- Questione mediatica → focus sulla comunicazione
- Playbook gestione DDoS (limiti geografici, bilanciatori…)
- Efficiente collaborazione inter-istituzionale

TIPO 3: Incidenti gravi su AdS

Incidente #1 → ransomware su file server + mimikatz
Incidente #2 → server esposto con credenziali *default*

ACTIONS

- Checklist azioni ravvicinate, monitoraggio continuo;
- Coinvolgimento autorità per analisi ad alto carattere tecnico;
- Priorità → rimettere in piedi i servizi.



KEY TAKEAWAYS:

- **Gestione complessa del perimetro, attenzione ad ogni risorsa (specialmente esposta!)**
- Coordinamento necessario ma non sempre facile (attenzione **fornitori**!)

Liguria Digitale

Grazie per l’ascolto

Ing. Sandro Pellerano