Liguria Digitale

Cybersecurity: le priorità dell'Agenda Digitale nella Regione Liguria

Ing. Sandro Pellerano

Liguria Digital Summit, 13 Dicembre 2018

Agenda

- Evoluzione delle minacce
- Control Room Liguria: SOC e NOC
- Misure tecnologiche
- Misure organizzative

Liguria Digitale

Liguria Digitale, come società in House di Regione Liguria, fornisce servizi tecnologici, consulenza e soluzioni innovative a Pubbliche Amministrazioni, ASL e Ospedali Liguri e Cittadini.

	**Fascicolo Sanitario Elettronico** E' l'insieme di dati e informazioni cliniche di ogni paziente; contiene documenti di tipo sanitario, amministrativo, prescrizioni mediche e farmaceutiche.
	**Ricetta Dematerializzata** I medici di medicina generale ed i pediatri di libera scelta prescrivono i farmaci e le prestazioni specialistiche con la ricetta dematerializzata che sostituisce la ricetta rossa.
	**PagoPA** La Liguria è stata una delle prime Regioni ad avere un Nodo regionale dei pagamenti, dove tutti i servizi del territorio si collegano per consentire ai cittadini ogni metodo di pagamento elettronico, anche senza carta di credito.
	**Server Farm** Infrastruttura tecnologica che offre una serie di soluzioni complete, integrate e flessibili per adattarsi alle esigenze di ogni tipologia di cliente: Cloud Computing, Housing, Hosting, Outsourcing.
	**SPID** Identità digitale per i cittadini liguri. SPID, Sistema Pubblico di Identità Digitale, è la soluzione nazionale per accedere a tutti i servizi online della pubblica amministrazione e dei privati con un'unica credenziale sicura.

I target degli attacchi

AZIENDE PUBBLICHE E PRIVATE

PERSONE

OPERATORI DI SERVIZI ESSENZIALI

- Energia (elettricità, petrolio, gas)
- Trasporti (ferroviari, aerei, vie d'acqua)
- Banche e società finanziarie
- Salute (ospedali, cliniche private)
- Acqua (fornitura e distribuzione)
- Infrastrutture digitali (IXP, DNS, TLD)

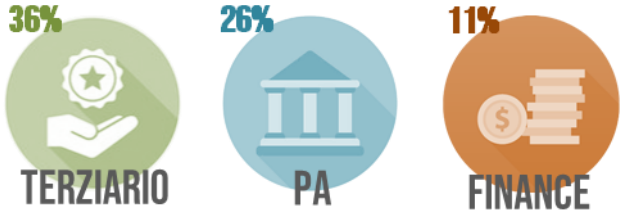
ORGANI GOVERNATIVI E MILITARI

Trend delle minacce

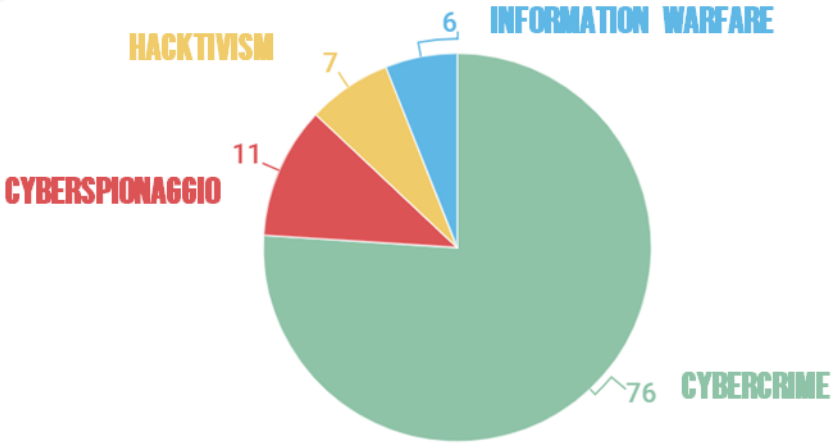
Il **cybercrime** (attacchi tesi a sottrarre informazioni e/o denaro) è la prima causa di attacchi a livello mondiale. La quasi totalità del **cyberspionaggio** e dell'**information warfare** rientra all'interno degli attacchi critici, che maggiormente mettono a rischio capitale, dati e reputazione.

1 azienda vittima di cybercrime ogni **5 minuti**

Top settori colpiti



Finalità degli attacchi



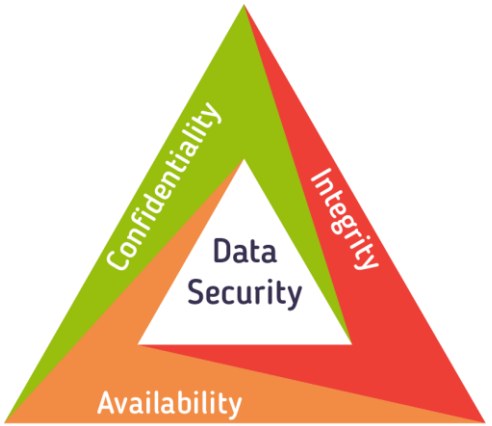
Control Room Liguria

A partire dalla fine del 2017, Liguria Digitale ha avviato la realizzazione di una **Control Room allo stato dell'arte**, centralizzando **tecnologie e competenze** relative a sicurezza informatica, gestione di sistemi e infrastrutture di rete, monitoraggio e risposta agli incidenti.

La **Control Room** è una infrastruttura tecnica di alto livello gestita da un gruppo di specialisti ed è composta da:

- **Security Operations Center (SOC)**
- **Network Operations Center (NOC)**

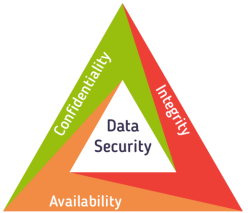
- **Riservatezza**
- **Integrità**
- **Disponibiltà**



Network Operations Center (NOC)

Il Network Operations Center è il centro operativo da cui viene **gestita, controllata e monitorata la funzionalità fisica e logica di servizi e infrastruttura di rete**.

La sua funzione principale è quella di mantenere l'operatività dell'infrastruttura rispetto degli SLA dei servizi gestendo gli incidenti in modo da ridurre i downtime.



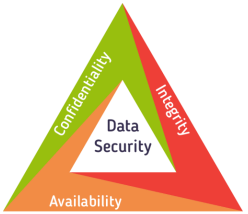
- Riservatezza
- Integrità
- **Disponibilità**

Componenti e attività:

- Monitoraggio della rete
- Disponibilità e prestazioni di sistemi e applicazioni
- Conformità degli SLA e limitazione dei downtime
- Monitoraggio del Data Center (temperatura, alimentazione elettrica, rilevamento di fumo e acqua)
- Videosorveglianza

Security Operations Center (SOC)

Il Security Operations Center di Liguria Digitale è il centro unico di gestione delle problematiche di sicurezza a livello tecnico e organizzativo attraverso strumenti e soluzioni per la **prevenzione e il trattamento di incidenti di sicurezza IT**.



- **Riservatezza**
- **Integrità**
- **Disponibilità**

Elementi e attività:

- Antispam
- Next-Generation Firewall
- Security Information and Event Management (SIEM)
- Endpoint detection and remediation
- Vulnerability assessment / management
- Gestione degli incidenti
- Threat intelligence
- Computer forensic
- Policy e procedure di sicurezza

Liguria Digitale

Misure tecnologiche

Antispam	Intercettazione di e-mail dal contenuto sospetto, allegati o URL, attraverso tecnologie antimalware e di intercettazione di phishing.
Endpoint detection and remediation	Sistemi avanzati di protezione degli endpoint in grado di rilevare minacce e applicare rimedi automatici in caso di attacchi tradizionali e avanzati, quali zero-day, ransomware, rootkit, trojan, virus e worm.
Next-Generation Firewall	Sistemi firewall tradizionali con funzionalità di deep packet inspection (DPI) e intrusion prevention system (IPS).
SIEM	Raccolta log dall'infrastruttura IT (client, server, database, applicazioni, dispositivi di rete e di sicurezza), monitoraggio real-time e correlazione di eventi finalizzata all'identificazione di potenziali minacce e attività sospette.
Vulnerability management	Processo continuo di identificazione, classificazione in base al rischio, risoluzione e mitigazione di vulnerabilità su sistemi e applicazioni.

Misure organizzative

Misure organizzative in grado di assicurare un livello di sicurezza adeguato al rischio:

- **Certificazione ISO 9001 e 27001 di server farm e servizi control room**
- **Analisi del rischio**
- **Gestione degli incidenti**: Identify, Protect, Detect, Respond and Recover (come indicato nel Cybersecurity Framework 2015)
- Protocollo di intesa con la **Polizia Postale e delle Comunicazioni della Liguria** per la prevenzione di attacchi informatici su sistemi critici di Regione Liguria (Information sharing, notifica di emergenze relative a vulnerabilità, minacce e incidenti, identificazione di sorgenti di attacco)
- **Training** e **awareness**
- **Policy e procedure di sicurezza** per lo sviluppo del Sistema di Gestione della Sicurezza delle Informazioni (SGSI)
- Completamento del progetto di **Risk Assessment & Business Continuity**

Liguria Digitale

Grazie

s.pellerano@liguriadigitale.it