Liguria Digitale

Cyber security: guardie e ladri ai tempi di internet

Enrico Castanini, Direttore Generale

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.**

Liguria Digitale

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 **2000 m²** e ospita **4000 server** (tra fisici e virtuali), più di **100 km di cavi** in fibra e rame, oltre **8000 TB di storage**.

TRAFFICO DATA CENTER

Circa **9.500** utenti

Oltre **10.000** client di rete

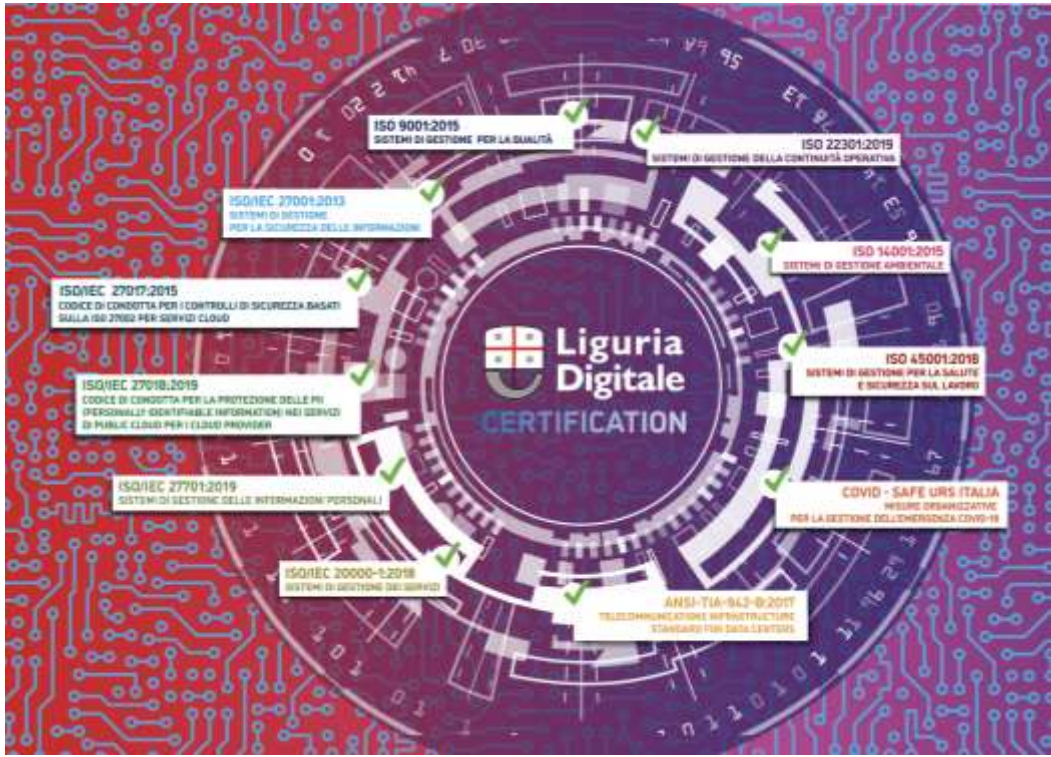
Circa **10.000** indirizzi e-mail

Oltre **200.000** e-mail ogni giorno

CERTIFICAZIONI DI QUALITÀ

Tra i **primi in Italia**, il **Data Center** di Liguria Digitale ha ottenuto diverse **certificazioni,** tra cui:
ISO 14001:2015 “Sistema di Gestione Ambientale”
ISO 45001:2018 “Sistemi di Gestione per la Salute e Sicurezza sul lavoro”
ISO 27001:2013 “Sistemi di Gestione per la sicurezza delle informazioni ”

A queste si sono aggiungono anche **le certificazioni** per il **Sistema di Gestione Integrato.**



Liguria Digitale

SECURITY OPERATION CENTER

Il **SOC – Security Operation Center -** è la struttura dove vengono **centralizzate** tutte le informazioni sullo **stato di sicurezza** dell'IT e viene costantemente controllato quello che avviene a livello di **traffico dei dati**.

Il SOC tratta la **sicurezza di primo livello**, dai firewall alle tecnologie "anti-intrusione".

Liguria Digitale

NETWORK OPERATION CENTER

Il **NOC – Network Operation Center -** è un'unità costituita da un insieme di **persone, processi e tecnologie** che, internamente all'azienda o da remoto, **presidia reti e infrastrutture**.

Lo scopo del NOC è vigilare sul **corretto funzionamento di apparati di rete e server fisici e virtuali**.

Insieme di **strumenti** e **tecnologie** per proteggere i sistemi informatici dagli attacchi dall'esterno.

Nella **cyber security** sono presenti elementi **organizzativi**, **tecnici**, **giuridici** e **umani** in grado di analizzare e **proteggere** i punti vulnerabili di un sistema, le **minacce** e i **rischi** associati.

Liguria Digitale

ATTACCHI NEL MONDO

In media, **ogni 10 secondi,** un'organizzazione nel mondo è vittima di un **attacco ransomware**.
Una misura che rende l'idea di quanto questa tipologia di **attacco informatico** sia diventata frequente.

Liguria Digitale

ATTACCHI NEL MONDO

Nel **2020** i **cyber attacchi** gravi a livello globale sono cresciuti del **29%** rispetto all'anno precedente.

Il **53%** di questi ha avuto un impatto "alto" o "critico", mentre tra i **bersagli più colpiti** - per effetto della pandemia - figurano sempre di più i settori **"healthcare"** (12%) e **"research/education"** (11%).

Fonte: **Rapporto Clusit 2021**

Liguria Digitale

ATTACCHI ALLE AZIENDE

Fonte: **Trend Micro**

L'**84% delle aziende ha subito un attacco di phishing o ransomware nell'ultimo anno** e la metà non riesce a contrastare efficacemente queste minacce.

La crescita del **lavoro da remoto** ha aumentato il **numero degli attacchi**.

Liguria Digitale

ATTACCHI ALLA PUBBLICA AMMINISTRAZIONE

1.871 gli attacchi gravi di dominio pubblico, con un **incremento del 12%** rispetto al 2019. In aumento gli **eventi di spionaggio cyber**, con il vaccino Covid-19 nel mirino dei criminali.
Nel settore della **sanità**, il **55%** degli attacchi a tema Covid-19 è stato perpetrato a scopo di cybercrime, ovvero **per estorcere denaro**; con finalità di "Espionage" e di "Information Warfare" nel 45% dei casi.

Fonte: **Rapporto Clusit 2021**

Liguria Digitale

LA SITUAZIONE IN LIGURIA

Tra **16.000 e 19.800** i messaggi di **spam** e i **virus** identificati **ogni giorno** da Liguria Digitale nel 2021 sulla posta di: Regione Liguria, Asl3 e Liguria Digitale.

Rispetto al **2019**, sono **aumentate del 50% le criticità relative alla cyber security**, anche se con un lieve calo rispetto al periodo del lockdown.

Liguria Digitale

PHISHING E POSTA CERTIFICATA

Persiste il **phishing**, la **truffa digitale** che cerca di ottenere dati personali e accessi a conti correnti, veicolato attraverso messaggi di posta elettronica e anche via **pec**.

La **posta certificata**, in genere considerata più sicura, può indurre gli utenti ad **aprire i messaggi** e cadere nella **trappola**.

SEGNALAZIONE VIRUS E DOMINI PERICOLOSI

Nel **2019** il team di **SOC&NOC** ha scoperto la nuova versione di un **virus** e lo ha segnalato a **Microsoft.**

Liguria Digitale fornisce frequentemente segnalazioni anche a **fornitori di firewall** per identificare i **malicious website** (domini pericolosi).

LIGURIA DIGITALE

Virus stanato, minacciava i computer della Regione

È un Emotet, virus che ruba credenziali e si diffonde via mail. Lo hanno scoperto al "Security Operation Center" di Liguria Digitale. Saputo della scoperta, Microsoft ha aggiornato il suo sistema antivirus.

SIMULAZIONI E CAMPAGNE DI PHISHING

Il **team del SOC&NOC di Liguria Digitale** è costituito in gran parte da **giovani ingegneri** affiancati da **figure senior** e dal **CISO**, il responsabile dell'**information security** in azienda.

Tra le varie attività che svolge, il team simula **attacchi hacker** e **campagne di phishing mirate** in base alla competenza dei lavoratori, come suggerito anche da **Agid,** per aumentare la **consapevolezza degli utenti** e sensibilizzarli sui temi della **sicurezza**.

Liguria Digitale

MISURE TECNOLOGICHE E ORGANIZZATIVE

- **Protezione endpoint avanzata** (soluzioni di tipo Endpoint Protection and Response)
- **Awareness**, prevista dal piano triennale AgID
  - Phishing assessment
  - Formazione
- Collaborazione con **Polizia Postale** e intesa (in corso)
- **Monitoraggio SOC e information sharing** per soci e clienti

TARGET DEGLI ATTACCHI

Nelle aziende il **target** degli **attacchi** sono in genere i **dirigenti**, perché sono quelli che hanno accesso a **fonti di informazioni riservate**.