

# MONITORA

LA DATA PROTECTION CHE PREVIENE **OGNI ATTACCO**

LSG EDIZIONI

№ 01 - PRIMAVERA 2015



**Proteggi oggi. Sopravvivi domani**

A SUPPORTO DEL TUO BILANCIO DI SOSTENIBILITA'

# Direttiva NIS2

La direttiva NIS2 (Network and Information Security 2) è una normativa europea che mira a migliorare la sicurezza informatica nell'Unione Europea.

## Obiettivi

- ✓ Rafforzare la sicurezza informatica delle infrastrutture critiche.
- ✓ Creare un livello comune di cybersicurezza in tutti gli Stati membri.
- ✓ Migliorare la resilienza informatica delle organizzazioni.

## Applicazione

- ✓ Si applica a un'ampia gamma di settori, tra cui e-commerce, cloud computing, sanità, pubblica amministrazione, trasporti.
- ✓ Si integra con altre normative, come il GDPR, il Regolamento DORA, e il Cyber Resilience Act.

**Requisiti Gestione del rischio, Governance d'impresa, Segnalazione di incidenti, Continuità aziendale, Misure di base per la sicurezza informatica.**

## Sanzioni

- ✓ Sanzioni pecuniarie, amministrative e penali.
- ✓ Sanzioni modulate in base alla qualifica dell'azienda coinvolta.

## Registrazione

- ✓ La registrazione obbligatoria prevista dalla Direttiva NIS2 doveva essere completata entro il 28 febbraio 2025. Il mancato rispetto di questo termine comporterebbe sanzioni economiche.

| Settori<br>altamente critici             | Settori critici                                                      | Ulteriori tipologie<br>di soggetti             |
|------------------------------------------|----------------------------------------------------------------------|------------------------------------------------|
| Energia                                  | Servizi postali e di corriere                                        | Pubblica Amministrazione<br>centrale           |
| Trasporti                                | Gestione dei rifiuti                                                 | Pubblica Amministrazione<br>regionale e locale |
| Settore bancario                         | Fabbricazione, produzione<br>e distribuzione<br>di sostanze chimiche |                                                |
| Infrastrutture dei<br>mercati finanziari | Produzione, trasformazione<br>e distribuzione di alimenti            |                                                |
| Settore sanitario                        | Fabbricazione                                                        |                                                |
| Acqua potabile                           | Fornitori di servizi digitali                                        |                                                |
| Acque reflue                             | Ricerca                                                              |                                                |
| Infrastrutture digitali                  |                                                                      |                                                |
| Gestione dei servizi TIC (b2b)           |                                                                      |                                                |
| Spazio                                   |                                                                      |                                                |

*la nuova normativa Nis 2  
amplia il campo di  
applicazione della normativa  
a 18 settori di cui 11  
altamente critici*

**STANLUCA GIUDICI AMMINISTRATORE LSG**





# Attacco Ransomware Devastante

- Immagina questo: una mattina, tu e i tuoi dipendenti arrivate in ufficio e scoprite che tutti i computer sono bloccati.

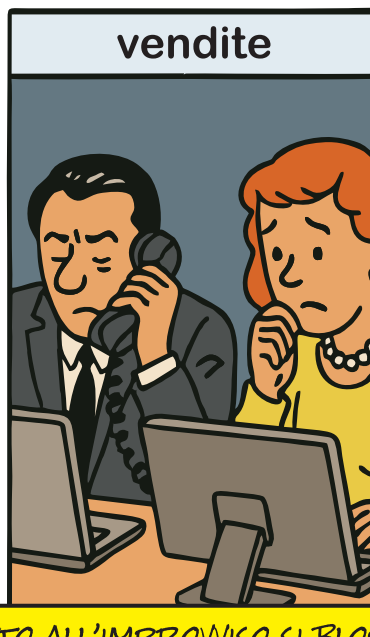
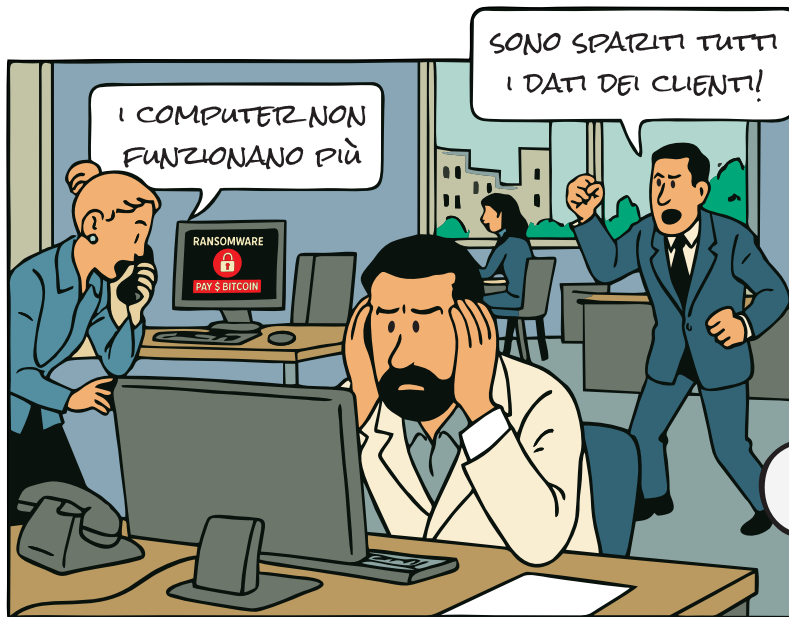
- Un messaggio sullo schermo chiede un riscatto in criptovaluta per sbloccare i file.

- La tua azienda è stata colpita da un **ransomware**.\*

\* Un **ransomware** è un tipo di malware (VIRUS) che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in inglese) da pagare per rimuovere la limitazione.



MA TUTTO RISOLVIBILE!



TUTTO ALL'IMPROVISO SI BLOCCA

# Conseguenze Immedieate:

## **Blocco Totale delle Operazioni:**

L'azienda è paralizzata.

Non puoi accedere ai dati dei clienti,  
agli ordini, ai progetti, alla contabilità.

La produzione si ferma, le vendite si bloccano,  
i servizi sono interrotti.

## **Panico e Confusione:**

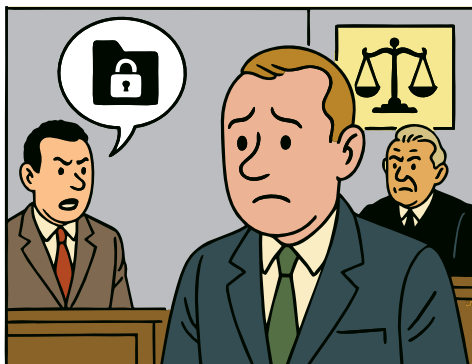
I dipendenti sono nel panico,  
i clienti sono furiosi,  
i fornitori sono preoccupati.

## **Tu sei sotto pressione:**

Devi trovare una  
soluzione immediata.  
Regna il caos!



**MA TUTTO RISOLVIBILE!**



LO SCENARIO È PREOCCUPANTE ....E I CONCORRENTI SE LA TRIDONO

# Conseguenze a Breve Termine:

## **Perdita di Dati Critici:**

Anche se paghi il riscatto, non c'è garanzia che i tuoi dati vengano recuperati. Potresti perdere informazioni preziose, come contratti, progetti, dati finanziari.

## **Danni Finanziari Enormi:**

Costi per il riscatto (se decidi di pagare).  
Costi per il ripristino dei sistemi (tecnici, software, hardware).  
Perdita di guadagni a causa dell'inattività.  
Possibili sanzioni legali per violazione della privacy.

## **Danni alla Reputazione:**

La notizia dell'attacco si diffonde rapidamente.  
I clienti perdono fiducia nella tua azienda.  
I concorrenti sfruttano la situazione a loro vantaggio.





...NON HO QUESTA  
CIFRA, COME FACCIO?



...LA SITUAZIONE È SEMPRE PIÙ TESA



# Conseguenze a Lungo Termine:

*più gravi di quello che si possa pensare*

## **Difficoltà a Ripartire:**

Potrebbe essere difficile recuperare i clienti persi.  
Potrebbe essere necessario investire ingenti somme di denaro per ricostruire la tua reputazione.

## **Rischio di Chiusura:**

In alcuni casi, un attacco informatico può portare al fallimento dell'azienda.

## **Responsabilità Legali:**

Potresti essere perseguito legalmente dai clienti, fornitori, e dallo stato, per non aver protetto adeguatamente i dati sensibili.

## **Danni Personali:**

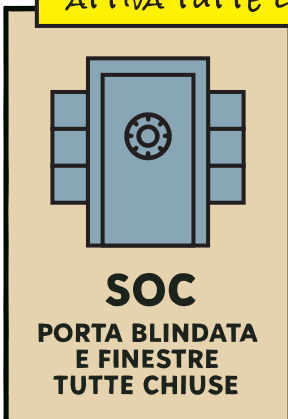
Stress, ansia, problemi di salute legati alla pressione.  
Possibile perdita di fiducia da parte di familiari e amici.



**MA TUTTO RISOLVIBILE!**



ATTIVA TUTTE LE PRECAUZIONI!



# Cosa puoi fare Ora?

- **Investi in sicurezza informatica:**

Firewall, antivirus, backup regolari, formazione dei dipendenti.

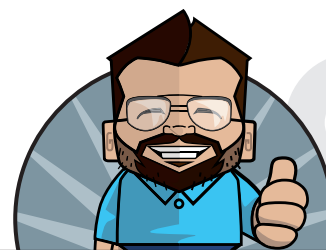
- **Crea un piano di risposta agli incidenti:**

Cosa fare in caso di attacco.

- **Mantieniti aggiornato:**

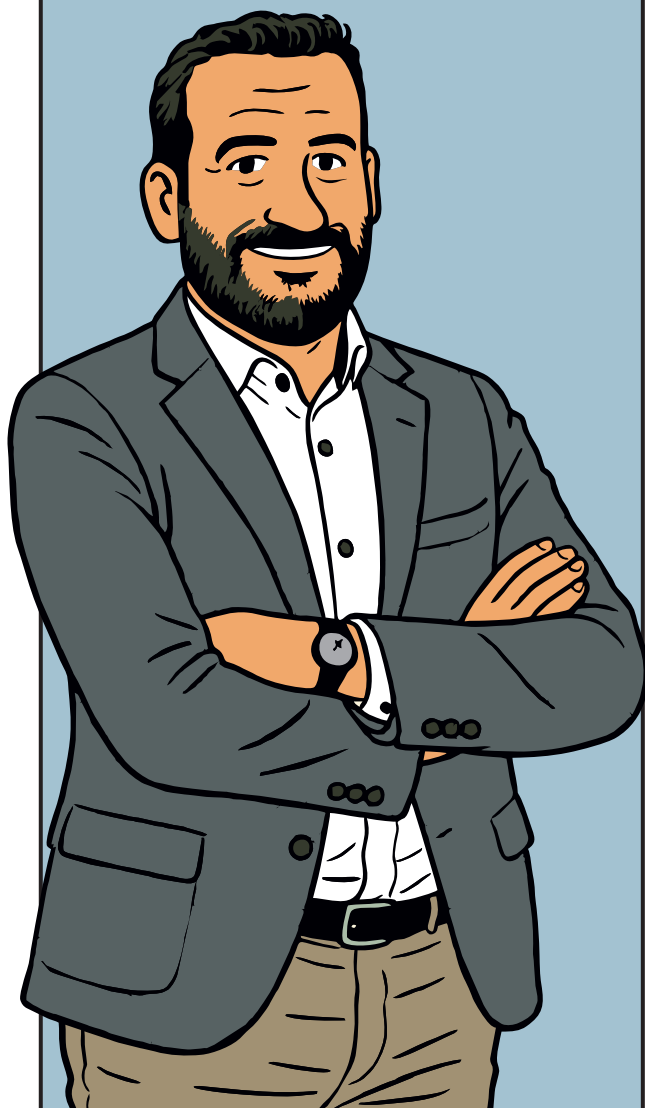
Informati sempre sulle ultime minacce informatiche.

La prevenzione è fondamentale.  
Non aspettare che sia troppo tardi.

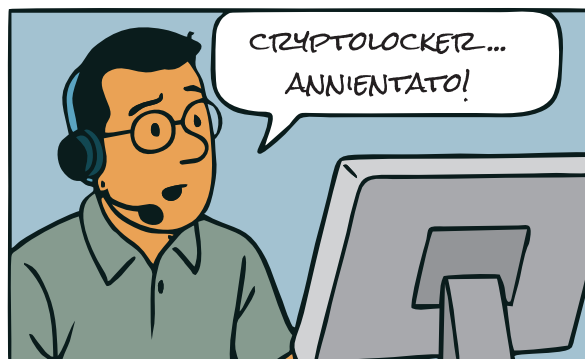


TUTTO È RISOLVIBILE!

AFFIDATI AD UN TEAM ESPERTO!



FABIO PATELLI, AMMINISTRATORE USG



**LA PREVENZIONE  
È FONDAMENTALE.**



**NON ASPETTARE CHE  
SIA TROPPO TARDI.**

# Chi siamo

LSG servizi informatici srl è questo, un team di persone che ogni giorno mettono la propria faccia eseguendo lavori sartoriali con minuzia artigianale per accontentare ogni esigenza dei propri clienti. LSG è composta da un reparto di programmazione, la Software House, e da un reparto Hardware che abbraccia consulenza, vendita e sicurezza informatica.

In un'epoca in cui le minacce digitali sono in continua evoluzione e **le informazioni sono diventate il bene più prezioso**, abbiamo deciso di investire nella protezione dei dati e delle infrastrutture informatiche.

**MONITORA è la divisione dedicata.**

## **i nostri servizi**

- ✓ ASSISTENZA TECNICA
- ✓ SOFTWARE SU MISURA
- ✓ HARDWARE
- ✓ CYBERSECURITY
- ✓ SERVER E RETI
- ✓ Ai PROJECT  
Intelligenza  
Artificiale



è la divisione di sicurezza informatica di



azienda certificata

ISO 9001:2015 | ISO/IEC 27001:2022

Via Rondinera, 74/C - 24060 ROGNO (BG)  
Tel. +39 035 977127 - alert@monitora.zone

[www.monitora.zone](http://www.monitora.zone)

[www.lsgoffice.it](http://www.lsgoffice.it)



inquadra con  
il tuo smartphone  
il QR CODE  
per ottenere  
più informazioni.

Lsg ha cura l'ambiente e lavora attivamente alla realizzazione del suo Bilancio di Sostenibilità, dimostrando il proprio impegno verso pratiche economiche, sociali e ambientali responsabili utilizzando anche per le proprie attività di comunicazione e stampa materiali sostenibili come la carta Crush Mais: una carta naturale ed ecologica con 15% di residui agro-industriali e il 40% di fibra riciclata post-consumo e cellulosa da foreste correttamente gestite. La carta Crush è riciclabile e biodegradabile.



partner

**cyberglobal<sup>7</sup>**

certificazioni

