



COMUNICATO STAMPA

Milano, 17 ottobre 2024

**NIS 2, la nuova era della cybersecurity per le infrastrutture critiche.
Spindox pronta ad aiutare i clienti coinvolti nel perimetro della direttiva**

La Direttiva NIS 2, in vigore dal 18 ottobre, introduce requisiti di sicurezza più rigorosi per le imprese che operano in settori critici come infrastrutture digitali, energia e sanità. Spindox rafforza la propria postura di cybersecurity per aiutare i clienti, implementando misure avanzate di gestione del rischio, continuità operativa e formazione.

Spindox S.p.A. (la "Società" o "Spindox", TICKER: SPN), società italiana leader nella consulenza tecnologica di frontiera, ricorda che in data odierna la **Direttiva NIS 2** entra pienamente in vigore, a conclusione di un iter di recepimento durato un anno. Si tratta della **nuova disciplina comunitaria in materia di sicurezza delle reti e delle informazioni per i servizi essenziali e le infrastrutture critiche**.

La NIS 2 include nel perimetro di applicabilità le imprese europee che operano in alcuni settori, considerati appunto «critici»:

- Infrastrutture digitali e provider di servizi digitali;
- Energia, Oil & Gas;
- Reti idriche;
- Salute;
- Trasporti;
- Pubblica Amministrazione;
- Fornitori di reti e servizi per la comunicazione elettronica pubblica;
- Gestione rifiuti;
- Industria aerospaziale;
- Prodotti critici (es. farmaci, dispositivi medicali, prodotti chimici ecc.);
- Servizi postali;

- Filiera agro-alimentare;
- Ulteriori piattaforme di servizi digitali (es. data center e social network).

Sono interessati molti clienti di Spindox, che erogano servizi ritenuti essenziali a livello europeo e che da domani saranno soggetti a requisiti di sicurezza più stringenti rispetto a quelli attuali. Ed è interessata la stessa Spindox, che a tali clienti fornisce supporto proprio nell'ambito della cybersecurity. Per il nostro Gruppo, dunque, vi è un duplice motivo di interesse.

Pur non rientrando, direttamente, tra i soggetti obbligati ad adeguarsi, Spindox ha deciso di potenziare ulteriormente la propria postura di sicurezza informatica per rispondere al meglio alle nuove esigenze di tutti i clienti che operano nei settori coinvolti. Come ricorda **Giuseppe Longo, Chief Information Security Officer del Gruppo Spindox**, *«i clienti si affidano a noi per proteggere i loro sistemi critici e per garantire la continuità operativa. Non conformarsi ai nuovi requisiti potrebbe comportare non solo la perdita di opportunità commerciali, ma anche conseguenze legali e sanzioni. Adottare queste nuove misure significa dimostrare un impegno verso la sicurezza e la resilienza operativa, un fattore cruciale per il nostro vantaggio competitivo»*.

In concreto, come risponde alla nuova sfida il Gruppo Spindox?

È ancora **Longo** a spiegarlo: *«Partendo dal Sistema di Gestione della Sicurezza delle Informazioni (SGSI), certificato ISO 27001 con le estensioni ISO 27017 e 27018, già in essere da tempo nella nostra organizzazione, abbiamo definito nuovi obiettivi al suo percorso di miglioramento continuo in diverse aree»*. Sono quattro, in particolare, gli ambiti di intervento identificati:

Gestione del rischio e misure di sicurezza - Spindox ha deciso di implementare e di esercitare con cadenza almeno annuale una seconda analisi del rischio, che avrà come fulcro i processi aziendali e che si andrà ad aggiungere a quella già in uso, basata sul NIST Security Framework.

Continuità operativa - Al canonico test annuale di Disaster Recovery / Business Continuity, Spindox aggiunge un secondo test, riducendo così a sei mesi l'intervallo delle verifiche della resilienza della propria infrastruttura.

Segnalazione e gestione delle violazioni - Spindox ha deciso di rivedere completamente il proprio processo interno di gestione degli incidenti, integrandolo e migliorandolo non solo con l'adozione di nuove versioni di sistemi di controlli (ad es. adozione di nuovo sistema DLP) ma anche, laddove se ne verificherà l'esigenza, con miglioramenti sulla propria struttura organizzativa.

Formazione e consapevolezza - Spindox è impegnata nel miglioramento continuo della qualità dell'informazione e della formazione, anche attraverso l'adozione di nuovi strumenti di test e sensibilizzazione sui temi "caldi" della

consapevolezza, quali QRishing e Ransomware simulation.

Conclude **Longo**: «Queste iniziative si vanno ad aggiungere a quanto Spindox ha già fatto nel corso degli ultimi due anni dotandosi, ad esempio, di un SOC 24/7, adottando un nuovo sistema SIEM e sostituendo il vecchio EDR con un sistema di Endpoint detection and response di nuova generazione».

A quanto definito internamente, si aggiunge l'impegno di Spindox per i propri clienti. Lo illustra **Claudio Merulla, Amministratore Delegato di Oplium Italia**, la società di cybersecurity del Gruppo: «Oplium ha definito strategie e pratiche che anticipano le normative emergenti. I contenuti della NIS 2 sono stati oggetto della nostra analisi fin dalla sua entrata in vigore, il 17 gennaio 2023. Dal punto di vista dei nostri clienti, la esigenza fondamentale è di incorporare i requisiti di legge nelle strutture di Sicurezza, Compliance e Legal. Si tratta di adottare un approccio sistematico e allo stesso tempo pratico ed efficace, per consolidare la gestione del rischio e, al tempo stesso, minimizzare l'impatto operativo e sul business. Oplium sta supportando numerose organizzazioni ad adeguarsi a tale normativa attraverso una metodologia strutturata e personalizzata. Si parte da una fase di assessment e valutazione, per poi definire una strategia di gestione dei rischi e infine implementare un programma di interventi necessario a garantire l'aderenza alla normativa e potenziare la loro postura di sicurezza».

Riguardo Spindox

Spindox Spa opera nel mercato dell'information technology, con la missione di sostenere l'innovazione dei propri clienti attraverso la consulenza tecnologica di frontiera, la ricerca industriale e l'offerta di prodotti. Le competenze del Gruppo coprono le seguenti aree: IT Strategy and Governance, User Centric Experience, Products & Services, Quality Assurance, Data Intelligence, Operations & Maintenance, Vertical Solutions, Emerging Technologies e R&D, Cyber Security. Spindox è fra le realtà del settore con il più alto tasso di crescita (CAGR 2021-2023 pari al 25,5%). Il Gruppo conta 1.300 dipendenti (al 31 dicembre 2023) distribuiti in dieci sedi italiane: Milano, Roma, Maranello MO, Torino, Firenze, Cagliari, Baronissi SA, Trento, Bari e Ivrea TO e quattro filiali estere in Spagna, Svizzera, Regno Unito e USA.

Spindox S.p.A.

Sede legale: Via Bisceglie 76, 20152 – Milano

Referente: Paolo Costa, Chief Marketing and Communications Officer, Investor Relations Manager

E-mail: paolo.costa@spindox.it

Tel.: +39 02 910 95101

Euronext Growth Milan Advisor & Specialist

Sito internet: www.spindox.it

LinkedIn: <https://www.linkedin.com/company/spindox/>



Integrae SIM S.p.A.

Piazza Castello, 24, 20121 – Milano

E-mail: info@integraesim.it

Tel.: +39 02 80506160



Sito internet: www.spindox.it

Linkedin: <https://www.linkedin.com/company/spindox/>