PRESS

DIRETTIVA NIS2 E ORGANIZZAZIONI ITALIANE: LE RISPOSTE DI SANGFOR TECHNOLOGIES

Gallarate, 15 aprile 2024 **-** La direttiva NIS2 (**Network and Information Security 2 Directive)** punta a migliorare la sicurezza informatica nell'UE e prepara le organizzazioni a essere pronte per qualsiasi potenziale minaccia informatica. Gli Stati membri dell'UE devono recepire la direttiva NIS2 entro **il 17 ottobre 2024** e le misure inizieranno a entrare in vigore il 18 ottobre 2024.

Per preparare meglio gli Stati dell'UE contro **le minacce informatiche**, la direttiva NIS2 ha incluso requisiti organizzativi più severi, estesi in **quattro aree**: la gestione del rischio, la responsabilità aziendale, gli obblighi di rendicontazione e la continuità aziendale.

NIS2 richiede inoltre che le organizzazioni dispongano di **misure minime di sicurezza** informatica. Ciò include l'esecuzione di risk assesment, l'esecuzione di backup, la formazione per la sicurezza informatica, l'utilizzo dell'autenticazione a più fattori, l'utilizzo della crittografia e dell'encryption.

"*NIS2 nasce dall'esigenza di superare i limiti della precedente Direttiva NIS, anche in funzione dei nuovi scenari che vedono un aumento delle problematiche relative alla sicurezza. Tuttavia, la nostra esperienza sul campo dimostra che l'impatto delle normative non è immediatamente recepito dalle imprese. Per questo motivo da diversi mesi ci stiamo impegnando nel fare chiarezza sulla nuova Direttiva. In tal senso stiamo anche partecipando a un roadshow, iniziato il 9 aprile a Genova, che entro metà maggio toccherà molte città italiane, per supportare i nostri partner e tutte le aziende che hanno la necessità di orientarsi*", afferma **Francesco Addesi, Country Manager Italy di** Sangfor Technologies**.**

La direttiva NIS2 contempla 15 settori considerati infrastrutture critiche e li divide in due entità: **Essential Entity (EE) e Important Entity (IE)**.
Le Entità Essenziali sono classificate in 8 categorie: **energia, trasporti, finanza, pubblica amministrazione, sanità, spazio, approvvigionamento idrico e infrastrutture digitali**. NIS2 è applicabile alle organizzazioni di questi settori con oltre 250 dipendenti, un fatturato annuo di almeno 50 milioni di euro o uno stato patrimoniale di almeno 43 milioni di euro.
Sette settori rientrano tra gli Enti Importanti: i **servizi postali, la gestione dei rifiuti, i prodotti chimici, la ricerca, gli alimenti, la produzione e i fornitori digitali**. La NIS2 si applica alle imprese di questi settori con un numero di dipendenti compreso tra 50 e 250 e un fatturato annuo non superiore a 50 milioni di euro o uno stato patrimoniale non superiore a 43 milioni di euro.

Le organizzazioni dell'UE che non rispettano la direttiva NIS2 possono essere soggette a **tre tipi di sanzioni** che includono rimedi non monetari, sanzioni amministrative e sanzioni penali.

COME L'ITALIA PREVEDE DI IMPLEMENTARE LA NIS2?

L'Italia mira a raggiungere l'autonomia strategica nazionale ed europea puntando sul dominio digitale. Il Paese ha lanciato la **National Cybersecurity Strategy (NCS),** che mira ad attuare 82 misure entro il 2026, attraverso **tre obiettivi chiave: protezione, risposta, sviluppo.**

Il quadro del National Cyber Crisis Management è suddiviso in tre livelli: politico, operativo e tecnico, ognuno dei quali ha un organo di governo che è responsabile della supervisione dei problemi e dell'implementazione.

"La NIS2, come tutte le direttive, può sembrare solo una delle tante costrizioni, piuttosto che una tutela per le aziende. In Sangfor siamo consapevoli della nostra responsabilità e, senza alcun dubbio, siamo pronti ad assumercele totalmente e ad accompagnare le aziende verso le strade più sicure. E' importante che l'azienda, sia essa pubblica o privata, di grande o piccola dimensione, sia altrettanto consapevole che l'IT non è un costo, bensì un investimento", **prosegue Addesi.**

COME SANGFOR TECHNOLOGIES PUÒ AIUTARE LE ORGANIZZAZIONI CON LA CONFORMITÀ NIS2?

Sangfor **supporta le organizzazioni nell'adesione alla direttiva NIS2 offrendo una suite completa di soluzioni di sicurezza** che includono:

- **Network Secure**: un firewall di nuova generazione progettato per salvaguardare le reti.
- **Endpoint Secure**: una piattaforma di protezione degli endpoint che garantisce la sicurezza dei dispositivi.
- **Internet Access Gateway**: un gateway web sicuro per un accesso sicuro a Internet.
- **Cyber Command**: una soluzione di Network Detection and Response (NDR) focalizzata sul rilevamento delle minacce di rete avanzate sotto forma di comportamenti anomali.
- **Access Secure**: una soluzione SASE (Secure Access Service Edge) per l'accesso remoto sicuro alle risorse di rete e cloud.
- **Servizi Cyber Guardian**: una gamma di servizi, tra cui Managed Detection and Response (MDR), Incident Response e Security Risk Assessment, per una maggiore sicurezza.

L'integrazione di questi prodotti nel framework **XDDR (eXtended Detection, Defense, and Response)** fornisce un solido ecosistema di sicurezza. Questa integrazione è in linea con i requisiti della direttiva NIS2 per una gestione completa del rischio. Essa aiuta le organizzazioni a ottenere informazioni in tempo reale su potenziali rischi come vulnerabilità, errori di configurazione e password deboli, che sono obiettivi primari per le minacce informatiche.

Utilizzando **l'intelligenza artificiale (IA) e l'apprendimento automatico (Machine Learning),** le soluzioni Sangfor offrono un rilevamento preciso e rapido delle minacce. La natura interconnessa di questi prodotti consente una risposta automatizzata e coordinata, riducendo significativamente l'impatto degli incidenti di sicurezza e **supportando l'enfasi posta dalla direttiva NIS2 sulle strategie di sicurezza proattive e reattive**. Le tecnologie di Sangfor migliorano anche il rilevamento delle minacce correlando i dati tra diversi livelli di sicurezza, fornendo un contesto dettagliato per gli eventi della rete. Questa funzione è anche fondamentale per **adempiere agli obblighi di comunicazione completi della direttiva NIS2**, mentre gli strumenti di segnalazione integrati di Sangfor aiutano a generare i report necessari per la conformità normativa.

Per la continuità operativa, Sangfor incorpora funzionalità di ripristino all'interno delle proprie soluzioni. Ad esempio, **Endpoint Secure** include funzionalità di ripristino ransomware, che consentono il ripristino dei dati in caso di attacco.

PRESS

Informazioni su Sangfor Technologies

Sangfor Technologies è azienda leader globale di soluzioni di infrastruttura IT iperconvergente, specializzata in Cloud Computing & Cyber Security. Grazie all'ampia gamma di soluzioni e servizi e alla collaborazione con una rete capillare di partner certificati, Sangfor può rispondere alle esigenze delle imprese di tutt'Italia. Rendere la trasformazione digitale più semplice e sicura è l'obiettivo di Sangfor Technologies, che si impegna a fornire un servizio tempestivo e professionale. Sono già oltre 4.000 i clienti che in Italia utilizzano le soluzioni Sangfor tra pubblica amministrazione locale e centrale, sanità, università, finance e imprese private. Fondata nel 2000, Sangfor conta più di 9.500 professionisti distribuiti in oltre 60 sedi in tutto il mondo.
www.sangfor.it

Informazioni per la stampa

Francesca Sanguineti Communication Opportunities
Mob. +39 334.6818607
Email ufficiostampa@francescasanguineti.it
www.francescasanguineti.it