TREVISOTODAY

Santarelli: «Scudetto meraviglioso, solo noi sappiamo quanto abbiamo sofferto»

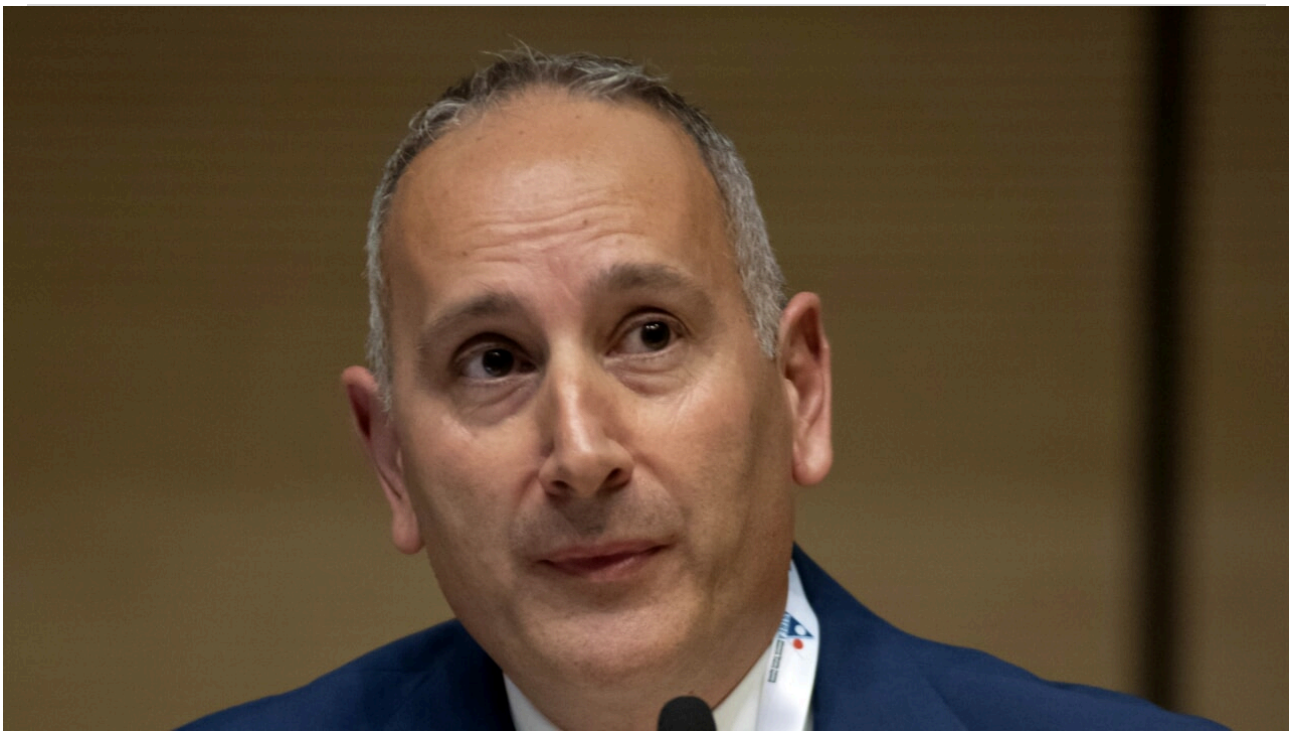
ECONOMIA

Cyber security, le imprese venete chiamate all’azione

La formazione di UNIS&F per affrontare le nuove sfide digitali imposte dalla Direttiva NIS2. L’esperienza della "Nonno Nanni"

Redazione

22 aprile 2026 06:32



Pasquale Costanzo, direttore di UNIS&F

Più sicurezza, più responsabilità, ma anche nuove opportunità: la rivoluzione della cyber security passa dalla Direttiva NIS2 e chiama le imprese venete a un cambio di passo e UNIS&F le accompagna in questo percorso. La NIS2 – recepita in Italia con il D.Lgs. 138/2024 –in particolare, impone standard più elevati in materia di gestione dei rischi, sicurezza delle infrastrutture e responsabilità del management. Tradotto in pratica: nuovi protocolli di sicurezza, difese più robuste, formazione continua e una governance digitale più solida. Il tutto accompagnato da un sistema sanzionatorio significativo per chi non si adegua. Ma non è solo una questione di obblighi. La NIS2 rappresenta anche una leva concreta di crescita: investire in cyber security significa proteggere dati e processi, rafforzare la fiducia di clienti e partner e migliorare la competitività sul mercato. E grazie a tecnologie come intelligenza artificiale e automazione, le imprese possono oggi rendere più efficiente la gestione delle minacce, riducendo tempi e costi.

L’esperienza di Latteria Montello S.p.a, quando tradizione fa rima con innovazione

Latteria Montello S.p.A, leader nel mercato dei formaggi freschi con il brand Nonno Nanni, e Caseificio Tonon S.r.l., specializzata nella produzione di Pizza Cheese, avendo provveduto alla registrazione al portale entro il termine previsto (28 febbraio 2025) sono stati qualificati quali soggetti importanti e come tali stanno procedendo all’adeguamento di quanto previsto dalla normativa NIS 2 e dalla Determinazione ACN con il supporto di UNIS&F che, attraverso propri consulenti tecnici e legali, coopera attivamente al fine di far sì che le Società rispettino gli obblighi e risultino essere conformi a quanto previsto dalla normativa NIS 2 entro i termini stabiliti dal Decreto.

«Grazie al supporto di UNIS&F – ha dichiarato Renato De Faveri, Responsabile dei Sistemi Informativi (SI) Latteria Montello – abbiamo adempiuto al primo obbligo previsto dal Decreto Legislativo 138/2024 entro gennaio 2026. Il nostro sistema di gestione e notifica degli incidenti verso il CSIRT Italia è pienamente operativo e ben conosciuto a livello aziendale in entrambe le organizzazioni. Ciò è stato possibile anche grazie a specifiche attività formative dai consulenti di UNIS&F, durante le quali sono stati approfonditi i criteri che qualificano un incidente come

“significativo” e le procedure operative da seguire per effettuare correttamente la notifica. Tali iniziative hanno contribuito ad accrescere la consapevolezza interna in materia di cyber security, ambito che non è mai stato trascurato ma, al contrario, è sempre stato considerato strategico. L’organizzazione, infatti, ha da tempo investito nella formazione e sensibilizzazione del personale rispetto ai rischi informatici quotidiani. Nonostante ciò l’adeguamento completo alla normativa NIS2 comporta comunque un impatto significativo sull’organizzazione, in particolare in termini di tempi necessari per l’implementazione delle misure richieste e di costi complessivi, pur partendo da una struttura già solida sotto il profilo della sicurezza delle reti e della consapevolezza del personale».

«Sappiamo che l’adeguamento non si esaurirà nel breve periodo, ma rappresenterà un processo continuo che coinvolgerà non solo l’anno in corso, bensì anche quelli futuri» continua De Faveri «È tuttavia importante evidenziare che non si parte da zero: esistono già competenze, processi e modalità operative consolidate che costituiscono una base solida su cui costruire e rafforzare il sistema di gestione della sicurezza in linea con i requisiti normativi. È ciò che sta emergendo anche dalla messa in pratica delle singole specifiche di base richieste dalla normativa NIS 2, in particolare dalla gestione del rischio nell’organizzazione. Spesso questa normativa viene percepita come un ulteriore adempimento burocratico, anche perché non sempre è immediatamente chiaro il suo obiettivo concreto e l’impatto reale che può avere sulle singole organizzazioni. In molti casi, infatti, si fatica a comprendere fino in fondo le finalità della Direttiva NIS 2 e il valore strategico delle misure richieste. Proprio per questo motivo, risulta fondamentale l’attività svolta da UNIS&F, al fine di diffondere una maggiore consapevolezza sulla complessità della materia e sull’importanza che ogni organizzazione riveste nell’implementazione di un sistema efficace di cyber security. Il rispetto della normativa non può essere considerato un adempimento limitato all’area IT, ma rappresenta un impegno trasversale che coinvolge l’intera organizzazione. Un ruolo centrale è ricoperto dal management, che deve essere adeguatamente informato, sensibilizzato e formato anche alla luce delle responsabilità e delle sanzioni previste dalla normativa di settore. L’obiettivo delle nostre realtà è quindi quello di riuscire a trasformare la percezione della cybersecurity, e della normativa NIS 2 medesima, da obbligo formale a leva strategica per la protezione, la continuità e la crescita delle nostre organizzazioni».

«La Direttiva NIS2 segna un passaggio cruciale per il sistema economico – spiega Pasquale Costanzo, Direttore generale di UNIS&F –. Non si tratta solo di adeguarsi a una normativa, ma di cogliere un’opportunità per rafforzare la resilienza e la competitività delle imprese».

«Durante gli incontri di formazione - ha detto Alberto Mercurio, Responsabile Cyber security UNIS&F - sono stati affrontati in modo concreto tutti i nodi principali: chi è coinvolto, quali sono le scadenze, quali misure adottare e come evitare sanzioni. Grande interesse suscitano gli interventi dell’Agenzia per la Cybersicurezza Nazionale che porta esempi di strumenti di controllo che le aziende possono utilizzare per comprendere a che punto sono in tema di cyber sicurezza. E poi vengono proposti i casi di aziende del nostro territorio che hanno dovuto gestire un attacco hacker o ancora, simulazioni di incidenti in modo da fornire gli step per far fronte all’emergenza».