IT•NEWS

EDIZIONE SPECIALE!

N. 27 GEN./FEB. 2026

L'indispensabile road-book

per rendere sempre più digitale
e competitiva la tua impresa

IN QUESTO NUMERO:

Speciale NIS2

Governance, sicurezza e continuità dei servizi

Lo ***Speciale NIS2*** nasce a seguito di ***GlobalNeXt***, l'evento organizzato da ***GlobalNet***, società del gruppo ***i-TEAM***, che si è svolto il ***23 gennaio presso il Museo Piaggio*** e ha riunito consulenti, aziende e partner tecnologici in un momento di confronto dedicato alla cyber security e alla nuova Direttiva europea NIS2.

La NIS2 rappresenta un cambiamento profondo nel modo in cui imprese e organizzazioni sono chiamate a gestire la sicurezza informatica.
Non si tratta più solo di adottare misure tecniche, ma di costruire un modello di ***governance del rischio***, che coinvolge processi, responsabilità, persone e tecnologia.

Lo Speciale raccoglie e rielabora i contenuti emersi durante l'evento, con l'obiettivo di offrire una lettura chiara, concreta e accessibile della NIS2, andando oltre la norma e mettendo al centro la ***resilienza dei servizi digitali***.

GLOBALNeXt

I·TEAM

NIS2

dalla norma alla responsabilità di governance

La Direttiva NIS2 rappresenta un passaggio decisivo nel modo in cui l'Unione Europea affronta la sicurezza informatica. Se la prima NIS aveva introdotto un quadro di riferimento iniziale, nel tempo sono emersi limiti evidenti: un perimetro ristretto, applicazioni disomogenee e una forte focalizzazione sugli aspetti tecnici.

Nel frattempo, il contesto digitale è profondamente cambiato. Le organizzazioni sono sempre più interconnesse, dipendono da fornitori esterni, utilizzano servizi cloud e piattaforme digitali condivise. In questo scenario, un incidente informatico non è mai un evento isolato, ma può propagarsi lungo l'intera filiera.

La NIS2 nasce per rispondere a questa complessità, introducendo un modello basato sulla governance del rischio. Il cambiamento più rilevante riguarda le responsabilità:

le aziende non sono chiamate solo ad adottare misure di sicurezza, ma a dimostrare di conoscere i propri asset critici, valutare i rischi e gestire gli incidenti in modo strutturato.

Un elemento centrale è il coinvolgimento diretto degli organi di amministrazione e direzione, che diventano parte attiva del sistema di sicurezza. La cyber security esce dall'ambito esclusivamente tecnico e diventa una componente della governance aziendale.

In Italia, l'attuazione della NIS2 è coordinata dall'Agenzia per la Cybersicurezza Nazionale (ACN), con il supporto del CSIRT Italia, responsabile della gestione delle notifiche di incidente. Dal confronto emerso durante GlobalNeXt è stato chiarito che chi rileva un incidente non coincide necessariamente con chi è obbligato a notificarlo: anche in presenza di fornitori o servizi gestiti, la responsabilità resta in capo al soggetto NIS.

Le recenti determinazioni ACN segnano il passaggio definitivo all'operatività. Dal ***1° gennaio 2026*** scatteranno gli obblighi operativi di notifica, mentre dal ***15 gennaio 2026*** entrerà in vigore la disciplina generale prevista dal decreto NIS e dalle determinazioni attuative. Il tempo per prepararsi è limitato: affrontare ora la NIS2 significa ridurre il rischio e rafforzare la resilienza dell'organizzazione.

Continuità operativa e gestione del rischio:

dalla NIS2 ai processi concreti

Uno dei messaggi più chiari emersi durante Global-NeXt è che la NIS2 non può essere affrontata come un semplice adempimento tecnico.
Il cuore della Direttiva è la continuità operativa, intesa come capacità di garantire servizi essenziali anche in condizioni di incidente o crisi.

Marco Cecchi (Omega Sistemi Srl), esperto in ***cybersecurity*** e ***gestione dei sistemi informativi aziendali, realtà del gruppo I-TEAM***, ha approfondito il ruolo delle misure tecniche, della gestione degli asset e dei processi di vulnerability assessment come elementi chiave per trasformare gli obblighi normativi in controllo operativo e continuità dei servizi.

> ***La business continuity non è un piano teorico, ma un insieme di processi che partono dalla conoscenza del business. Significa identificare i servizi critici, comprenderne le dipendenze tecnologiche e organizzative e valutare l'impatto di possibili interruzioni.***

In questo contesto, le attività di ***vulnerability assessment*** assumono un ruolo centrale. La NIS2 richiede alle aziende di dimostrare di aver valutato i rischi in modo strutturato, dando priorità alle vulnerabilità che possono compromettere i servizi essenziali.
Non tutte le vulnerabilità hanno lo stesso peso: il criterio guida diventa l'impatto sul business.

Un altro pilastro è la ***gestione degli asset***.
Non è possibile proteggere ciò che non si conosce. Le organizzazioni devono disporre di una visione chiara e aggiornata dei sistemi informativi e di rete rilevanti, degli asset critici e delle dipendenze dai fornitori. Questo inventario rappresenta la base per definire misure di sicurezza efficaci e piani di risposta agli incidenti.

La NIS2 parla esplicitamente di ***misure tecniche e organizzative***. Le tecnologie sono fondamentali, ma non sufficienti se non inserite in un modello di governance chiaro, con ruoli, responsabilità e flussi decisionali definiti prima che si verifichi un incidente.

Il messaggio emerso dal confronto è che la NIS2 può diventare un fattore di maturità. Le aziende che strutturano processi di gestione del rischio e continuità operativa non solo rispettano la norma, ma migliorano l'affidabilità complessiva dei propri servizi.

Tecnologia e resilienza:
infrastrutture e servizi a supporto della NIS2

La NIS2 non impone l'adozione di specifiche tecnologie, ma definisce un obiettivo chiaro: ***servizi digitali resilienti***. La tecnologia diventa quindi un abilitatore fondamentale della conformità e della continuità operativa.

> ***Gli endpoint rappresentano uno dei principali punti di esposizione. La capacità di rilevare comportamenti anomali e di reagire rapidamente è fondamentale per limitare la propagazione di un attacco e supportare gli obblighi di notifica previsti dalla NIS2.***

Durante la seconda tavola rotonda di GlobalNeXt è emersa l'importanza di un approccio integrato: la resilienza richiede capacità di ***prevenzione***, ***rilevazione*** e ***risposta agli incidenti*** lungo tutta l'infrastruttura.

Riccardo Gervasi, ***Presales Manager Omada by TP-Link***, ha evidenziato il valore di un governo centralizzato della rete, che consenta visibilità, controllo e reporting continuo, elementi fondamentali per supportare sia la continuità dei servizi sia le esigenze di compliance.

Gabriele Petroni, ***Owner Oscar WIFI***, ha richiamato l'attenzione sul ruolo delle reti Wi-Fi, evidenziando come sicurezza, gestione degli accessi e semplicità operativa siano aspetti fondamentali in contesti aziendali e hospitality.

Anche ***infrastruttura*** e ***cloud*** richiedono un governo consapevole.

Paolo Vannini (***All You Srl***), esperto in infrastrutture IT complesse e soluzioni Datacenter, altra realtà del gruppo I-TEAM, ha posto l'accento sull'importanza di progettare ambienti infrastrutturali e cloud con criteri di:

- ***affidabilità***
- ***ridondanza***
- ***revisione continua della sicurezza***

elementi indispensabili per garantire continuità operativa e conformità normativa.

Rete e accesso restano elementi centrali. Segmentazione, controllo degli accessi e visibilità sui flussi di traffico sono aspetti spesso sottovalutati, ma determinanti per ridurre la superficie di rischio.

Anche reti Wi-Fi e sistemi di accesso, se non governati correttamente, possono diventare punti di vulnerabilità.

Un ulteriore elemento chiave è il monitoraggio centralizzato, che consente di individuare anomalie, supportare le decisioni e produrre evidenze in caso di verifiche o incidenti.

> ***L'outsourcing non elimina la responsabilità del soggetto NIS: le aziende devono conoscere le proprie dipendenze, valutare l'impatto di un incidente sui servizi esterni e integrare ambienti cloud e on-premise in un unico modello di sicurezza.***

Persone e cultura della sicurezza:

il fattore umano della NIS2

Accanto a norme e tecnologia, la NIS2 riconosce il ruolo centrale delle persone. Molti incidenti informatici nascono da errori involontari, phishing o comportamenti inconsapevoli. La Direttiva non tratta il fattore umano come un problema, ma come un ambito da governare.

Durante GlobalNeXt è emerso che la formazione non può essere episodica. Serve un approccio continuo, capace di incidere sui comportamenti quotidiani e di rendere le persone parte attiva della sicurezza. L'awareness diventa così una vera misura di protezione.

La cultura della sicurezza è strettamente legata alla governance.

Ruoli chiari

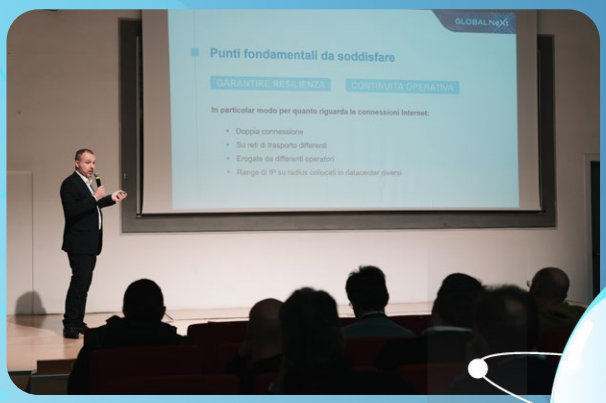
Responsabilità definite

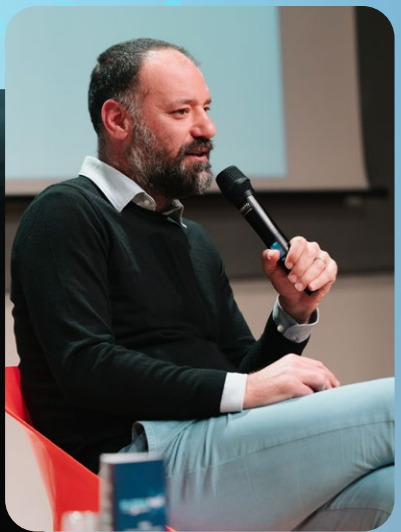
Coinvolgimento dei vertici

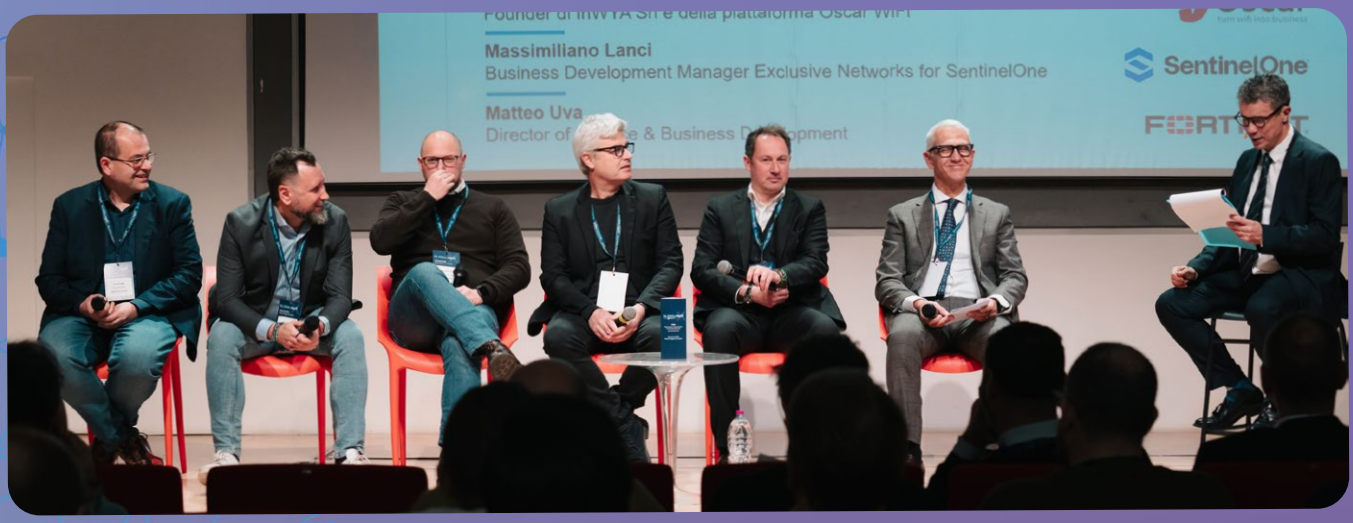
sono elementi indispensabili per rendere efficaci le misure tecniche e organizzative.

Un altro tema centrale riguarda la ***filiera cliente-fornitore***. La NIS2 chiarisce che la sicurezza si estende all'ecosistema di partner e servizi esterni, richiedendo maggiore coordinamento e requisiti più strutturati.

La NIS2 rappresenta anche un'opportunità: per le aziende significa rafforzare affidabilità e fiducia; per i partner significa accompagnare i clienti in percorsi strutturati di maturità digitale.







L'evento ha valorizzato il ruolo della consulenza, fondamentale per interpretare correttamente la Direttiva e tradurla in modelli operativi sostenibili. Accanto a questo, sono emersi prodotti e servizi come abilitatori concreti della resilienza:

- endpoint
- cloud
- monitoraggio
- rete
- infrastruttura
- accesso
- awareness

GlobalNeXt ha rappresentato un dialogo aperto e costruttivo tra tecnologia, impresa e diritto, tre dimensioni oggi inseparabili.
La cyber security non è più un tema settoriale, ma un fattore strategico che incide su responsabilità normative, scelte organizzative e continuità dei servizi.

I·TEAM

Cinque società che si sono unite per dare
forma ad un grande progetto: aiutare le imprese a
crescere nella digitalizzazione e nella rvoluzione digitale,
per avere performance sempre più efficaci ed efficienti, all'altezza
dei grandi cambiamenti dell'economia e della società contemporanea.

Allyou.srl

ego communication

GLOBALNET ITALIA

OMEGA SISTEMI
Soluzioni Informatiche Professionali

PANTAREI INFORMATICA
La tecnologia resa semplice

www.i-team.tech

project by Allyou.srl

Via Benedetto Dei 64 • 50127 FIRENZE • Numero Verde 800-199760 • info@i-team.tech