PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5768 di Giovedì 16 gennaio 2025

Sicurezza informatica: le scadenze del NIS2 e le videopillole informative

Le principali scadenze del 2025 della Direttiva NIS2, tra cui la registrazione alla piattaforma ACN e le videopillole informative di che illustrano in modo chiaro i principali contenuti della Direttiva.

Dal 16 ottobre 2024 è in vigore la nuova normativa Network and Information Security (direttiva NIS) di derivazione europea, recepita con il dlgs 138/2024. ACN coordina l'attuazione della nuova normativa in qualità di Autorità nazionale competente NIS. Per garantire un'implementazione efficace, sono previste alcune tappe fondamentali.

La prima è la registrazione tramite il portale dei servizi dell'Agenzia per la cybersicurezza nazionale, da parte delle organizzazioni pubbliche o private che possiedono i requisiti specifici previsti dalla normativa NIS.

La registrazione avviene:

- **entro il 17 gennaio 2025**: per i soggetti di cui all'articolo 42, comma 1, lettera a), tra cui i fornitori di cloud computing, data center, servizi (anche di sicurezza) gestiti e mercati online;
- **entro il 28 febbraio 2025**: per tutti gli altri soggetti inclusi nell'ambito di applicazione del decreto.

La registrazione è funzionale a consentire ad ACN di censire i soggetti operanti nei settori NIS, anche al fine di fornire loro supporto in fase di implementazione degli obblighi, attraverso le articolate attività di monitoraggio e ausilio nel loro percorso condiviso di crescita. Sul sito dell'ACN sono disponibili le informazioni relative ai settori e sottosettori inclusi nel mondo NIS e le modalità per determinare se un'organizzazione è "essenziale" o "importante".

Le altre scadenze

L'Agenzia, entro metà aprile, notificherà a tutti i soggetti registrati se sono stati inseriti, o meno, nell'elenco dei soggetti NIS e pubblicherà gli obblighi di base in materia di notifica di incidenti e di misure di sicurezza informatica.

I soggetti NIS dovranno:

- **a partire da gennaio 2026**, notificare gli incidenti;
- **entro ottobre 2026,** completare le misure di sicurezza informatica di base.

Prepararsi per tempo è fondamentale per gestire con successo l'implementazione della nuova normativa volta ad aumentare la sicurezza informatica delle reti e dei sistemi informativi dei soggetti NIS.

Approfondimenti

- Il video tutorial ACN che descrive le modalità di registrazione, i passaggi da seguire e le informazioni da inserire per potersi registrare come "soggetto NIS"

- Una guida utile alla scoperta della nuova direttiva NIS
- Termini e procedimenti (Determinazione 38565/2024)
- Domande frequenti

Le videopillole informative

La cybersicurezza italiana si appresta ha fatto un significativo passo avanti con l'entrata in vigore della Direttiva NIS2. Per agevolare l'adeguamento alle nuove normative da parte di imprese e pubbliche amministrazioni, l'Agenzia per la Cybersicurezza Nazionale (ACN) ha lanciato un'iniziativa di sensibilizzazione guidata da Marco Camisani Calzolari, noto esperto di digitale e divulgatore televisivo.

Camisani Calzolari ha creato tre videopillole informative, pubblicate sul canale YouTube dell'ACN, per illustrare in modo chiaro e coinvolgente i principali contenuti della Direttiva NIS2. Questi video, destinati a tutti i soggetti coinvolti, mettono in luce i punti salienti della normativa e il loro impatto sulla sicurezza e resilienza delle infrastrutture digitali.

In questo video dell'Agenzia per la cybersicurezza nazionale, il docente e divulgatore televisivo Marco Camisani Calzolari racconta l'importanza della nuova normativa NIS e ne elenca tempi e modi.

La NIS copre quasi tutta la superficie digitale dell'Italia. Riguarda imprese e Pubbliche Amministrazioni, quelle regionali e locali, anche il nostro comune, se capoluogo di regione o provincia, anche quelli sopra quelli i centomila abitanti, anche se non sono capoluogo di provincia e di regione.
Saranno migliaia i soggetti, pubblici e privati, che ne faranno parte, però sarà necessario registrarsi perché abbiamo scelto che siano i protagonisti della NIS a farsi avanti. Il modello è bottom up. I requisiti di appartenenza alla NIS potrete trovarli sul sito dell'Agenzia.
È lì che troverete indicati i settori e sottosettori che rientrano nel mondo NIS.
Ma non basta.
Bisogna sapere se si è soggetti essenziali o soggetti importanti. Anche qui il sito di ACN vi darà tutte le coordinate per capirlo.
Per quelli essenziali ci sono requisiti più stringenti e questo cambia la compliance; pertanto, è importante sapere a quale delle due categorie si appartiene.
A questo punto avrete avuto tutte le informazioni necessarie per iscrivervi correttamente sulla piattaforma gestita da ACN.
Sarà possibile farlo dal primo dicembre 2024 ma per tutto gennaio e tutto febbraio del 2025 sarà possibile continuare a farlo.

Se avete trovato la risposta sul sito ACN alla vostra domanda, "appartengo alla NIS?". Allora non vi resta che collegarvi al sito ACN e procedere alla registrazione seguendo correttamente la procedure che vi sarà mostrata sul sito.
È come un tutorial, in realtà, perché contiene tutte le informazioni e istruzioni che sono contenute in un filmato che spiega con poche e semplici immagini, come si effettua la registrazione. La piattaforma di ACN è progettata per essere interattiva: si possono fare domande e ottenere risposte per risolvere dubbi e avere solo certezze.

La terza videopillola realizzata da Marco Camisani Calzolari, parla di sicurezza informatica di PA, imprese e supply chain.
La NIS2 ha cambiato totalmente il modo di guardare alla sicurezza informatica. E c'è una ragione. Dopo la precedente direttiva NIS, il mondo ha conosciuto prima la pandemia da Covid e poi l'inizio del conflitto russo ucraino. Due eventi che hanno influenzato, seppure in modo diverso, il nostro rapporto con la dimensione digitale e la sicurezza delle relazioni che le passano attraverso.

L'applicazione della NIS2 ai 18 settori critici e altamente critici ha ampliato la sicurezza informatica ovunque gli hacker criminali possano portare le loro insidie, destabilizzando le infrastrutture sia fisiche che digitali, entrambe cruciali per la qualità della nostra vita quotidiana, come quelle che tutelano la salute e la sicurezza delle reti di trasporto.
In aggiunta, anche l'attuale contesto geopolitico vede settori che possono essere il bersaglio privilegiato di campagne offensive: l'energia e le telecomunicazioni, ma anche l'alimentare, la gestione rifiuti, la logistica e la fabbricazione. L'attenzione alla sicurezza informatica coinvolge tutti gli attori della catena del valore e per questo è importante proteggere la supply chain ? ovvero i fornitori, i manutentori, e ogni altra terza parte coinvolta negli approvvigionamenti essenziali per la corretta erogazione delle attività e dei servizi inseriti nel contesto NIS.

Basta un solo anello debole, per rendere insicura tutta la catena. Basta un singolo punto di attacco per propagare l'infezione a tutti gli altri anelli, finendo per colpire anche gli altri soggetti coinvolti. Le misure di sicurezza per i soggetti della NIS2, pubblici e privati, saranno definite dall'Agenzia per la cybersicurezza nazionale ad aprile 2025, e conterranno indicazioni specifiche per proteggere anche la supply chain.
Sarà un documento che indicherà come difendersi efficacemente dagli attacchi, basato sulla precisa analisi del rischio che ciascun operatore sarà chiamato a fare.

Saranno quindi regole, necessariamente flessibili, perché capaci di adattarsi ai diversi profili di rischio.
Adeguarsi alle misure di sicurezza non è un optional, ma una necessità. Dalla garanzia della sicurezza dei propri sistemi e servizi digitali dipende anche il futuro dell'azienda, cioè la sua stabilità e capacità di stare sul mercato.
In altre parole, il rispetto delle regole è un affare anche per l'azienda, le consente di scoprire la convenienza della sicurezza.
E per ACN la vostra sicurezza vale quanto quella del Paese intero.

Fonte: ACN

www.puntosicuro.it