NEWSLETTER/NEWSALERT

DATA PROTECTION E CYBERSECURITY

Direttiva NIS 2: al via la seconda fase

Introduzione

L'Agenzia per la Cybersicurezza Nazionale (ACN) sta inviando in questi giorni le comunicazioni ai soggetti identificati come essenziali o importanti circa l'inclusione nell'ambito di applicazione della Direttiva (UE) 2022/2555 (cosiddetta "Direttiva NIS 2").

Inoltre l'ACN ha avviato la seconda fase delle attività ed il 16 aprile u.s. ha pubblicato la determinazione relativa ai cd. "obblighi di base" e contenente i dettagli sulle misure di sicurezza da adottare e gli obblighi di notifica.

I I prossimi passi per le aziende

LE ATTIVITÀ DA SVOLGERE ENTRO MAGGIO 2025

Con la comunicazione di inclusione nell'ambito di applicazione della normativa, l'Agenzia per la Cybersicurezza Nazionale ha richiesto agli enti di fornire ulteriori dettagli.

Nello specifico, tale attività grava in capo al punto di contatto, che dovrà indicare:

- i nominativi, il ruolo e i dati di contatto delle persone fisiche responsabili dell'ente o che agiscono in qualità di legali rappresentanti con l'autorità di rappresentare, di prendere decisioni o di esercitare un controllo sul soggetto;
- lo spazio di indirizzamento IP pubblico e i nomi di dominio in uso e nella disponibilità del soggetto;
- gli Stati membri nei quai sono erogati i servizi;
- un sostituto del punto di contatto.

Tali informazioni dovranno essere comunicate entro il **31 maggio 2025**.

LE ATTIVITÀ DA SVOLGERE ENTRO GENNAIO 2026

La determinazione dell'Agenzia per la Cybersicurezza Nazionale precisa la tassonomia degli incidenti soggetti all'obbligo di notifica, ossia:

- la perdita di riservatezza verso l'esterno dei dati digitali, anche solo parziale;
- la perdita di integrità con impatto verso l'esterno dei dati digitali, in questo caso anche qualora fosse solo parziale;
- la violazione dei livelli di servizio attesi, stabiliti dall'ente.

In aggiunta agli eventi sopra riportati, i soggetti essenziali dovranno notificare anche l'accesso ai dati digitali non autorizzato o con abuso dei privilegi concessi.

Le attività da svolgere entro metà ottobre 2026

La determinazione di ACN introduce anche le misure organizzative, tecniche e operative "di base", ossia quelle che dovranno essere implementate dai soggetti essenziali e importanti entro metà ottobre 2026.

Le misure sono articolate in sei diverse categorie: *(i)* quelle relative al governo, volte a stabilire le strategie di gestione del rischio, i ruoli e le relative responsabilità e poteri nel contesto di gestione della sicurezza delle informazioni; *(ii)* quelle di identificazione, finalizzate ad individuare gli asset necessari all'erogazione dei servizi, a definire i rischi e a gestirli in coerenza la strategia dell'azienda; *(iii)* le misure di protezione degli asset; *(iv)* le misure volte alla rilevazione di eventuali violazioni di sicurezza; (*v)* le misure volte a garantire una risposta efficace ad eventuali violazioni di sicurezza; *(vi)* quelle volte a ripristinare la normale operatività dell'azienda.

A tal proposito si ricordi come i soggetti in ultima istanza responsabili per l'implementazione delle misure individuate dall'Agenzia per la Cybersicurezza Nazionale sono i rappresentati della società, ossia i legali rappresentanti o i soggetti che hanno potere decisionale o esercitano un controllo. Dunque, sebbene le misure di cui alla Determinazione sopra sintetizzate e le attività connesse possano apparentemente sembrare di natura prettamente tecnica, in realtà richiedono la partecipazione attiva da parte dei vertici societari, nonché un corretto inquadramento dal punto di vista giuridico nell'ottica di schermare l'organo di gestione da potenziali responsabilità. In aggiunta, occorre precisare che tra le misure di sicurezza ve ne sono numerose finalizzate a stabilire le strategie di gestione del rischio: tali profili devono necessariamente essere condivisi e approvati dai vertici aziendali.

Pertanto, per conformarsi alle recenti indicazioni di ACN, sarà opportuno avviare un processo di mappatura dei sistemi in essere ed eventualmente rivedere la configurazione dei propri processi interni. Questo potrebbe includere ad esempio la revisione delle procedure operative standard, l'aggiornamento delle politiche di sicurezza e la riorganizzazione delle responsabilità all'interno dell'azienda. La riorganizzazione non sarà solo un esercizio tecnico, dunque, ma avrà anche implicazioni strategiche e legali, potrebbero essere necessari, ad esempio, cambiamenti nelle politiche aziendali, nella formazione del personale e nei processi di gestione delle informazioni

II Conclusioni

L'ACN con l'avvio della fase due richiede alle aziende di rivedere i propri processi aziendali e la governance in materia di cybersecurity. Si tratta di interventi ampi, di natura tecnica, organizzativa e strategica. Inoltre, molte misure necessitano di una revisione approfondita dei processi e delle procedure interne, che deve essere condotta tenendo sempre in considerazione i requisiti normativi, anche nell'ottica di una gestione efficace del rischio cibernetico globale.

Contatti

Pierluigi Perri
Of Counsel – Chiomenti
Data Protection & Cybersecurity
T. +39.02.721.571
pierluigi.perri@chiomenti.net

Marilena Hyeraci
Of Counsel – Chiomenti
Data Protection & Cybersecurity
T. +39. 02.721.571
marilena.hyeraci@chiomenti.net

Lucrezia Falciai
Associate – Chiomenti
Data Protection & Cybersecurity
T. +39.02.721.571
lucrezia.falciai@chiomenti.net

Carlo Piva
Associate – Chiomenti
Data Protection & Cybersecurity
T. +39.02.721.571
carlo.piva@chiomenti.net