La nuova Direttiva Nis2 in materia di cybersicurezza.

di Stefano Manina

Sulla Gazzetta dell'Unione Europea L 333 del 27 dicembre scorso è stata pubblicata la Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione meglio nota come Direttiva NIS2, che introduce nuovi obblighi di cyber sicurezza per le aziende in materia di sicurezza dei dati e maggiori responsabilità per i soggetti interessati.
La direttiva che dovrà essere recepita dai singoli paesi membri entro 21 mesi mira a rafforzare il livello globale di cybersicurezza tra i 27 Stati membri con lo scopo di determinare una base di garanzie destinate a sviluppare un sistema di fiducia andando ad ampliare in regime di continuità la precedente direttiva NIS, adeguandosi ai flussi digitali post pandemia Covid-19, che hanno visto il considerevole aumento di traffico nella rete e delle relative superfici di attacco e ampliare i settori di attività, finendo per coinvolgere un numero e una varietà sempre maggiore di organizzazioni.
Infatti **la Direttiva NIS2 è l'evoluzione della Direttiva NIS1** che, recepita in Italia con il D. Lgs. N. 65/2018, prevedeva che le società rientranti nel suo ambito di applicazione fossero tenute ad adottare misure tecniche ed organizzative adeguate e proporzionate rispetto alla gestione dei rischi cyber, dovendo altresì prevenire e minimizzare l'impatto degli eventuali incidenti di sicurezza subiti.

Le novità introdotte dal provvedimento vanno in quattro direzioni principali:

- rideterminazione e ampliamento dell'ambito di applicazione delle norme in materia di sicurezza dei dati;
- potenziamento degli organi e delle attività di supervisione a livello comunitario, con l'obiettivo di migliorare la collaborazione per contrastare la minaccia informatica globale;
- razionalizzazione dei requisiti minimi di sicurezza e delle procedure di notifica obbligatoria degli incidenti informatici;
- estensione dei concetti di gestione del rischio e di valutazione delle vulnerabilità a tutti i soggetti interessati.

1. Certamente la novità principale della Direttiva NIS2 è proprio l'ampliamento del suo ambito di applicazione andando a coinvolgere anche i seguenti settori:

    - infrastrutture digitali e digital provider;
    - finanza;
    - salute;
    - reti idriche;
    - energia;
    - oil & gas;
    - trasporti;
    - **pubblica amministrazione intese le amministrazioni centrali e regionali con facoltà per i singoli stati membri di valutare se inserire anche gli Enti Locali**
    - reti e servizi per la comunicazione elettronica pubblica;
    - servizi postali;
    - aerospazio
    - prodotti medicali, prodotti chimici, prodotti farmaceutici e dispositivi medicali;

- rifiuti;
- filiera agro-alimentare;
- data center, social network,

estendendo i suoi effetti, dal punto di vita dimensionale, non solo alle medie e grandi società, ma anche alle piccole e piccolissime imprese dividendo le società in società importanti e società essenziali.

2. In secondo luogo la Direttiva NIS2 prevede che gli Stati Membri debbano fare in modo che le società interessate adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi per la sicurezza dei sistemi di rete e di informazione che utilizzati per le loro operazioni o per la fornitura dei loro servizi al fine di prevenire o ridurre al minimo l'impatto degli incidenti sui destinatari dei loro servizi.

   Tali misure tecniche, operative ed organizzative dovranno riguardare in modo particolare:

   1. policy sull'**analisi dei rischi** e sulla **sicurezza dei sistemi informativi;**
   2. sistemi di **gestione degli incidenti**;
   3. sistemi di **business continuity**, come la gestione dei backup e il disaster recovery, e la gestione delle crisi;
   4. misure di gestione della **sicurezza della supply chain**;
   5. la sicurezza nell'acquisizione, sviluppo e manutenzione di reti e sistemi informativi, compresa la gestione e la **divulgazione delle vulnerabilità**;
   6. policy e procedure per **valutare l'efficacia delle misure di gestione del rischio di cybersecurity**;
   7. pratiche di **igiene informatica di base** e formazione in materia di sicurezza informatica;
   8. policy e procedure relative all'uso della **crittografia**;
   9. misure sulla sicurezza delle **risorse umane**, le politiche di controllo degli accessi e la gestione degli asset;
   10. l'uso di **soluzioni di autenticazione a più fattori** o di autenticazione continua, di comunicazioni vocali, video e di testo protette.

   Inoltre, la direttiva prevede che nell'analisi della adeguatezza delle misure di sicurezza si debba tener conto non solo di quelle adottate dalle società rientranti nella normativa, ma anche dai loro rispettivi fornitori.

3. Nel caso di incidenti informatici che abbiano un impatto sulla continuità e fornitura del servizio, l**a Direttiva NIS2 introduce un obbligo di notifica senza ritardo al CSIRT (Team di risposta agli incidenti di sicurezza informatica che ogni Stato deve istituire presso le proprie autorità competenti) e alle stesse autorità competenti** che andrà fatta anche a beneficio dei destinatari del servizio interessato dal cyber attacco, indicando le misure che detti destinatari sono in grado di adottare per reagire all'attacco. Tale notifica dovrà essere effettuata entro 24 ore dalla conoscenza per l'invio di un "early warning" che andrà seguito, entro 72 ore dalla conoscenza, dalla notifica di una analisi dettagliata dell'incidente.

4. La Direttiva NIS2 prevede l'applicazione del **principio dello stabilimento** secondo il quale le società sono soggette solo alla giurisdizione delle autorità dello Stato Membro in cui sono stabilite ad eccezione dei servizi di comunicazione e di rete elettronica che sono soggetti alla

competenza del Paese in cui si trovano i destinatari dei loro servizi e di alcuni servizi online che sono soggetti alla competenza del Paese dell'Unione Europea dove si trova il loro stabilimento principale.

5. La norma prevede poi **poteri minimi di indagine** che le autorità locali devono avere per valutare l'adeguatezza delle misure adottate dalle società fornitrici di servizi essenziali ed importanti tra i quali:

    a) ispezioni in loco e vigilanza a distanza, compresi controlli casuali, effettuati da professionisti formati;
    b) audit sulla sicurezza periodici e mirati effettuati da un organismo indipendente o da un'autorità competente;
    c) audit ad hoc, ivi incluso in casi giustificati da un incidente significativo o da una violazione della presente direttiva da parte del soggetto essenziale;
    d) scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario in cooperazione con il soggetto interessato;
    e) richieste di informazioni necessarie a valutare le misure di gestione dei rischi di cibersicurezza adottate dal soggetto interessato, comprese le politiche di cibersicurezza documentate, nonché il rispetto dell'obbligo di trasmettere informazioni alle autorità competenti;
    f) richieste di accesso a dati, documenti e altre informazioni necessari allo svolgimento dei compiti di vigilanza;
    g) richieste di dati che dimostrino l'attuazione di politiche di cibersicurezza, quali i risultati di audit sulla sicurezza effettuati da un controllore qualificato e i relativi elementi di prova.

    Nonché il potere di:

    a) emanare avvertimenti relativi a violazioni da parte dei soggetti interessati;
    b) adottare istruzioni vincolanti o un'ingiunzione che impongano ai soggetti interessati di porre rimedio alle carenze individuate o alle violazioni;
    c) imporre ai soggetti interessati di porre termine ai comportamenti vietati o di astenersi dal ripeterli;
    d) imporre ai soggetti interessati di provvedere affinché le loro misure di gestione del rischio di cibersicurezza siano conformi alla normativa o di adempiere gli obblighi di segnalazione nei termini previsti;
    e) imporre ai soggetti interessati di informare le persone fisiche o giuridiche cui forniscono servizi o per cui svolgono attività che sono potenzialmente interessati da una minaccia informatica significativa;
    g) designare un funzionario addetto alla sorveglianza con compiti ben definiti nell'arco di un periodo di tempo determinato;
    h) imporre ai soggetti interessati di rendere pubblici gli aspetti delle violazioni in una maniera specificata;
    i) imporre o chiedere l'imposizione, da parte degli organismi o degli organi giurisdizionali pertinenti secondo il diritto nazionale, di una sanzione amministrativa pecuniaria. Gli importi delle sanzioni previste sono fino a € 10 milioni o al 2% del fatturato globale dell'anno precedente in caso di società essenziali, mentre sanzioni fino a € 7 milioni o al 1,7% del fatturato globale in caso di società importanti.
    l) Viene previsto l'obbligo per gli Stati Membri di stabilire la possibilità di sospendere l'attività aziendale dell'impresa e di imporre specifici divieti;

6. Infine la Direttiva prevede l'istituzione di un gruppo di cooperazione tra i CSIRT degli Stati membri e della rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) al fine di collaborare a livello comunitario in materia di cybersicurezza.