NIS 2, novità e dibattito: cosa ci aspetta?

Le minacce in ambito digitale, specialmente di recente, hanno obbligato a rivedere e modificare le prassi e le direttive relative alla protezione dei dati, focalizzando l'attenzione sulla pressante necessità di intervenire tempestivamente su tali rischi. Di fatto sono sempre più numerosi i settori che si affidano alle nuove tecnologie, pertanto concepire sistemi atti a prevenire ed arginare il costante pericolo dei cyberattacchi è diventato non solo necessario, ma addirittura vitale. In quest'ottica si profilano i cambiamenti relativi alla NIS (*Network and Information Security*), noti con la dicitura "NIS 2". Nel presente elaborato verranno analizzati gli aspetti principali di questo documento, posto a confronto con la precedente versione.

Fabio D'Ambrosio

INDICE

Introduzione

In epoca coeva una delle questioni cruciali, spesso oggetto di accese controversie nazionali ed internazionali, è rappresentata dalle ripetute violazioni alle norme di sicurezza informatica. Ricerche recenti ribadiscono infatti quanto queste siano diventate frequenti, complici di un devastante circolo vizioso che dev'essere prontamente interrotto. Il report *Threat landscape 2021* dell'Agenzia dell'Unione europea per la cybersecurity ha registrato un incalzante aumento delle offensive alla sicurezza informatica nel biennio appena trascorso, dovuto anche alla dilagante pandemia di Coronavirus. Come riporta la piattaforma Help Net Security:

"Global lockdowns and remote work caused a rush to put more assets online, which led to an increase in vulnerabilities. In turn, security buyers invested heavily to incentivise ethical hackers to find critical threats, causing P1 and P2 bugs to make up 24% of all valid submissions for the year"[1].

Ciò implica, di conseguenza, l'urgenza crescente dell'implementazione di regolamenti in grado di garantire una difesa maggiore e, al contempo, una celere risposta alle perturbazioni in materia di cybersecurity. Tutto questo concepito nell'ottica di una riacquisita consapevolezza dei riverberi che attacchi digitali possono esercitare su vasta scala, soprattutto in ambito europeo.

[1] HELPNETSECURITY, *Cybersecurity industry trends from 2021 bound to shape this year's threat landscape*, www.helpnetsecurity.com, 21.01.2022.

Per fronteggiare tali pericoli, proprio la Commissione Europea nel 2016 aveva proposto la Direttiva NIS 2016/1148, posta in essere grazie al Decreto Legislativo del 18 maggio 2018, n. 65[2]. La suddetta direttiva si prefiggeva come scopo ultimo quello di stabilire i requisiti minimi relativi alla sicurezza informatica, come anche quelli dei sistemi informativi. In buona sostanza, il *fil rouge* di questa proposta era costituito dalla necessità di delineare un iter strategico che fosse univoco per tutti gli Stati dell'Unione, e che tutelasse da questa tipologia di danni. Nella fattispecie, la Direttiva spazia dalla protezione dai cyberattacchi, al controllo dei rischi informatici, all'identificazione degli incidenti informatici e all'impatto che questi possono esercitare. I suoi obiettivi sono rivolti sostanzialmente a due tipi di operatori nell'ambito dei sistemi informativi, ossia soggetti (privati o pubblici) che elargiscono un certo tipo di servizi. Sintetizzando, sono oggetto di interesse:

- Gli **Operatori di Servizi Essenziali**, i quali operano in ambito sanitario, bancario, infrastrutture digitali, energia, trasporti, ecc.
- I **Fornitori di Servizi Digitali** (FSD), persone giuridiche che operano sul territorio nazionale, offrendo servizi, ad esempio, di e-commerce e *cloud computing*.

Per entrambe queste categorie, la NIS prevede alcuni obblighi inderogabili:

[2] Contaldo A., Flaviano Peluso, *Cybersecurity. La nuova disciplina italiana ed europea alla luce della direttiva NIS*, Pisa, Pacini Giuridica, 2018.

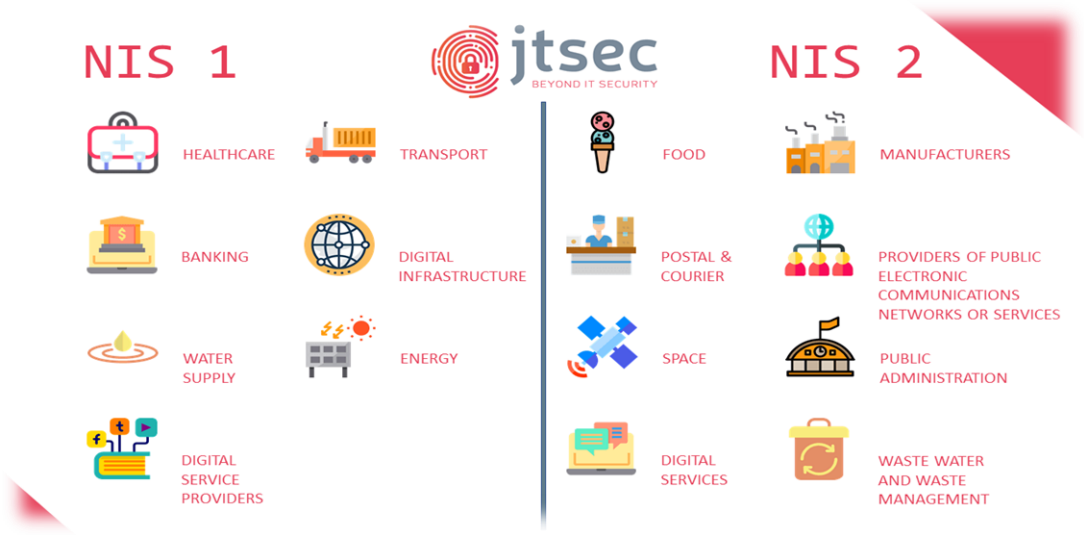
- l'implementazione di prassi organizzative che gestiscano opportunamente i potenziali rischi, e la prevenzione/minimizzazione degli impatti dovuti ad incidenti relativi alla sicurezza delle reti e dei sistemi informativi;
- l'obbligo di rendere noti i suddetti incidenti, nello specifico quelli che inficiano la continuità dell'erogazione dei servizi.

Come prevedibile, lo scopo ultimo della presente direttiva è proprio quello di scongiurare qualsiasi interruzione in questo senso. Benché, quindi, la NIS costituisca uno strumento valido per contrastare l'aumento esponenziale dei cyberattacchi, la Commissione europea ha ritenuto necessario agire in maniera ancora più incisiva, al fine di irrobustire il livello di cybersecurity e cyberresilienza in Europa. In che modo? Mediante un'altra Direttiva, nota come "NIS 2", la quale andrebbe ad abrogare e a perfezionare la precedente disposizione. Tale decisione è stata dettata dall'esigenza di aggiornare quanto specificato nella versione originale, in quanto quest'ultima è stata ritenuta lacunosa in diversi punti decisivi. Secondo Thierry Breton, commissario europeo per il mercato interno, era da tempo che occorreva agire in questo senso. L'urgenza, quindi, è innegabile.

NIS 2: cosa cambia e in che modalità

Quali cambiamenti sono stati apportati alla NIS precedente, e in cosa si differenzia dalla sopracitata NIS 2? Nella fattispecie, il nuovo testo della NIS 2 non contempla la diversificazione tra fornitori di servizi essenziali e digitali, pertanto il parametro di distinzione delle imprese è sancito dalle criticità dei servizi che elargiscono e, in base a

questi, vengono categorizzate in “essenziali” e/o “importanti”. Ad esempio, chi fornisce servizi DNS (*Domain Name System*), di data center/cloud, viene considerato *essenziale*, a differenza dei motori di ricerca o dei social network, che invece vengono catalogati come *importanti*. Inoltre, a differenza della prima versione, la NIS 2 amplia il range della soglia di dimensione di un’azienda, in quanto anche le imprese medie e grandi, operanti in questi settori, verranno incluse nella direttiva (quindi anche le entità con più di cinquanta dipendenti e con un fatturato annuo superiore ai dieci milioni). Tra i servizi essenziali rientrano, inoltre, il settore della Pubblica Amministrazione e il Perimetro di Sicurezza Nazionale Cibernetica, mentre tra gli importanti si annoverano lo smaltimento rifiuti, la manifattura, i servizi postali logistici, ecc. (come si evince dal grafico).



Differenze tra NIS e NIS 2 (*Fonte: www.jtsec.es*)

Nel dettaglio, al punto 20 la proposta asserisce che:

“Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water, health, certain aspects of public administration, as well as space in as far as the

provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market. The COVID-19 pandemic has shown the vulnerability of our increasingly interdependent societies in the face of low-probability risks"[3].

In altre parole, le forti interconnessioni tra gli attori operanti in Europa che forniscono servizi specifici causano, di fatto, un effetto domino su ogni soggetto coinvolto in queste collaborazioni, impattando pesantemente sulla stabilità del mercato interno. La NIS 2, invero, è stata concepita per impedire tutto questo. Oltretutto, costituisce una svolta anche per l'attenzione rivolta ai servizi relativi al settore alimentare e farmaceutico, nonché a quelli specializzati in dispositivi medici e prodotti chimici. Va precisato, in ogni caso, che le aziende di modeste dimensioni vengono escluse dalla direttiva, a meno che non forniscano servizi essenziali all'interno del contesto internazionale, o riguardino settori automaticamente contemplati dalla direttiva, a prescindere dalle dimensioni.

Degno di nota risulta poi l'aspetto del *supply chain*[4]. Cruciale obiettivo strategico della proposta nota come NIS 2, l'ambito della sicurezza informatica relativa alla catena di

[3] European Commission, *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148*, eur-lex.europa.eu

[4] Ruocco T., Network Digital 360, *Direttiva NIS 2, gli sviluppi attuali e gli scenari futuri: il punto*, www.cybersecurity360.it, 20.12.2021.

approvvigionamento viene scandagliato meticolosamente. Testualmente, al punto 43 si legge:

"Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers is particularly important given the prevalence of incidents where entities have fallen victim to cyber-attacks and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should therefore assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures"[5].

Di conseguenza l'importanza degli scambi tra enti e fornitori, dal punto di vista informatico, necessita di un'attenzione particolare, in quanto queste reti risultano notevolmente suscettibili ai cyberattacchi. Di concerto con la Commissione Europea e l'ENISA, secondo la direttiva andrebbero predisposte delle valutazioni dei rischi settoriali delle catene di approvvigionamento, come chiarisce anche il punto 46 della NIS 2:

"To further address key supply chain risks and assist entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related cybersecurity risks, the Cooperation Group involving relevant national authorities, in cooperation with the Commission and ENISA, should carry out coordinated sectoral supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks 21 , with the aim of

[5] *Ibidem*

identifying per sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities"[6].

Le ragioni che soggiacciono alla base di questa focalizzazione sul *supply chain* sono tutt'altro che stocastiche, in quanto rafforzare questa particolare fase concernente le attività delle imprese, garantirebbe maggiore sicurezza nell'ottica dell'intero sistema informativo (compreso il trattamento dei dati personali). Nel dettaglio, il punto 47 ribadisce:

"To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria should be taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, systems or products; (ii) the relevance of specific critical ICT services, systems or products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, systems or products; (iv) the resilience of the overall supply chain of ICT services, systems or products against disruptive events and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities"[7].

Come si evince dal paragrafo appena riportato, la NIS 2 si concentra molto sul promuovere la qualità complessiva delle prassi di cybersicurezza sia delle aziende che dei fornitori, nonché dei prodotti associati. Ad interessare maggiormente, inoltre, è la natura delle dinamiche del mercato ICT: la Commissione europea ha in più di un'occasione ribadito quanto risulti cruciale identificare sistemi e prodotti ICT in stato di criticità, per ogni singolo settore di riferimento.

[6] *Ibidem*
[7] *Ibidem*

Per questa ragione, la direttiva NIS 2 si propone come obiettivo fondamentale il consolidamento dei poteri degli enti nazionali, i quali saranno chiamati a rispettare specifici requisiti e, di conseguenza, verranno sottoposti a controlli e monitoraggi rigorosi. Infatti, in base alla proposta ivi presa in esame, le autorità statali avranno la facoltà di esaminare le entità essenziali attraverso:

- esami in loco;
- supervisione fuori sito (richieste di accesso ai dati, audit regolari, ecc.).

In altri termini, avranno diritto ad accedere a qualsiasi informazione appaia necessaria o propedeutica all'individuazione di criticità eventuali degli scambi informativi.
Altra importante novità della NIS 2 è rappresentata dalla segnalazione degli incidenti: la proposta, stringente su questo punto, obbliga le aziende a segnalare un incidente entro e non oltre un tempo previsto di ventiquattro ore. Dovranno altresì presentare un rapporto iniziale, che verrà poi corredato da uno finale (entro e non oltre un tempo stimato di un mese). *Last but not least*, la NIS 2 conferisce agli Stati membri dell'Unione il potere di imporre sanzioni amministrative di un certo spessore. Nel dettaglio, si riportano cifre pari a 10.000.000 euro, o corrispondenti al 2% del fatturato annuale dichiarato dall'azienda in esame. Il messaggio che viene trasmesso dalla proposta, quindi, è chiaro: ogni qualvolta i servizi offerti violano le norme di cybersicurezza, vi è un obbligo di segnalazione imprescindibile.

…e per quanto riguarda l'Italia?

Quanto esposto sinora si è concentrato sulla proposta NIS 2 dal punto di vista europeo e sovranazionale. Per quanto concerne l'Italia, invece, occorre fare delle specifiche.

Operando una breve digressione, nel caso italiano si richiama l'attenzione sulla nuova *Agenzia per la cybersicurezza*. Quest'ultima, istituita nel maggio dell'anno scorso, è un organo che gode di una discreta autonomia, tuttavia viene costantemente sottoposto a vigilanza dalla presidenza del Consiglio. L'agenzia contempla otto servizi generali, e prevede un organico di circa trecento addetti. Nei prossimi anni sarà previsto un aumento delle risorse ad essa destinate, infatti si stima un budget di centoventidue milioni da destinare all'Agenzia dal 2026[8].

In passato, prima che questa struttura venisse introdotta e resa operativa, l'ambito della cybersicurezza rientrava nelle competenze del *Dipartimento di informazioni per la sicurezza della Repubblica* (DIS). Oggi l'Agenzia, grazie al nuovo Decreto, si trova fuori dal comparto di intelligence, sebbene restino comunque in costante contatto. Infatti il coordinamento col settore dell'intelligence viene assicurato sia dalla delega di quest'ultima (in materia di cybersicurezza) al sottosegretario del governo, sia dall'operato dei rappresentanti delle agenzie d'intelligence presenti nel nucleo per la cybersicurezza (dove operano anche i rappresentati degli altri ministeri). Inoltre, il rappresentante del ministero della difesa garantisce il collegamento con il *Comando operazioni in rete* (Cor), un organo specializzato in cyber-difesa. Di fatto, però, dal punto di vista normativo non è previsto nessun collegamento tra l'Agenzia e il Cor.

NIS 2 e problemi da risolvere: una risposta per tutto?

Dopo aver analizzato brevemente la nuova proposta in materia di cybersicurezza, alla luce anche della precedente versione, ci si interroga sulla sua validità e sulle sue potenziali criticità. Nel confronto datato 18 marzo 2021 era stata valutata positivamente

[8] Openpolis, *L'Italia e le istituzioni per la cybersicurezza*, www.openpolis.it, 04.01.2022

la revisione della NIS, così come anche le novità proposte dalla NIS 2. La NIS 2 si profila, quindi, come una soluzione assoluta e impeccabile? Purtroppo no. Le motivazioni, che a breve verranno enucleate, tengono conto degli aspetti difettivi emersi dall'approfondimento dei suoi punti nevralgici. In primis, è necessario sottolineare come la NIS 2 si mostri lontana da un approccio univoco al problema, in quanto la parcellizzazione del recepimento della direttiva nell'Unione risulta ravvisabile in più di uno snodo. Basti pensare alla proposta dell'Unione Europea per un *regolamento sulla resilienza operativa digitale* (DORA): ciò implicherebbe non poca confusione delle linee guida giuridiche previste per tale disciplinamento, nonché ridondanze difficili da evitare. Un altro aspetto critico della NIS 2 concerne i cambiamenti relativi agli oneri amministrativi aggiuntivi concepiti dalla direttiva, i quali graverebbero eccessivamente sulle aziende, oltre che sul personale che analizza queste informazioni. Risulterebbe opportuno, al contrario, comunicare con esattezza entro quali soglie si è tenuti a segnalare una criticità. La notifica degli incidenti, che la NIS 2 impone di far pervenire entro le ventiquattro ore, all'atto pratico si mostra eccessivamente stringente e inflessibile. Tale onere apparirebbe di fatto oltremodo impegnativo, dal momento che le aziende interessate sono attive in compartimenti intra ed inter statali.

Tempistiche molto più accettabili sarebbero, ad esempio, quelle già contemplate dal *regolamento generale sulla protezione dei dati* (ossia settantadue ore)[9]. A rigor di logica, infatti, i tempi a cui fa riferimento la seconda direttiva non appaiono realistici, tenendo conto dei ritmi serrati a cui sono sottoposte le aziende e i loro collaboratori. È di certo importante raggiungere livelli di sicurezza informatica eccellenti, ma questo può avvenire solo grazie ad una maggiore cooperazione tra i governi e le aziende. Gli

[9] Garante per la protezione dei dati personali, *Violazioni di dati personali (data breach) in base alle previsioni del Regolamento (UE) 2016/679*, www.garanteprivacy.it

attacchi di questo tipo sono rischiosi, e revisionare la precedente NIS è stato di certo doveroso. Tuttavia, per ottenere realmente sistemi più efficaci e protetti, occorre riconsiderare i punti oscuri della proposta, specialmente se si guarda a settori come quello delle forniture. Come spesso accade, non è semplice passare dalla teoria alla pratica ma, qualora gli obiettivi della nuova NIS 2 risultino maggiormente fattibili ed attuabili, i nobili scopi relativi alla cybersicurezza apparirebbero non solo raggiunti, ma anche frutto di una buona sinergia tra gli Stati Membri.

Riferimenti bibliografici/sitografici

- Contaldo A., Flaviano Peluso, *Cybersecurity. La nuova disciplina italiana ed europea alla luce della direttiva NIS*, Pisa, Pacini Giuridica, 2018.
- European Commission, *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148*, eur-lex.europa.eu
- Garante per la protezione dei dati personali, *Violazioni di dati personali (data breach) in base alle previsioni del Regolamento (UE) 2016/679*, www.garanteprivacy.it
- HELPNETSECURITY, *Cybersecurity industry trends from 2021 bound to shape this year's threat landscape*, www.helpnetsecurity.com, 21.01.2022.
- Openpolis, *L'Italia e le istituzioni per la cybersicurezza*, www.openpolis.it, 04.01.2022.
- Ruocco T., Network Digital 360, *Direttiva NIS 2, gli sviluppi attuali e gli scenari futuri: il punto*, www.cybersecurity360.it, 20.12.2021.