DIGITALEUROPE

Recepimento della Direttiva sulla Sicurezza delle reti e dei sistemi informativi nell'Unione (NIS)

Bruxelles, 5 Luglio 2016

SINTESI

ll Consiglio dell'Unione europea ha pubblicato la versione finale della Direttiva sulla Sicurezza delle reti e dei sistemi informativi nell'Unione il 21 aprile 2016. Se, da una parte, questa deve essere formalmente firmata dal Parlamento europeo in estate, dall'altra è vero però che il testo stesso ha già ricevuto il consenso delle tre istituzioni dell'UE e non si prevedono cambiamenti. Gli Stati membri sono ora tenuti a recepire questo testo nella propria legislazione nazionale entro 21 mesi dalla sua adozione. Allo scopo di agevolare questo processo, mettiamo a vostra disposizione nell'Appendice una guida alle migliori prassi che illustrano come recepire gli aspetti rilevanti per l'industria dell'informatica e come riflettere effettivamente le intenzioni di coloro che hanno redatto il testo.

La direttiva NIS dell'Unione europea è la prima legislazione paneuropea sulla sicurezza informatica; si concentra sul rafforzamento delle autorità informatiche, incrementandone il coordinamento, e introduce requisiti di sicurezza per i settori industriali chiave.

Ciascuna legislazione nazionale che la adotti non dovrebbe perdere di vista i due obiettivi principali della Direttiva: (1) garantire un livello elevato di sicurezza informatica delle infrastrutture critiche del paese; (2) porre in essere un meccanismo di cooperazione tra gli Stati membri dell'UE al fine perseguire ulteriormente questo obiettivo. Le risorse dovrebbero essere innanzitutto rivolte al perseguimento di questi due importanti obiettivi.

Per l'industria informatica, le disposizioni relative ai cosiddetti DSP ovvero i fornitori di servizi digitali sono di particolare interesse. La Direttiva stabilisce chiaramente che vi sono differenze fondamentali tra gli operatori di servizi essenziali (OES) ed i fornitori di servizi digitali (DSP). Infatti, questi ultimi non sono da considerare infrastrutture critiche in quanto tali. Come riconosciuto dalla legislazione, un incidente che abbia un impatto su questi servizi digitali apporterebbe un livello di rischio alla sicurezza economica e pubblica di un paese decisamente inferiore. Mantenere la distinzione è fondamentale al fine di utilizzare efficacemente ed efficientemente le scarse risorse a disposizione delle autorità che dovranno controllare l'attuazione delle regole ed applicarle.

Ne consegue che riserviamo una grande attenzione al campo di attuazione dei servizi in questione e chiediamo ai politici di non sottoporre settori diversi da quelli identificati come DSP e OES ai requisiti di sicurezza, nella legislazione nazionale.

In merito alla **giurisdizione**, i DSP dovrebbero essere in grado di fare riferimento alla legislazione vigente nel paese dove sono insediati in via principale anche nei casi in cui siano coinvolte le autorità competenti di più paesi. In fatto di sorveglianza, le autorità competenti dovrebbero seguire un approccio ex-post invece d'imporre un obbligo generale di supervisione dei DSP. Inoltre, dovrebbero concentrarsi sui risultati e mantenere la distinzione tra OES e DSP non assoggettando questi ultimi a requisiti non previsti dalla Direttiva, quali audit e istruzioni cogenti.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Bruxelles [Belgio]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Membro del registro di trasparenza per la Commissione europea: 64270747023-20

Le misure di sicurezza applicate ai DSP dovrebbero differire da quelle per gli OES, dal momento che la Direttiva afferma che questi rappresentano un rischio di sicurezza considerevolmente inferiore. I decisori dovrebbero raggiungere l'obiettivo di armonizzare questi servizi, riconoscere gli standard internazionali esistenti e portati avanti dalle realtà industriali, evitare mandati sulla tecnologia e rispettare il diritto dei DSP alla definizione delle misure di sicurezza più appropriate per i propri sistemi, come contemplato dalla Direttiva. La segnalazione degli incidenti dovrebbe anch'essa essere armonizzata il più possibile a livello europeo e dovrebbe concentrarsi sugli incidenti che abbiano un impatto sulla continuità del servizio, rispettare la flessibilità in fatto di notifica e creare un ambiente di fiducia che incoraggi la condivisione d'informazioni senza esporre la parte notificante a maggiori responsabilità.

Le misure imposte agli OES avranno anch'esse un impatto su altri settori industriali poiché le misure di sicurezza e le segnalazioni degli incidenti saranno contemplate tra le regole del contratto. Ciò vale particolarmente per i servizi cloud. Ne consegue che i DSP potrebbero essere indirettamente soggetti alle leggi nazionali dei loro clienti; abbiamo pertanto un grande interesse nel vedere misure di sicurezza riconosciute a livello internazionale applicate a questi servizi. Proponiamo inoltre il massimo coordinamento e sinergie possibili tra gli obblighi di segnalazione sia per gli OES che per i DSP, visto che è molto probabile che questi ultimi siano soggetti a doppia notifica.

La Direttiva ambisce a raggiungere un alto livello comune di sicurezza delle reti e sistemi d'informazione al fine di migliorare il funzionamento del mercato interno. Al fine di raggiungere questo ambizioso obiettivo, i recepimenti nazionali dovrebbero concentrarsi su un approccio basato sul rischio, armonizzato ed internazionale che consenta ai privati la flessibilità di adeguarsi ad un ambiente di rischio in continuo mutamento, che consenta alle autorità informatiche di concentrare le limitate risorse sulle sfide più significative, e che riconosca che la soluzione a problemi che non conoscono frontiere debba essere globale. Speriamo che questa guida sia uno strumento utile a questo fine e restiamo a vostra disposizione per qualunque ulteriore domanda che potreste avere in merito.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Bruxelles [Belgio]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Membro del registro di trasparenza per la Commissione europea: 64270747023-20

Allegato: Guida alle Migliori Prassi per il recepimento della Direttiva NIS

1. Provider di servizi digitali (DSP)

a) Campo di applicazione

- La Direttiva stabilisce che i mercati online, i motori di ricerca online e i servizi cloud debbano essere considerati erogatori di servizi digitali online e quindi debbano rientrare nel campo d'applicazione della stessa Direttiva. Sebbene questa sia una Direttiva di armonizzazione minima (Articolo 2), è importante mantenere coerenza in tutta l'UE; di conseguenza gli Stati membri non dovrebbero assoggettare ai requisiti di sicurezza nessun settore se non quelli individuati come DSP o OES – come definito dall'Articolo 3 –, nella legislazione nazionale.

- La Direttiva stabilisce esplicitamente che i produttori di hardware e gli sviluppatori di software non sono OES o DSP e quindi non dovrebbero essere coperti dalle leggi nazionali in attuazione della Direttiva (Considerando 50).

- La Direttiva esclude esplicitamente dal suo campo d'applicazione i servizi online offerti su mercati online che agiscano come intermediari verso servizi terzi dove le vendite o i contratti di servizio vengono poi conclusi (e.g. siti comparazione) (Considerando 15).

- Le funzioni di ricerca limitate al contenuto di uno specifico sito web non dovrebbero essere coperte alla stregua dei motori di ricerca online, anche se fanno uso di un provider esterno (Considerando 16).

- La definizione di un servizio informatico cloud secondo la Direttiva dipende dalle risorse informatiche condivise con una molteplicità di utenti (Articolo 4(19) e Considerando 17). Visto che le cloud private (diversamente dalle cloud pubbliche) sono riservate a singole organizzazioni, non dovrebbero rientrare nel novero in questione.

- La Direttiva sottolinea che vi sono differenze fondamentali tra OES e DSP, ragion per cui i DSP sono soggetti a regole diverse (Considerando 57). Tale distinzione dovrebbe essere mantenuta nell'attuazione della Direttiva.

b) Giurisdizione e Controllo

- La giurisdizione sui DSP dovrebbe essere attribuita ad un unico Stato Membro, segnatamente quello ove l'operatore ha il suo stabilimento principale nell'UE, che corrisponde essenzialmente al luogo dove ha la sua sede centrale (Articolo 18.1 e Considerando 64). Noi sosteniamo che i DSP dovrebbero fare tale determinazione loro stessi e che questa decisione sia soggetta a revisione unicamente nei casi in cui le autorità competenti non siano d'accordo in merito, nell'ambito delle operazioni di supervisione ex-post.

- Laddove i DSP abbiano sistemi di rete ed informazione in paesi altri rispetto a quelli dove hanno il proprio stabilimento principale, l'Articolo 17.3 prevede che le autorità competenti cooperino. Dal punto di vista dei DSP, comunque, è importante che la legge vigente rimanga quella del paese in cui hanno stabilimento

principale e che rimangano responsabili unicamente di fronte all'autorità competente in tale giurisdizione, la quale fungerà da loro interlocutore.

- La Direttiva sottolinea che i DSP sono soggetti a supervisione ex-post reattiva e che pertanto le autorità competenti non hanno generalmente l'obbligo di supervisionare i DSP e dovrebbero intervenire attivamente solo quando previsto per provata necessità. (Articolo 17.1 e Considerando 60). Tali disposizioni dovrebbero essere mantenute nell'attuazione della Direttiva.

- Diversamente da quanto stabilito per gli OES, nel caso dei DSP le autorità possono soltanto richiedere informazioni e richiedere che i DSP rimedino a qualsiasi problema intervenuto. La Direttiva chiarisce che le autorità non hanno alcun potere di audit e non possono determinare nessuna istruzione cogente. Queste disposizioni dovrebbero essere rispettate anche a livello nazionale.

c) Requisiti ulteriori

- I requisiti di sicurezza e notifica per i DSP sono soggetti ad un'armonizzazione massima (Articolo 16.10). Questo Articolo dovrebbe essere considerato applicabile a prodotti, servizi e soluzioni che ne costituiscono la rete, e sistemi d'informazione. Ne consegue che disposizioni aggiuntive, come i test di prodotto, non dovrebbero essere richieste nella misura in cui prodotti e servizi siano utilizzati in questo contesto.

d) Misure e Standard di Sicurezza

- Le misure di sicurezza applicate ai DSP dovrebbero essere meno stringenti rispetto a quelle per gli OES. I DSP dovrebbero essere liberi di definire il modo in cui garatiscono la sicurezza oltre che il modo in cui intendono garantire la protezione della loro rete e sistemi d'informazione, ritenuti appropriati in considerazione dei rischi connessi (Considerando 49).

- Le misure di sicurezza dovrebbero essere orientate ai processi e concentrarsi sulla gestione del rischio. Non dovrebbero richiedere che i prodotti ICT siano concepiti, sviluppati o prodotti in una maniera particolare (Considerando 51).

- La Direttiva enfatizza che gli Stati membri non impongano nessun requisito di sicurezza ulteriore ai DSP (Articolo 16.10).

- Ciononostante, ci aspettiamo linee guida da diversi attori. Gli Stati membri garantiranno che le misure definite dalla Direttiva siano adottate (Articolo 16.1), potranno incoraggiare l'uso di standard per la loro implementazione (Articolo 19.1) e discutere gli standard con le Organizzazioni di normalizzazione europee all'interno del Gruppo di cooperazione (Articolo 11.3(h)). L'ENISA consiglierà circa gli standard appropriati (Articolo 19.2) e la Commissione europea è incaricata degli atti di esecuzione sulle misure di sicurezza (Articolo 16.8).

- Visto il livello di complicazione e dei benefici dell'armonizzazione, consigliamo che il processo nazionale sia fondamentalmente rinviato agli atti attuativi per convenire le misure appropriate, i quali, in ogni caso, dovranno essere finalizzati nel giro di un anno dall'adozione della Direttiva. Gli atti d'esecuzione

dovrebbero essere tali da non recare pregiudizio alla capacità dei DSP di definire le misure di sicurezza più appropriate per i propri sistemi.

- L'Articolo sugli standard consente agli standard europei o accettati a livello internazionale di essere referenziati (Articolo 19.1). Vista la maturità degli standard internazionali vigenti in questo ambito, raccomandiamo che laddove sussistano standard appropriati, la certificazione che si riferisca ad uno di essi (come ISO 27001) sia considerata sufficiente per ottemperare ai requisiti.

- In ogni caso, la certificazione standard dovrebbe essere opzionale, non obbligatoria. L'Articolo 19 sottolinea che un qualsiasi standard può essere solo "incoraggiato" e questo "senza imporre o discriminare a favore dell'uso di una particolare tecnologia."

e) Ricadute sulla segnalazione di incidenti di sicurezza

- Per quanto riguarda le misure di sicurezza, secondo quanto disposto della Direttiva NIS, diversi attori svolgono un ruolo nell'impostazione delle segnalazioni di incidenti. Gli Stati membri devono assicurare che i DSP notifichino gli incidenti di sicurezza che abbiano un impatto significativo sull'erogazione del servizio (che rientri nell'ambito di applicazione della Direttiva) che offrono (Articolo 16.3); il Gruppo di cooperazione è incaricato di discutere le modalità per le notifiche (Articolo 11.3(m)); e la Commissione è incaricata degli atti di esecuzione (Articoli 16.8 e 9).

- Ancora una volta, la nostra raccomandazione è che i recepimenti a livello nazionale rinviino il processo agli atti di esecuzione, il cui atto di esecuzione relativo alla soglia per la notifica deve essere adottato entro un anno dalla finalizzazione della Direttiva.

- In merito al tipo d'incidenti che dovrebbero essere segnalati, corre l'obbligo per i DSP di notificare "qualsiasi incidente che abbia un impatto sostanziale sull'erogazione del [proprio] servizio" (Articolo 16.3). Per quanto riguarda l'attuazione di disposizioni equivalenti per gli operatori telefonici ai sensi dell'Articolo 13a della Direttiva quadro, riteniamo che ciò dovrebbe essere interpretato concentrandosi sulla **continuità (o disponibilità)** dei servizi erogati. In altre parole, quelle interruzioni che raggiungono una particolare soglia (da determinare attraverso gli atti di esecuzione) dovrebbero essere segnalate piuttosto che qualsiasi altro tipo d'incidente di sicurezza. Ciò presenta il vantaggio di concentrarsi sugli incidenti che abbiano maggiore probabilità d'impattare l'economia o la società minimizzando (senza per questo eliminarla completamente) la sovrapposizione con il disposto relativo alla notifica di violazione dei dati personali di cui al Regolamento Generale sulla Protezione dei Dati.

- Inoltre, l'obbligo di segnalazione per gli "Operatori di servizi essenziali" (OES) specifica che questi operatori dovranno notificare gli "incidenti che abbiano un impatto significativo sulla continuità dei servizi essenziali che offrono ", il che pone l'accento nuovamente sulla continuità (o disponibilità)" del servizio. I colegislatori hanno convenuto che gli obblighi per i DSP dovrebbero essere meno stringenti di quelli previsti per gli OES (vedi Considerando 49). Pertanto, l'obbligo di notifica degli incidenti per i DSP, come disposto dalla Direttiva NIS, non dovrebbe essere più ampio rispetto a quello previsto per gli OES, ed anzi dovrebbe essere ancor più rigorosamente impostato in termini di soglie. Questo, ancora una volta, sottolinea che la segnalazione d'incidenti per i DSP dovrebbe essere limitato agli incidenti che raggiungono una particolare soglia e **hanno un impatto sulla continuità/disponiblità del servizio** e non gli

incidenti afferenti all'integrità o riservatezza dei dati, i quali sono in larga misura coperti dai relativi obblighi di notifica disposti dai regolamenti GDPR ed eIDAS.

- In merito ai tempi di notifica, apprezziamo la flessibilità implicita nella formulazione linguistica riguardante la segnalazione "senza indebito ritardo" (Articolo 16.3). L'attuazione non dovrebbe portare a scadenze perentorie poiché gli incidenti variano significativamente nella loro complessità. Tempi uniformi per la segnalazione porterebbero a segnalazioni inaccurate dove la portata iniziale dei sistemi impattati non è chiara e avrebbero un impatto sulla capacità dei professionisti che si occupano di gestione degli incidenti di dare priorità alla reazione all'incidente piuttosto che alla relativa segnalazione.

- Come discusso, gli incidenti di sicurezza da notificare secondo quanto disposto dalla Direttiva potrebbero richiedere anche una notifica ai sensi della legge sulla protezione dei dati, a seconda se vi sia una violazione dei dati personali. Non solo questo significa segnalare lo stesso incidente a diverse autorità, ma queste autorità potrebbero anche trovarsi in Stati membri diversi dipendendo dalla giurisdizione applicabile ai DSP ai sensi dei due diversi diritti vigenti. Raccomandiamo agli Stati membri di riconoscere la necessità e sforzarsi di prevedere la notificazione singola degli incidenti e cercare di creare canali di comunicazione per condividere tra loro informazioni pertinenti, senza recare pregiudizio alla riservatezza dei dati aziendali.

- Le autorità competenti dovrebbero prendere in considerazione le implicazioni reputazionali e commerciali per i DSP prima di condividere informazioni sugli incidenti pubblicamente. Ancor più importante, la divulgazione dell'incidente potrebbe esacerbare il rischio di sicurezza. Pertanto, è importante coordinarsi con gli attori coinvolti prima della divulgazione.

- La Direttiva enfatizza che l'informazione che sia considerata confidenziale sia trattata come tale (Considerandi 41, 59, Articolo 1.5).

- L'Articolo 16.3 sottolinea che la notifica d'incidenti di sicurezza non dovrebbe esporre la parte notificante ad una maggiore responsabilità.

2. Operatori essenziali

a) Ricadute sulle Misure di Sicurezza

- I DSP che hanno degli OES come clienti saranno soggetti a misure di sicurezza applicabili derivanti dagli obblighi statutari imposti agli operatori essenziali, scaturite dalle trattative contrattuali (Articolo 14.1). In questo modo, potrebbero essere indirettamente soggetti alla legge nazionale dei loro clienti, a prescindere dalla legge vigente nel paese delle loro sedi centrali europee.

- Ne risulta che sforzi per armonizzare le misure di sicurezza sugli operatori essenziali sono benvenuti. Se è vero che gli Stati membri hanno il diritto d'imporre obblighi più stringenti agli operatori essenziali rispetto a quelli previsti dalla Direttiva (Articolo 3), raccomandiamo moderazione a riguardo e incoraggiamo gli Stati membri a lavorare per un approccio armonizzato. Ciò potrebbe essere raggiunto evitando misure ulteriori nei recepimenti nazionali e cercando di determinare misure di sicurezza appropriate in seno al Gruppo di cooperazione, piuttosto che concentrarsi sulla procedura nazionale.

- Gli obbilghi di sicurezza dovrebbero essere il più possibile basati su standard internazionali (come le serie ISO 27) e buone pratiche di sicurezza riconosciute.

- Le misure di sicurezza imposte agli OES non dovrebbero in nessun caso richiedere che particolari prodotti ICT siano concepiti, sviluppati o prodotti in un modo specifico (Considerando 51).

b) Ricadute sulla segnalazione degli incidenti di sicurezza

- Gli OES sono tenuti a segnalare ai propri DSP contrattati incidenti di sicurezza che abbiano un impatto sulla continuità dei loro servizi essenziali (Articolo 16.5). Ai DSP verrà quindi chiesto per contratto di segnalare all'operatore essenziale in questione gli incidenti di sicurezza che potrebbero avere un impatto su di essi.

- Apprezziamo la flessibilità in fatto di tempi di notifica stabilito per gli OES di cui alla frase "senza indebito ritardo" (Articolo 14.3). I recepimenti nazionali non dovrebbero introdurre particolari scadenze e, in ogni caso, se agli OES viene chiesto di giustificare il tempo necessario per la notifica, il periodo rispetto a cui vengono giudicati dovrebbe iniziare dal momento in cui gli OES sono informati dell'incidente, non da quando i DSP ne sono informati.

- L'Articolo 14.7 prevede che sia il Gruppo di cooperazione a stilare una guida sulle circostanze per la notifica, diversamente dal ruolo di armonizzazione attribuito alla Commissione per le notifiche dei DSP. Dato il doppio obbligo di segnalazione per i DSP, è importante che i requisiti di notifica rispettivi non siano in contraddizione e siano allineati il più possibile. Pertanto, questo processo dovrebbe essere vagliato in vista di questo obiettivo. Inoltre, i requisiti di notifica per i DSP dovrebbero rispettare gli obblighi di riservatezza che hanno rispetto ai loro clienti OES e non chiedere loro di condividere informazioni aziendali riservate e confidenziali.

A PROPOSITO DI DIGITALEUROPE

DIGITALEUROPE rappresenta l'industria della tecnologia digitale in Europa. Fra i suoi membri conta le più grandi società al mondo nel settore dell'IT, telecomunicazioni ed elettronica di consumo oltre che associazioni nazionali da ogni parte d'Europa. DIGITALEUROPE mira a che le aziende ed i cittadini europei beneficino pienamente delle tecnologie digitali e che l'Europa possa dunque crescere, attrarre e sostenere le migliori società al mondo nel settore della tecnologia digitale.

DIGITALEUROPE garantisce la partecipazione all'industria nello sviluppo ed attuazione delle politiche UE. I membri DIGITALEUROPE sono 62 società e 37 associazioni commerciali nazionali di tutta Europa. Il nostro sito web http://www.digitaleurope.org fornisce maggiori informazioni sulle nostre novità ed attività recenti. http://www.digitaleurope.org/

MEMBRI ADERENTI

Società

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Ingram Micro, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies, ZTE Corporation.

Associazioni commerciali nazionali

Austria: IOÖ
Bielorusssia: INFOPARK
Belgio AGORIA
Bulgaria: BAIT
Cipro CITEA
Danimarca: DI Digital, IT-BRANCHEN
Estonia: ITL
Finlandia FFTI
Francia: AFNUM, Force Numérique, Tech in France
Germania: BITKOM, ZVEI
Grecia SEPE
Ungheria: IVSZ
Irlanda ICT Irlanda
Italia ANITEC
Lituania: INFOBALT
Paesi Bassi: Nederland ICT, FIAR
Polania: KIGEIT, PIIT, ZIPSEE
Portogallo: AGEFE
Romania: ANIS, APDETIC
Slovachia: ITAS
Slovenia: GZS
Spagna AMETIC
Svezia: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Svizzera: SWICO
Turchia Turchia Digital Turkey Platform, ECID
Ucraina: IT UKRAINE
Regno Unito techUK