Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

NIS in Italia, due rischi per le aziende con l'applicazione del decreto

LINK: https://www.agendadigitale.eu/sicurezza/nis-in-italia-due-rischi-per-le-aziende-con-lapplicazione-del-decreto/

NIS in Italia, due rischi per le aziende con l'applicazione del decreto Home Sicurezza digitale Condividi questo articolo L'applicazione della Direttiva NIS rischia di creare problemi alle aziende italiane. Per la moltiplicazione degli obblighi di notifica di incidenti informatici e per le possibili conseguenze sullo sviluppo del commercio elettronico in Italia. Ecco qualche dubbio applicativo 1 minuto fa Giuseppe Vaciago Partner R&P Legal e fondatore di Tech&Law Center Sorgono alcuni problemi applicativi, rilevanti per le aziende, dall'applicazione della Direttiva NIS (Network Information Security), dopo il D.lgs. 18 maggio 2018, n. 65 che la attua in Italia. Con danni possibili, in particolare, per le aziende del commercio elettronico italiano. Vediamo perché, ricordando per prima cosa che la Nis si occupa dell'ambito dell'economia digitale esposto in maniera più grave alle conseguenze degli attacchi informatici. Si tratta delle cosiddette 'infrastrutture critiche' gestite dagli operatori di servizi definiti 'essenziali'. La difesa dei servizi essenziali richiede gestione e valutazione del rischio cibernetico e degli impatti legati agli attacchi ai servizi medesimi. A questi operatori di sistema sono sempre più intimamente connessi i fornitori di servizi digitali anch'essi destinatari di tale normativa. A distanza di 3 mesi dall'entrata in vigore (24 giugno 2018) del Decreto e in attesa che, entro il 9 novembre 2018, i 5 ministeri competenti per materia (sviluppo economico, infrastrutture e trasporti, economia, salute e ambiente), identifichino per ciascun settore e sotto-settore, gli operatori di servizi essenziali, è forse giusto porsi un paio di dubbi applicativi, rimandando agli ottimi articoli di Luca Tosoni, Corrado Giustozzi e Luisa Franchina per un approfondimento più esaustivo sulla Direttiva NIS e la sua attuazione in Italia. Indice degli argomenti La moltiplicazione degli obblighi di notifica L'applicazione della Direttiva NIS al commercio elettronico I numeri del commercio elettronico in Italia Le nuove incognite per il settore La moltiplicazione degli obblighi di notifica Il primo dubbio è stato già oggetto di alcuni commenti e riguarda la c.d. duplicazione delle notifiche di incidenti informatici. A livello europeo le normative che hanno previsto l'obbligatorietà di notifica oltre al GDPR e alla Direttiva NIS sono: il Regolamento (UE) n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS) . la Direttiva 2009/136/CE (direttiva sui diritti dei cittadini) e regolamento (UE) n. 611/2013 (regolamento sulla notifica delle violazioni). Il risultato di questa proliferazione normativa, come ci ricorda puntualmente Giusella Finocchiaro, può avere delle conseguenze significative in termini pratici: nel settore Bancario, ad esempio, gli obblighi di notifica sono addirittura quattro. Oltre, ai 3 citati (GDPR, NIS e eIDAS) si aggiunge quello della Circolare n. 285 del 17 dicembre 2013 della Banca d'Italia la quale prescrive una tempestiva comunicazione degli incidenti di sicurezza informatica alla Banca Centrale Europea o alla Banca d'Italia. Insomma, uno scenario frammentato e piuttosto complesso soprattutto se, come saggiamente già il Garante Europeo ci anticipava nel 2013 nel suo parere alla proposta di Direttiva NIS, non

Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

viene elencato il contenuto e il formato di detta notifica, compresi i tipi di dati personali che devono essere notificati e se, e in quale misura, la notifica e i relativi documenti giustificativi debbano includere parti di dati personali interessati da uno specifico incidente di sicurezza (come ad esempio gli indirizzi IP). Inoltre, non sono stabilite appropriate misure di salvaguardia per garantire l'adeguata protezione dei dati trattati dalle autorità competenti per la sicurezza delle reti e dell'informazione. L'applicazione della Direttiva NIS al commercio elettronico Il secondo dubbio applicativo riguarda l'applicazione del D.lgs. 65/18 al settore del commercio elettronico. Come ricordato, le due macro-categorie sono gli operatori di servizi essenziali e i fornitori di servizi digitali. Questi ultimi sono stati suddivisi in tre sotto-settori: mercato online; motori di ricerca online; servizi di cloud computing. Si definisce 'servizio digitale', un servizio ai sensi dell'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, di un tipo elencato nell'allegato III. In sostanza, è fornitore di servizio digitale, qualsiasi persona giuridica che fornisce un servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi. Pertanto, quando pensiamo ai fornitori di servizi digitali non dobbiamo pensare solo ai grandi provider, ma a tutte le società che offrono servizi di commercio elettronico. È vero che sono invece esenti dall'ambito di applicazione della NIS le microimprese e le piccole imprese quali definite nella raccomandazione della Commissione europea del 6 maggio 2003, n. 2003/361/CE. Per intenderci, sono escluse le imprese che occupano meno di 250 persone, il cui fatturato annuo non supera i 50 milioni di euro oppure il cui totale di bilancio annuo non supera i 43 milioni di euro. I numeri del commercio elettronico in Italia Tuttavia, il commercio elettronico è un settore (forse l'unico in Italia) in costante sviluppo. Mi permetto una piccola digressione citando alcuni dei dati pubblicati in una recente ricerca sull'e-commerce di Casaleggio e Associati. In Italia, sono 43 i milioni di italiani che dichiarano di poter accedere ad Internet attraverso dispositivo fisso o mobile, pari all'89,9% della popolazione. Molti di questi scelgono di acquistare online. Per questa ragione, il 74% delle aziende italiane investirà parte delle proprie risorse per poter vendere online anche su piattaforma autonoma considerati gli esigui margini garantiti da marketplace come Amazon ed Ebay. In particolare, il 58% di loro lo farà tramite risorse interne, il 42%, con consulenti esterni specializzati su marketing e e-commerce (25%), legata alla funzione generale di pianificazione (11%) o specializzata in anticipazioni di futuri possibili (6%). Le nuove incognite per il settore Sulla base di questi numeri è evidente che molte realtà imprenditoriali italiane (ossia quelle con un fatturato superiore ai 50 milioni) si stanno timidamente affacciando al mondo del commercio elettronico. Le domande (assolutamente non retoriche) da porsi sono le seguenti: queste realtà lo sanno che devono rispettare la Direttiva NIS? E se lo sanno, l'obbligo di rispettare una direttiva pensata per proteggere le infrastrutture critiche di un Paese non rischia di frenare iniziative di questo tipo, sicuramente utili per la crescita del Paese, e di portare tale imprenditoria a delegare a intermediari terzi (Amazon, eBay) tale tipologia di business? Non è facile dare una risposta a queste domande perché il bilanciamento degli interessi in gioco (libertà d'iniziativa economica vs sicurezza dei cittadini) è sicuramente rilevante. Posso solo dire che ho la sensazione che la prossima ricerca sugli investimenti nel settore dell'e-commerce mostrerà, nella categoria consulenti esterni specializzati, anche la voce relativa ai consulenti legali e agli esperti in cybersecurity.