@iip Associazione Italiana INTERNET Provider

Spettabili Commissioni Riunite
I° - Affari costituzionali, Presidenza del Consiglio e Interni
IX° - Trasporti, Poste e Telecomunicazioni

Oggetto: memoria scritta di AIIP in relazione all'Atto del Governo n. 164, recante recepimento della direttiva (UE) 2022/2555

L'Associazione Italiana Internet Provider ("AIIP") ringrazia per l'opportunità di presentare le proprie osservazioni sullo *"Schema di decreto legislativo recante recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione..."* (cd. "Direttiva NIS 2").

AIIP è attiva dal 1995 e conta circa 60 imprese (prevalentemente medie e alcune grandi): operatori italiani che forniscono reti e servizi di comunicazioni a banda ultralarga, anche in fibra ottica (FTTH) e/o radio (*FWA*) e i principali fornitori italiani di servizi *cloud*.

AIIP offre quindi una visione ampia ed equilibrata sulla cibersicurezza poiché rappresenta gli interessi sia dei fornitori di reti e servizi di comunicazione sia di servizi *cloud* e *edge*, tutti direttamente e pervasivamente disciplinati dallo Schema di provvedimento in esame.

1. Considerazioni preliminari: le ragioni sottese alle osservazioni di AIIP.

Reti e servizi di comunicazioni e servizi *cloud* ed *edge* sono sempre più convergenti tra loro, anche per la progressiva virtualizzazione di prodotti, *software* e servizi di comunicazione (quasi tutto è virtualizzabile: *Software As a Service* "SAaS", *Infrastructure as A Service "IAaS"*, etc.). Inoltre, la dimensione di tali mercati è sempre più ampia, sia per il perimetro geografico, pressoché globale, sia quanto ai volumi di fatturato generato.

Garantire la sicurezza di reti e servizi di comunicazioni e dei servizi *cloud* ed *edge* è dunque fondamentale non solo perché sono le strutture, fisiche e virtuali, portanti e di connessione del tessuto sociale ed industriale del Paese ma anche perché, in prospettiva, diverranno esse stesse il mercato, la piazza, sulla quale si svolgeranno le attività del Paese.

Tale inquadramento del problema, tuttavia, viaggia di pari passo con la valutazione che la sicurezza di una rete, di una struttura fisica (datacenter) o di sistemi informativi fisici non fornisce alcuna garanzia sulla sicurezza del *software* che viene eseguito al di sopra di essi o per il tramite di essi e quindi sulla sicurezza delle *applicazioni*. Le politiche di sicurezza, quindi, dovrebbero concentrarsi prevalentemente a livello *applicativo* con le stesse procedure software che dovrebbero essere progettate sull'assunto di utilizzare una struttura considerata *non-sicura (zero trust)* e di ottenere quindi la sicurezza tramite adeguata progettazione *software*.

La sicurezza costituisce però un costo industriale, per lo più fisso, che pesa diversamente su servizi e prodotti finali in funzione delle diverse dimensioni dei soggetti gravati. Occorre quindi soppesare rischi ed opportunità per le imprese italiane che competono, in una dimensione

globale, con i cd "*hyperscalers*", che dominano il mercato mondiale[1]: qualora fossero imposti costi eccessivi rispetto agli altri Paesi, si rischierebbe l'ennesima migrazione di imprese italiane all'estero, agevolata dalla virtualizzazione e dalla libera circolazione dei prodotti, prestazione dei servizi e stabilimento delle attività economiche in UE.

AIIP ha sempre sostenuto che i ricavi generati in Italia debbano essere tassati in Italia e reinvestiti efficientemente in Italia, anche valorizzando le realtà imprenditoriali da essa rappresentate, e ritiene essenziale che la sicurezza dell'intero sostrato sociale e produttivo sia garantita avendo a mente la dimensione globale del mercato e disciplinando nel modo più efficiente ed equilibrato possibile gli obblighi imposti alle imprese italiane.

Per AIIP è quindi necessario: circoscrivere adeguatamente i soggetti gravati dagli obblighi disposti dal decreto legislativo di recepimento della Direttiva NIS 2 e chiarire che le misure di gestione dei rischi per la sicurezza informatica, le attività di monitoraggio, di analisi e di supporto e le "misure di esecuzione" (sanzioni amministrative, etc.), siano distinte in funzione delle dimensioni degli operatori interessati e delle diverse attività da essi svolte.

2. Adeguata individuazione e/o differenziazione delle diverse misure di gestione dei rischi per la sicurezza informatica di cui all'art. 24 dello Schema

Benché il principio ricorrente nella NIS2, quanto alla definizione delle misure di gestione dei rischi per la sicurezza informatica sia quello della cd. "*accountability*", ossia la "responsabilizzazione" o "autodeterminazione" da parte dei destinatari della normativa recata dalla Direttiva NIS2, AIIP ritiene fondamentale, particolarmente in relazione alle PMI o quanto meno alle Piccole Imprese, che siano espressamente indicate, eventualmente anche dalla ACN in un momento successivo, prevedendo una espressa delega a tal fine nell'art. 24 dello Schema (ad esempio prevedendo diversi livelli di misure da adottare in funzione del diverso fatturato sviluppato dalle imprese interessate), le misure di gestione dei rischi per la sicurezza informatica di cui all'articolo 24 dello Schema.

Tali misure, come eventualmente indicate da ACN, dovranno essere proporzionate alle dimensioni delle imprese destinatarie degli obblighi relativi (e ciò anche all'interno di ciascuna delle categorie di soggetti importanti e di soggetti essenziali).

Diversamente, una modalità di esecuzione basata solo sulla autoresponsabilità rischia di rendere estremamente gravoso (prima ancora che rischioso e a "macchia di leopardo") il soddisfacimento degli obblighi da parte delle PMI.

3. Adeguata segmentazione delle attività di monitoraggio analisi e supporto di cui all'articolo 35 dello Schema

Parimenti, AIIP ritiene importante che le attività di monitoraggio analisi e supporto di cui all'articolo 35 dello Schema siano diversificate in funzione del diverso profilo dei destinatari delle stesse, mentre attualmente non è prevista alcuna segmentazione e/o diversificazione nei

1 Al 31/12/2021 Google Cloud, Amazon Web Services e Microsoft Azure avevano il 69% del mercato mondiale dei servizi *cloud* e *edge*, mentre OVH, il principale operatore europeo, appena il 2% circa.

poteri dell'Autorità Nazionale competente NIS (ACN) per lo svolgimento di tale attività, benché sia evidente che la richiesta di adottare specifici "*Audit*" sulla sicurezza (di cui all'articolo 35.3, lettera "b") ha una valenza molto diversa secondo il profilo dimensionale del destinatario della richiesta stessa).

Sarebbe necessario, ad avviso di AIIP, modificare l'articolo 34, comma 10, dello Schema per conferire la delega in tali termini ai fini della predisposizione del decreto del Presidente del Consiglio dei Ministri (prevista dalla norma cit.), per stabilire i criteri, le procedure e le modalità per lo svolgimento delle attività di verifica, vigilanza ed esecuzione di cui al capo V dello Schema di decreto.

Inoltre, sarebbe opportuno che, quanto alle attività che verranno svolte dalla Autorità Nazionale competente Nis2 (ACN) ai sensi dell'articolo 35, comma 3, dello Schema di decreto, fossero indicati specificamente "*modalità e termini ragionevoli e proporzionati per adempiere*".

4. Adeguata segmentazione delle misure di esecuzione di cui all'articolo 37 dello Schema

Ragionamenti analoghi a quelli svolto ai punti 2 e 3 valgono anche per le misure di esecuzione, di cui all'articolo 37 dello Schema di decreto, che possono essere disposte dalla autorità Nazionale competente NIS2 (ossia ACN), poiché attualmente non è effettuata alcuna distinzione in funzione del diverso profilo dimensionale dei destinatari delle misure di esecuzione.

5. Eliminare ogni discriminazione quanto a sanzioni amministrative tra privati pubbliche amministrazioni. Ridurre l'importo edittale minimo della sanzione, ove previsto, e prevedere un ammontare edittale minimo ove non previsto (così da consentire l'eventuale oblazione)

Ad avviso di AIIP è altresì necessario eliminare ogni discriminazione quanto agli importi delle sanzioni amministrative tra privati e pubbliche amministrazioni e ciò, non tanto per il massimo edittale (la cui differenza è comunque discriminatoria), ma soprattutto per l'assenza per le sanzioni relative ad alcuni specifici casi di violazione applicabili ai privati, del minimo edittale, che costituisce condizione necessaria per poter eventualmente procedere con l'oblazione.

Più in dettaglio, AIIP evidenzia che l'art. 38 comma 4 dello Schema di decreto che prevede una espressa eccezione quanto all'applicazione delle sanzioni ivi previste, limitatamente alle sole pubbliche amministrazioni (e non anche a categorie "più deboli" quali le PMI).

Tanto più che l'articolo 38 al comma 5 prevede la responsabilità personale delle persone fisiche che agiscano quali legali rappresentanti di persone giuridiche, creando quindi una responsabilità diretta per gli amministratori e i legali rappresentanti delle stesse.

Inoltre, al comma sesto prevede che ACN (Autorità competente NIS) possa disporre nei confronti delle persone fisiche che rappresentano un soggetto che non adempia nei termini stabiliti dalla diffida l'applicazione della sanzione amministrativa accessoria della sospensione

dai propri uffici e dalle proprie funzioni dirigenziali svolte rispetto ad un soggetto essenziale importante.

Tuttavia, non risulta che l'estensione in queste modalità di tale responsabilità e l'applicazione di tali misure accessorie siano previste dalla Direttiva; pertanto, le disposizioni dell'art. 38, commi 4 e 5 in questione, eccederebbero quanto previsto dalla direttiva stessa e sono discriminatorie, sproporzionate ed in violazione degli artt. 3 (nonché 24 e 97) della Costituzione.

Così, ad esempio, la sanzione accessoria prevista dall'art. 38, comma 7, per le persone fisiche che rappresentano soggetti privati corrisponde ad una misura interdittiva dei pubblici uffici che non si ravvisa nei confronti dei dipendenti pubblici che esercitano poteri analoghi, mentre nei confronti di questi ultimi è previsto esclusivamente che "*la violazione degli obblighi di cui al presente decreto può costituire causa di responsabilità disciplinare e amministrativo contabile* ".

Infine, chiaramente discriminatorio è anche:

- l'ammontare delle sanzioni amministrative pecuniarie previste per soggetti privati e per le pubbliche amministrazioni dal comma 9 dell'articolo 38
- la circostanza che è previsto un minimo edittale solo per le sanzioni alla pubblica amministrazione mentre per i privati per le violazioni di cui al comma 8, il comma 9 dell'articolo 38 prevede, alle lettere "a" e "b", soltanto le sanzioni massime e non anche il minimo edittale; parimenti il comma 11, lettere "a" e "b", per le violazioni di cui al comma 10 dispone solo la sanzione massima e non anche la minima. Poiché tali sanzioni, soltanto per i privati (diversamente dalla pubblica amministrazione), non prevedono un minimo, non sono oblabili dai privati mentre lo sarebbero da parte della Pubblica Amministrazione (anche in questo caso, la discriminazione è palese).

Peraltro, l'articolo 38, al comma 10, prevede una serie di sanzioni amministrative per specifiche violazioni che non hanno neppure riscontro nel testo della Direttiva NIS2.

Infine, è anche discriminatorio il comma 14 dell'articolo 38 dello Schema, che prevede una diversa disciplina per la reiterazione a favore della pubblica amministrazione rispetto ai privati.

******

Si acconsente alla pubblicazione sul sito internet della Camera del presente documento.

Rimanendo a disposizione per ogni chiarimento, si porgono distinti saluti.

Dott. Giuliano Claudio Peritore
Vice Presidente
Associazione Italiana Internet Provider

Dott. Roberto Loro
Vice Presidente
Associazione Italiana Internet Provider