ASSOTELECOMUNICAZIONI
ASSTEL

ADERENTE A **CONFINDUSTRIA**

Contributo Asstel
in merito al Disegno di legge
“Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici”

8 aprile 2024

Sommario

Premessa e considerazioni generali

Asstel è l'Associazione aderente a Confindustria che rappresenta la filiera delle telecomunicazioni.

E' costituita dalle imprese delle diverse aree merceologiche che appartengono a tale filiera, tra cui le imprese che gestiscono reti di telecomunicazioni fisse e radio-mobili e servizi digitali accessori, i produttori ed i fornitori di terminali-utente, i produttori ed i fornitori di infrastrutture di rete, di apparati e di servizi software per le telecomunicazioni, i gestori di servizi e di infrastrutture di rete, anche esternalizzati, i gestori di servizi di Customer Relationship Management e di Business Process Outsourcing.

Asstel ha la missione di favorire e promuovere lo sviluppo e la crescita della Filiera, nell'interesse generale del sistema economico-produttivo nazionale, curando la tutela degli interessi delle Imprese associate presso le sedi istituzionali, politiche ed economiche, pubbliche e private e la rappresentanza in materia sindacale e del lavoro delle imprese associate che applicano il CCNL TLC e/o l'Accordo Outbound.

Le aziende associate ad Asstel hanno sempre dato massima importanza a garantire la sicurezza di reti e servizi di comunicazione elettronica, secondo quanto disposto dalle norme e seguendo l'evoluzione stessa della disciplina di cybersicurezza a livello nazionale e comunitario, e la collaborazione con le Autorità competenti.

Le disposizioni normative in ambito cybersicurezza, che si stanno susseguendo nel corso degli ultimi anni, stanno delineando un quadro complesso e in rapida evoluzione in relazione al quale le aziende associate ad Asstel confermano la propria disponibilità a cooperare per contribuire alla messa in opera di un sistema che consegua le finalità di resilienza cibernetica nella maniera più efficace ed efficiente.

A tal proposito, si segnala l'esigenza di disporre di orientamenti che consentano agli attori del mercato di organizzarsi e strutturarsi in modo da garantire l'ottemperanza ai provvedimenti in un quadro complesso e dinamico. In altri termini, le imprese del settore ritengono importante orientarsi verso un approccio di semplificazione ed armonizzazione delle disposizioni normative che consenta, a tutti gli attori lungo la filiera, di perseguire in maniera efficace gli obiettivi di sicurezza nazionale senza incorrere in oneri eccessivi.

Il disegno di legge "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" interviene sul quadro normativo in vigore modificando e introducendo obblighi per i soggetti considerati strategici dal punto di vista della sicurezza nazionale. Al fine di garantire la massima chiarezza delle nuove disposizioni e la piena efficacia dei nuovi adempimenti, si ritiene importante sottoporre all'attenzione delle Istituzioni alcuni punti che, attualmente, rappresentano delle criticità per i soggetti coinvolti dallo specifico disegno di legge.

Ad integrazione delle considerazioni puntuali delle sezioni successive, si ritiene importante sottolineare che le disposizioni nazionali in materia di cybersecurity sono sempre caratterizzate da una criticità legata all'equità di applicazione delle stesse tra soggetti nazionali e internazionali, che offrono servizi agli utenti sul territorio nazionale. In particolare, in questo senso, si vuole sollevare la questione della parificazione delle norme a cui sono soggetti i diversi *player* di mercato. Le stesse disposizioni di cybersicurezza che si applicano ai soggetti nazionali devono essere applicate anche a quelli

internazionali. Tale principio di equità è essenziale per creare un ambiente competitivo e regolamentare che favorisca una sana concorrenza e protegga gli utenti.

Articolo 1

Articolo 1 – Obblighi di notifica degli incidenti

L'Articolo 1 del Capo I del disegno di legge "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" estende l'obbligo di notifica di incidenti previsto dal DL 21 settembre 2019, n. 105 (Perimetro di Sicurezza Nazionale Cibernetica, PSNC) alle pubbliche amministrazioni centrali, alle regione e alle province autonome di Trento e di Bolzano, ai comuni con popolazione superiore a 100.000 abitanti e ai comuni capoluoghi di regione nonché alle società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti e alle aziende sanitarie locali. Tali soggetti sono tenuti a notificare gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di propria pertinenza in accordo alla tassonomia già adottata dai soggetti rientranti nel PSNC per segnalare incidenti che si verificano sui beni diversi dai Beni ICT.

In relazione all'estensione dell'obbligo di notifica degli incidenti anche a soggetti al di fuori del PSNC, si ritiene importante evidenziare che tale disposizione potrebbe avere delle implicazioni e oneri indiretti sui fornitori di servizi di telecomunicazioni. Infatti, questi ultimi potrebbero essere coinvolti negli incidenti di sicurezza con impatti su reti, sistemi informativi e servizi informatici e potrebbero dover operare per conto dei nuovi soggetti specificati nell'Articolo 1. A questo proposito, si ritiene importante chiarire che la responsabilità di notifica e gli oneri di gestione degli incidenti di sicurezza che occorrono su reti, sistemi informativi e servizi informatici dei nuovi soggetti rientrano nell'area di competenza di questi ultimi, in modo da garantire che eventuali interventi da parte dei fornitori di servizi di telecomunicazioni possano essere previsti soltanto in accordo condizioni contrattuali specifiche che regolamentino la tipologia di intervento e il relativo compenso economico.

In aggiunta, nell'introduzione di tale obbligo, si ritiene importante prevedere un periodo transitorio, di 6 o 12 mesi, che consenta ai soggetti impattati di dotarsi delle opportune risorse e strutture e di mettere in atto i processi interni ed esterni con la gradualità adeguata alla portata della trasformazione. In particolare, si segnala la necessità di tenere in considerazione la disponibilità limitata di professionalità formate in materia di cybersicurezza, sia nell'organico dei soggetti tenuti ad ottemperare alle nuove disposizioni che dal mercato, con conseguenze sulla rapidità di avviamento delle incombenze e della qualità dei risultati ottenibili, anche attraverso la riorganizzazione dei rapporti con i fornitori di mercato.

Articolo 2

Articolo 2 – Mancato o ritardato adeguamento a segnalazioni dell'Agenzia per la cybersicurezza nazionale

L'Articolo 2 del Capo I del disegno di legge "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" prevede che i soggetti rientranti nel PSNC, nella direttiva NIS e nel Codice delle Comunicazioni Elettroniche, in caso di segnalazioni puntuali dell'Agenzia per la cybersicurezza nazionale circa specifiche vulnerabilità cui essi risultino potenzialmente esposti, provvedano, senza ritardo e comunque non oltre quindi giorni dalla comunicazione, all'adozione degli interventi risolutivi indicati dalla stessa Agenzia.

In relazione all'obbligo di adeguamento a segnalazioni di vulnerabilità da parte di ACN, si ritiene importante evidenziare che i soggetti della filiera delle telecomunicazioni sono consapevoli dell'importanza di attuare tempestivamente azioni di mitigazione e sono disponibili a collaborare ed attenersi agli interventi risolutivi previsti da ACN. Tuttavia, in tale scenario è importante considerare che gli interventi risolutivi devono essere attentamente programmati, per minimizzare gli impatti sui servizi, e devono essere coordinati con tutte le logiche e i meccanismi che garantiscono il funzionamento operativo delle infrastrutture di rete. In altri termini, si ritiene che vi siano dei tempi tecnici, per l'attuazione degli interventi di risoluzione, dai quali non si può prescindere e che, in alcuni casi, potrebbero rendere difficile il rispetto delle tempistiche previste, ovvero dei 15 giorni stabiliti. Si precisa che in molti casi la risoluzione della vulnerabilità dipende dalla disponibilità di una misura correttiva da parte del manifatturiero di un prodotto (e comunque da terze parti della supply chain coinvolta nell'intervento di manutenzione correttiva) ed è quindi vincolato alle tempistiche di messa a disposizione per il dispiegamento e comunque, i processi di dispiegamento su infrastrutture distribuite, con un numero rilevante di componenti impattate e di contesti di inserimento differenziati può richiedere programmi e tempistiche di dispiegamento delle misure risolutive difficilmente riconducibili al termine ultimativo massimo di 15 giorni, fermo restando l'interesse e l'impegno dei soggetti esposti ad attuare tempestivamente ogni misura atta a mitigare e contenere eventuali impatti derivanti dallo sfruttamento della vulnerabilità.

A questo proposito e al fine di evitare un eccessivo ricorso all'eccezione prevista dal comma 2 dell'Articolo 2 ("salvo motivate esigenze di natura tecnico-organizzativa") si propone di rivedere la formulazione attuale con la seguente revisione "I soggetti [...] in caso di segnalazioni puntuali dell'Agenzia per la cybersicurezza nazionale circa specifiche vulnerabilità cui essi risultino potenzialmente esposti, provvedono, senza ritardo e comunque non oltre quindici giorni dalla comunicazione, **a definire il piano di implementazione** degli interventi risolutivi indicati dalla stessa Agenzia".

In aggiunta, si ritiene importante specificare che ci si aspetta che ACN segnali, come vulnerabilità soggette all'obbligo di risoluzione specificato nell'Articolo 2, solo quelle associate ad un rischio critico (es. vulnerabilità relative ad asset con una certa esposizione verso l'esterno o vulnerabilità che, se sfruttate da attaccanti malevoli, possono avere impatti significativi) per limitare gli impatti e gli oneri associati.

Articolo 3

Articolo 3 – Norme di raccordo con le disposizioni del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133

L'Articolo 3 del Capo I del disegno di legge "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" apporta delle modifiche alla legge in materia di Perimetro di Sicurezza Nazionale Cibernetica, introducendo un obbligo di segnalazione di incidenti entro il termine massimo di ventiquattro ore, che va ad aggiungersi all'obbligo di notifica entro settantadue ore. Tale obbligo si applica a tutti gli incidenti con impatto sui beni che non rientrano nell'elenco dei Beni ICT.

In relazione al nuovo obbligo di segnalazione degli incidenti, si ritiene importante evidenziare che si comprende e si condivide l'introduzione di tale disposizione sia da un punto di vista della trasparenza in materia di sicurezza nazionale sia da un punto di vista dell'armonizzazione con le nuove norme di cybersicurezza (direttiva NIS 2). Fermo restando la condivisione di tale modifica, si ritiene doveroso far emergere che, per i soggetti nella filiera delle telecomunicazioni, tale nuova disposizione rappresenta comunque un onere aggiuntivo, pertanto, ci si aspetta che le informazioni richieste in sede di

segnalazione siano minimali in modo da contenere gli impatti sui soggetti che devono attenersi a tale obbligo. Gli elementi di dettaglio sono comunque forniti nel successivo processo di notifica.

Sempre nell'ambito del nuovo obbligo di segnalazione di incidenti, si ritiene importante chiarire che tale obbligo si applica agli stessi incidenti attualmente soggetti a segnalazione entro settantadue ore, ovvero si ritiene importante specificare che gli incidenti che dovranno essere segnalati sono quelli definiti dalla tassonomia già utilizzata in ambito PSNC per gli incidenti con impatti sui beni che non rientrano nell'elenco dei Beni ICT.

Articolo 7

Articolo 7 – Funzioni dell'Agenzia per la cybersicurezza nazionale in materia di intelligenza artificiale

L'Articolo 7 del Capo I del disegno di legge "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" ampia le funzioni dell'Agenzia per la cybersicurezza nazionale anche a tematiche di intelligenza artificiale, considerate una risorsa per il rafforzamento della cybersicurezza nazionale.

In relazione a tale estensione delle competenze di ACN, si segnala che si ritiene naturale e doveroso che emergano disposizioni regolatorie in materia di intelligenza artificiale volte a considerare le implicazioni in ambito di cybersicurezza. In questo contesto, si rileva come un aspetto positivo la confluenza delle stesse su ACN, in quanto ente di coordinamento delle diverse disposizioni in materia di cybersicurezza. Tale approccio potrebbe consentire la semplificazione di processi e procedure puntando ad una armonizzazione di eventuali nuove disposizioni in ambito cybersicurezza, riferite al settore dell'intelligenza artificiale.

Articolo 10

Articolo 10 – Disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e disposizioni di raccordo con il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133

L'Articolo 10 del Capo I del disegno di legge "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" prevede che nelle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici, devono essere tenuti in considerazione gli elementi essenziali di cybersicurezza, che saranno individuati con apposito DPCM da redigersi entro 120 giorni dalla data di entrata in vigore del DDL. Tali elementi essenziali di cybersicurezza sono definiti come l'insieme di criteri e regole tecniche che garantiscono la confidenzialità, l'integrità e la disponibilità dei dati da trattare.

In relazione al nuovo obbligo di valutazione della cybersicurezza nelle attività di approvvigionamento, si ritiene importante evidenziare che si condividono le logiche di tutela degli interessi nazionali alla base della definizione dello stesso e, proprio a questo proposito, si ritiene importante definire chiaramente l'ambito di applicazione di tale obbligo circoscrivendolo ai soli elementi considerati strategici per la sicurezza nazionale, per evitare che ricadano sui soggetti della filiera delle telecomunicazioni oneri aggiuntivi non necessari.

In aggiunta, si ritiene importante che i criteri, ovvero gli elementi essenziali di cybersicurezza, siano definiti in maniera oggettiva e proporzionata, in ossequio ai principi di imparzialità. A titolo esemplificativo si riportano alcuni criteri di natura organizzativa e tecnica che potrebbero essere utilizzati come riferimento:

- Criteri organizzativi: presenza di un'organizzazione interna all'azienda che si occupi di Cybersecurity in linea con le disposizioni ACN e AIPSA, possesso di certificazione del sistema di gestione Cybersecurity e Privacy su base standard ISO 27001 e ISO 277101, adozione di un processo di vulnerability management definito sulla base di standard internazionali, adozione di un processo di security by design nella catena di produzione, esecuzione periodica di audit interni ed esercitazioni come da standard, etc.
- Criteri tecnici: sviluppo di risk assessment, possesso di certificazioni di conformità dei prodotti sulla base di standard internazionali ed europei (es. CC, EUCC), assenza di incidenti significativi negli ultimi anni, etc.

Articoli 11 e 12

Articolo 11 – Modifiche al codice penale e al codice di procedura penale

Gli Articoli 11 e 12 del Capo II del disegno di legge "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" prevedono un inasprimento delle pene per i crimini informatici e introducono nuove fattispecie degli stessi che contemplano, in particolare, attacchi che causano inaccessibilità ad asset o dati.

In relazione all'inasprimento delle pene, si sottolinea la condivisione e l'apprezzamento di quanto previsto dal disegno di legge, interpretando tale misura come un segnale di attenzione alla rilevanza della cybersicurezza e di impegno verso la protezione dei sistemi informatici. In questo contesto, per garantire massima efficacia e chiarezza, ovvero per evitare situazioni di ambiguità e assicurare una corretta applicazione delle pene, si ritiene fondamentale specificare in maniera dettagliata le fattispecie che si configurano come reato e distinguerle dalle pratiche correnti di difesa che si basano sulla simulazione di attacchi per testare la tenuta delle proprie difese o di test, ovvero attività di vulnerability assessment e penetration testing.

Articolo 18

Articolo 18 – Disposizioni finanziarie

L'Articolo 18 del Capo II del disegno di legge "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" specifica che dall'attuazione della legge non derivano nuovi o maggiori oneri ed aggiunge che l'adempimento dei compiti è garantito attraverso le risorse umane, strumentati e finanziarie disponibili a legislazione vigente.

In relazione alla clausola di invarianza, si osserva che, seppur sia estremamente condivisa l'importanza di attuare misure volte a rafforzare la sicurezza informatica, le nuove disposizioni hanno degli impatti a livello di risorse umane, strumentali e finanziarie che non possono essere trascurati. In questo senso, l'invarianza menzionata nella legge non sembra essere proporzionata rispetto agli investimenti che saranno necessari per l'adeguamento, quindi per sostenere gli oneri previsti dalla legge.

Al fine di consentire ai soggetti coinvolti di affrontare efficacemente le ultime sfide della cybersicurezza e di rispettare i nuovi obblighi normativi, si suggerisce di istituire all'interno del PNRR un piano strategico

di investimenti per potenziare la cybersicurezza, in modo che i soggetti possano accedere a fondi e risorse significative per la protezione dei sistemi informatici. Tale proposta potrebbe fare leva anche sull'attuale divario di spesa per la cybersicurezza tra il contesto nazionale e altri Stati comparabili.