PROPOSTA

Ai sensi dell'articolo 116, paragrafo 6, della legge sulle comunicazioni elettroniche (UL RS nn. 130/22 e 18/23 - ZDU-1O), l'Agenzia per le reti e i servizi di comunicazione della Repubblica di Slovenia, tenendo conto della procedura di informazione ai sensi della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che istituisce una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (GU L 241 del 17.9.2015, pag. 1), emana quanto segue

ATTO GENERALE
relativo a requisiti e restrizioni di sicurezza aggiuntivi

Articolo 1
(Contenuto dell'atto generale)

Il presente atto generale fornisce:

1. gli orientamenti che gli operatori delle reti di comunicazione mobile (di seguito denominati "operatori") devono seguire per fornire tali reti a soggetti critici che sono gestori di infrastrutture critiche in altri settori della regolamentazione delle infrastrutture critiche, come specificato nella legge che disciplina il settore dell'infrastruttura critica (di seguito "gestori dell'infrastruttura critica"), fornitori di servizi essenziali secondo quanto stabilito dalla legge che disciplina la sicurezza delle informazioni (di seguito "fornitori di servizi essenziali"), organismi amministrativi statali quali stabiliti dalla legge che disciplina la sicurezza dell'informazione (di seguito "organismi amministrativi statali") o vettori di parti chiave del sistema di sicurezza del Paese; e
2. elementi critici della rete e sistemi informativi associati con le loro funzionalità di cui all'articolo 116, paragrafo 6, della legge sulle comunicazioni elettroniche (UL RS n. 130/22 e 18/23 - ZDU-1O; di seguito denominata "legge"), come indicato nell'allegato, che costituisce parte integrante del presente atto generale ed è redatto in collaborazione con l'organismo responsabile della sicurezza delle informazioni.

Articolo 2
(Significato dei termini)

(1) I termini utilizzati in questo atto generale hanno i significati seguenti.

1. Una catena di fornitura è l'intero sistema di processi, persone, organizzazione e distribuzione coinvolti nella progettazione, produzione, stoccaggio, distribuzione e fornitura, nonché nell'installazione e nella manutenzione di componenti di elementi di rete critici installati nella rete dell'operatore o presso il fornitore di servizi cloud che fornisce tali servizi all'operatore.

2. Gli elementi critici della rete sono gli elementi di rete, le funzioni, i servizi e i sistemi informativi di supporto in forma fisica, software o virtualizzata presso l'operatore o il fornitore di servizi cloud, elencati nell'allegato del presente atto generale.

3. I soggetti critici sono i gestori dell'infrastruttura critica in altri settori della regolamentazione delle infrastrutture critiche determinati in conformità alla legge che disciplina il settore delle infrastrutture critiche, i fornitori di servizi essenziali determinati dalla legge che disciplina la sicurezza delle informazioni, gli organismi amministrativi statali determinati dalla legge che disciplina la sicurezza delle informazioni e i vettori di parti chiave del sistema di sicurezza del Paese.

(2) Gli altri termini utilizzati nel presente atto generale hanno lo stesso significato definito dalla legge e dalla legge generale sulla sicurezza delle reti, dei servizi e dei dati.

Articolo 3
(Orientamenti generali)

(1) Gli operatori della catena di fornitura di componenti di elementi di rete critici e di servizi di supporto di terzo livello per tali componenti devono tenere conto almeno delle seguenti linee guida durante l'intero ciclo di vita di tali componenti:

1. per un singolo fabbricante o fornitore e per un fornitore di servizi di supporto di terzo livello a causa di relazioni e accordi con essi, devono effettuare una valutazione dei rischi in termini di fornitura e di potenziali impatti da parte di terze persone fisiche o giuridiche di diritto pubblico o privato (di seguito denominate "terze parti"), di compatibilità con apparecchiature di altri produttori, di qualità e sicurezza del prodotto e di potenziali impatti negativi sul funzionamento dei servizi e dei soggetti critici dell'operatore;
2. che la sicurezza sia integrata e implementata già nella progettazione e che i contratti prevedano scadenze per l'eliminazione delle vulnerabilità percepite;
3. che le principali caratteristiche di sicurezza (disponibilità, riservatezza, integrità e autenticità) siano garantite durante l'intero ciclo di vita del loro utilizzo;
4. che la sicurezza e la loro fornitura ininterrotta siano garantite e che sia confermato il supporto di caratteristiche di sicurezza elevate in conformità agli standard riconosciuti a livello internazionale (3GPP) e agli standard tecnici europei (ETSI);
5. che gli orientamenti di cui ai punti da 2 a 4 del presente paragrafo siano verificabili nella documentazione contrattuale con il fabbricante o con il fornitore;
6. per ciascun fabbricante o fornitore, siano valutati e presi in considerazione anche i rischi associati ai diritti d'uso delle tecnologie chiave, necessarie per la fabbricazione e l'uso dell'apparecchiatura, e i rischi connessi alla fornitura di apparecchiature, parti di ricambio o servizi di assistenza di terzo livello;
7. che i componenti utilizzati non presentino vulnerabilità critiche note non risolte o attivamente sfruttate;
8. evitare un singolo fabbricante o fornitore, laddove ciò sia tecnicamente fattibile ed economicamente sostenibile, con l'obiettivo di ridurre la dipendenza e aumentare la resilienza in caso di vulnerabilità di componenti critici, guasti catastrofici della rete o minacce alla sicurezza delle reti e dei servizi di soggetti critici da parte di terze persone fisiche o giuridiche di diritto pubblico o privato.

(2) Nel fornire apparecchiature, sistemi e servizi di informazione e comunicazione, gli operatori rispettano pienamente gli orientamenti dell'Agenzia dell'Unione europea per la cibersicurezza (di seguito "ENISA") e i regolamenti validi dell'Unione europea relativi ai requisiti di sicurezza di base per l'approvvigionamento di prodotti e servizi TIC sicuri. L'Agenzia pubblicherà sul proprio sito web i link ai documenti ENISA e ai regolamenti dell'UE vigenti nell'area summenzionata e li terrà aggiornati.

(3) Nel fornire componenti di elementi di rete critici o nell'utilizzo di servizi cloud, è data priorità alla scelta di componenti tra i fabbricanti o i fornitori o servizi di fornitori di servizi cloud certificati da organismi di valutazione della conformità accreditati e, se necessario, autorizzati a norma dell'articolo 60, paragrafo 3, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza delle tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (di seguito "regolamento") per il rilascio di certificati europei di cibersicurezza a un certo livello di affidabilità, come stabilito dall'articolo 52 del regolamento.

(4) Ai fini del paragrafo precedente, l'operatore controlla un sito web speciale, istituito dall'ENISA in conformità dell'articolo 55 del regolamento, destinato a informare il pubblico sui regimi europei di certificazione della cibersicurezza, sui certificati europei di cibersicurezza e sulle dichiarazioni di conformità dell'UE, comprese le informazioni relative ai regimi europei di certificazione della cibersicurezza non più validi o revocati e ai certificati europei di cibersicurezza e alle dichiarazioni di conformità dell'UE scaduti, nonché un archivio di link a informazioni sulla cibersicurezza.

Articolo 4
(Valutazione del rischio)

(1) Nel determinare il rischio del fabbricante o del fornitore di componenti e del fornitore di servizi di terzo livello per gli elementi critici della rete, l'operatore tiene conto dei seguenti aspetti di rischio che valuta.

(2) Nella valutazione di cui al paragrafo precedente, il gestore valuta e tiene conto almeno di quanto segue:

1. qualità complessiva (compresi gli aspetti di sicurezza) e affidabilità;
2. livello di utilizzo di standard e interfacce aperti che impediscono la dipendenza e il lock-in nei confronti dei prodotti di un particolare fabbricante o fornitore;
3. conformità alle norme tecniche internazionali ed europee riconosciute (3GPP, ETSI) e alle normative dell'Unione europea e alle impostazioni di sicurezza predefinite in conformità con le raccomandazioni professionali (associazione GSMA);
4. livello di compatibilità con apparecchiature e funzioni di rete di terze parti;
5. capacità di fornire aggiornamenti e personalizzazioni;
6. processo di gestione delle vulnerabilità, loro divulgazione e processo aggiornato con aggiornamenti e correzioni;
7. disponibilità e trasparenza della documentazione riguardante:
   - funzioni chiave, informazioni sulla sicurezza e altre caratteristiche del componente e possibili impostazioni, e
   - software utilizzato, compreso il codice open source (Bill Of Materials – SBOM);
8. livello di dipendenza da servizi di supporto di terzo livello nella gestione e manutenzione delle apparecchiature, se l'operatore non svolge questi servizi autonomamente con i propri dipendenti;
9. valutazione preliminare della conformità delle apparecchiature o di un soggetto che fornirebbe un servizio di supporto di terzo livello da parte di organismi accreditati nell'Unione europea secondo i sistemi europei di certificazione della cibersicurezza,

in base ai quali gli organismi accreditati sono pubblicati nella Gazzetta ufficiale dell'Unione europea.

(3) L'operatore documenta i fattori di rischio e i risultati della valutazione del rischio per ciascun fabbricante o fornitore o fornitore di servizi di terzo livello selezionato di cui ai paragrafi 2 e 3 del presente articolo e lo aggiorna regolarmente.

Articolo 5
(Orientamenti generali sul funzionamento degli elementi critici della rete)

(1) I componenti degli elementi critici della rete, il loro funzionamento e le impostazioni predefinite non devono contenere caratteristiche tecniche che potrebbero influire negativamente sulla sicurezza o sul funzionamento di soggetti critici, tra l'altro a causa di sabotaggio, spionaggio, furto di proprietà intellettuale o terrorismo.

(2) Gli elementi critici della rete sono generalmente situati nella Repubblica di Slovenia o, tenendo conto di tutti i rischi per la sicurezza e garantendo un elevato livello di misure di sicurezza, e se ciò non è specificato altrimenti dalla normativa applicabile, nell'Unione europea. L'operatore deve informare l'Agenzia per le reti e i servizi di comunicazione della Repubblica di Slovenia (di seguito "l'Agenzia") e l'organismo responsabile della sicurezza delle informazioni in merito al trasferimento previsto almeno 30 giorni prima del trasferimento al di fuori dell'Unione europea.

(3) I servizi di supporto di terzo livello per gli elementi critici della rete sono generalmente prestati nella Repubblica di Slovenia o, tenendo conto di tutti i rischi per la sicurezza e garantendo un elevato livello di misure di sicurezza, e se ciò non è specificato altrimenti dalla normativa applicabile, nell'Unione europea. L'operatore notifica all'Agenzia e all'organismo responsabile della sicurezza delle informazioni il trasferimento previsto dei propri servizi di supporto di terzo livello almeno 30 giorni prima del trasferimento al di fuori dei Paesi dell'Unione europea.

(4) L'attuazione di servizi di supporto di terzo livello non compromette la sicurezza o il funzionamento dei servizi dei soggetti critici o della sicurezza nazionale.

(5) L'operatore stabilisce e attua regolarmente il processo di identificazione degli elementi critici di rete. Tale processo deve essere eseguito almeno una volta all'anno o quando vengono acquistati componenti di elementi critici della rete.

(6) Se un singolo componente rappresenta solo parzialmente un elemento critico della rete, è considerato parte di un elemento critico della rete.

(7) L'operatore tiene un elenco aggiornato di tutti i componenti degli elementi critici della rete, delle loro funzioni, delle loro ubicazioni, dei loro amministratori e responsabili, dei loro fornitori di servizi di supporto di terzo livello e dei loro fabbricanti o fornitori. Su richiesta, l'elenco è messo a disposizione all'Agenzia e a un organismo responsabile della sicurezza dell'informazione.

Articolo 6
(Misure di sicurezza per la fornitura di componenti di elementi critici della rete)

(1) L'operatore è a conoscenza dell'intera catena di approvvigionamento e dei rischi a essa associati, compresi i subappaltatori di singoli componenti di elementi critici della rete, che comprendono anche chiavi di crittografia, UICC/eUICC e altri elementi di sicurezza, il cui uso improprio potrebbe compromettere la sicurezza dei soggetti critici.

(2) L'operatore garantisce che i requisiti di sicurezza tra l'operatore e i fabbricanti o i fornitori di componenti di elementi critici della rete o i suoi fornitori di servizi di supporto di terzo livello siano concordati e documentati contrattualmente e richiedano ai fabbricanti o ai fornitori di rispettare le misure di sicurezza concordate lungo l'intera catena di fornitura.

(3) Al fine di prevenire lo sfruttamento delle vulnerabilità da parte di soggetti malintenzionati in modo tempestivo, l'operatore garantisce che il produttore o il fornitore di componenti di un elemento critico della rete si impegni contrattualmente a informare immediatamente l'operatore della vulnerabilità rilevata e delle misure per ridurre i rischi e a consigliare le misure protettive o correttive che l'operatore può adottare in risposta alla minaccia.

(4) L'operatore verifica, almeno una volta all'anno, l'adeguatezza dei diritti di accesso sugli elementi critici della rete o li aggiorna senza indugio in conformità delle modifiche apportate all'organizzazione o ai fornitori di servizi di supporto di terzo livello.

(5) L'operatore impedisce la dipendenza da un singolo fornitore o da un fornitore di servizi di terzo livello (ossia il "vendor lock-in"), laddove ciò sia tecnicamente fattibile ed economicamente sostenibile, con l'obiettivo di ridurre la dipendenza e aumentare la resilienza in caso di vulnerabilità dei componenti critici, anche evitando contratti a lungo termine con singoli fabbricanti o fornitori o fornitori di servizi di supporto di terzo livello, o avendo la possibilità di cambiarli con l'obiettivo di ridurre al minimo livello possibile le interruzioni nella fornitura di servizi ai soggetti critici.

Articolo 7
(Condizioni contrattuali con fabbricanti, fornitori o fornitori di servizi di supporto di terzo livello)

Al fine di garantire un elevato livello di sicurezza, l'operatore deve includere almeno quanto segue nei nuovi termini contrattuali con produttori, fornitori o fornitori di servizi di supporto di terzo livello:

1. una dichiarazione del fabbricante o del fornitore attestante che il componente o le sue impostazioni predefinite non hanno backdoor non documentate o alcun impatto negativo sul funzionamento dei soggetti critici;
2. un impegno del fabbricante, del fornitore o del fornitore di servizi di terzo livello a proteggere i dati di cui vengono a conoscenza durante la fornitura di servizi o l'accesso ad essi in relazione alla fornitura del servizio di accesso;
3. un impegno del fabbricante o del fornitore o del fornitore di servizi di terzo livello a informare immediatamente l'operatore in caso di violazioni della protezione dei dati di comunicazione o dei dati sul traffico che interessano o potrebbero incidere

sull'operatore o sui soggetti critici di cui all'articolo 1, punto 1, del presente atto generale;

4. un impegno del fabbricante o del fornitore o del fornitore di servizi di terzo livello a notificare immediatamente all'operatore eventuali incidenti di sicurezza e vulnerabilità che potrebbero incidere sulla sicurezza della rete, dei servizi associati o dei dati dell'operatore;
5. un impegno del fabbricante, del fornitore o del fornitore di servizi di terzo livello a rispettare le norme e gli standard di sicurezza stabiliti dall'operatore e ad adottare misure di sicurezza adeguate per garantire la sicurezza dei sistemi e delle reti informatiche e dei dati dell'operatore o del soggetto critico;
6. la possibilità per l'operatore di esaminare in qualsiasi momento gli ambienti, le procedure, le misure di sicurezza e gli strumenti utilizzati dal fornitore di servizi di supporto di terzo livello per accedere alla rete e ai dati dell'operatore;
7. la responsabilità del fabbricante o del fornitore o del fornitore di servizi di supporto di terzo livello per i danni che sarebbero causati da vulnerabilità identificate o uso improprio di componenti di elementi critici di rete, dalla loro impostazione predefinita o durante la fornitura di servizi di supporto di terzo livello che il fabbricante, il fornitore o il fornitore di assistenza di terzo livello hanno trascurato o deliberatamente attuato;
8. l'obbligo di formare regolarmente il personale del produttore o del fornitore o del fornitore di servizi di supporto di terzo livello nel campo della sicurezza dei dati e dei sistemi e delle reti informatiche.

Articolo 8
(Norme relative all'accesso e all'uso degli elementi critici della rete)

(1) Quando accede fisicamente o logicamente ai componenti degli elementi critici della rete, alle loro impostazioni e ai dati dell'operatore in essi memorizzati, elaborati o modificati, l'operatore deve garantire che:

1. l'accesso sia strettamente limitato alle persone precedentemente autorizzate;
2. tutti gli interventi sugli elementi critici della rete effettuati in loco o tramite accesso remoto siano controllati dall'operatore;
3. sia effettuata l'autenticazione a più fattori per gli utenti ai quali sono assegnati i più alti privilegi di diritti per accedere ai singoli componenti degli elementi critici della rete, alle loro impostazioni o ai dati in essi memorizzati o elaborati;
4. ogni persona autorizzata a cui è concesso l'accesso disponga di un account utente e di una password unici;
5. siano utilizzate solo password che vengono modificate regolarmente o immediatamente in caso di abuso rilevato e che contengono almeno 15 caratteri e includono lettere maiuscole e minuscole, numeri e caratteri speciali, se il software lo consente;
6. il concetto di tolleranza zero o di fiducia sia implementato nell'accesso, ove possibile;
7. la sicurezza della connessione di comunicazione tra l'utente autorizzato e i singoli componenti sia protetta dall'uso della crittografia, tenendo conto degli ultimi sviluppi tecnologici e delle migliori buone pratiche industriali nel campo della sicurezza dell'informazione, o raccomandata da istituzioni consolidate nel settore della sicurezza dell'informazione;
8. venga effettuata una registrazione indelebile degli accessi e dei tentativi di accesso, che viene conservata per almeno 6 mesi, compresa una copia di backup, ma può anche essere per un periodo più lungo, quando l'analisi della gestione del rischio e la

valutazione del livello accettabile di rischio mostrano che i rischi dovrebbero essere adeguatamente gestiti mantenendo i registri per un periodo più lungo;

9. la registrazione e il monitoraggio di tutti gli interventi software sui componenti siano eseguiti ove possibile, comprese le modifiche alla configurazione. Le registrazioni, compresa una copia di backup di tali dati, sono conservate per tutto il tempo indicato al punto precedente;
10. l'accesso ai singoli componenti e ai dati memorizzati o elaborati su di essi sia limitato nel tempo e aperto solo per la durata del lavoro necessario.

(2) In caso di accesso a singoli componenti di elementi critici della rete da parte del personale o dei dipendenti di un fornitore di servizi di supporto di terzo livello:

1. utilizzano esclusivamente una postazione di lavoro intermedia dedicata e sicura ("jump server"), sottoposta a regolari controlli di sicurezza;
2. installano su una postazione dedicata solo gli strumenti, i componenti e i servizi attivi assolutamente necessari per accedere ad altre risorse della rete che sono assolutamente indispensabili e devono essere aggiornati con le ultime patch di sicurezza;
3. utilizzano operazioni e chiavi crittografiche sicure su una stazione di lavoro dedicata, che deve trovarsi nella rete dell'operatore ed essere sotto il suo esclusivo controllo;
4. ogni accesso è approvato e attivato dall'operatore manualmente e solo per la durata dell'accesso;
5. tutti gli accessi e le attività sono fisicamente controllati e registrati dall'operatore;
6. utilizzano l'autenticazione a due fattori e password di almeno 15 caratteri, con lettere maiuscole e minuscole, numeri e caratteri speciali, da modificare in base alla valutazione dei rischi.

(3) Prima di trasferire il servizio di gestione, manutenzione o aggiornamento degli elementi critici della rete o dei loro singoli componenti a terzi, l'operatore verifica e garantisce di disporre almeno degli stessi o migliori meccanismi di sicurezza e processi di gestione della sicurezza rispetto ai suoi meccanismi e processi. Egli informa immediatamente dell'intenzione di trasferimento il soggetto critico interessato, l'Agenzia e l'organismo responsabile della sicurezza delle informazioni.

(4) L'operatore verifica lo stato effettivo dei processi di sicurezza prima dell'inizio della fornitura del servizio e successivamente almeno una volta all'anno. L'operatore tiene i registri delle revisioni e dei controlli interni sulla fornitura di servizi di supporto di terzi e li conserva per tutta la durata della fornitura dei servizi e per un anno dopo la loro cessazione, ma non più di cinque anni.

DISPOSIZIONE TRANSITORIA E FINALE

Articolo 9
(Disposizioni transitorie)

(1) L'operatore notifica all'Agenzia e all'organismo responsabile della sicurezza delle informazioni le ubicazioni esistenti degli elementi critici di rete entro 30 giorni dall'entrata in vigore del presente atto generale.

(2) L'operatore notifica all'Agenzia e all'organismo responsabile della sicurezza delle informazioni le sedi esistenti dei servizi di supporto di terzo livello per gli elementi critici della rete entro 30 giorni dall'entrata in vigore del presente atto generale.

(3) L'Agenzia pubblica per la prima volta i documenti di cui all'articolo 3, paragrafo 2, del presente atto generale a decorrere dalla data della sua entrata in vigore.

Articolo 10
(Entrata in vigore)

Il presente atto generale entra in vigore il trentesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale della Repubblica di Slovenia, e gli operatori possono utilizzare le apparecchiature e mantenere la fornitura di servizi di supporto di terzo livello fino alla scadenza dei termini specificati nell'articolo 312, paragrafi 2 e 3, della legge.

N. _____ mag. Marko Mišmaš

Lubiana, il _____ direttore

EVA 2023-3150-0034

PROPOSTA

Allegato

Elenco degli elementi critici della rete e dei sistemi informativi associati:

Elementi critici della rete	**Funzionalità della rete e dei sistemi informativi**
Gestione degli abbonati e meccanismi di crittografia	- Gestione delle sessioni (voce e dati), - autenticazione degli utenti e delle apparecchiature con la rete, - gestione e conservazione delle chiavi per l'autorizzazione di abbonati e componenti di rete (UICC/eUICC, certificati digitali/HSM), - funzioni per l'autenticazione sicura, la protezione dell'integrità della comunicazione (crittografia) e la memorizzazione delle chiavi utente, componenti di rete e di gestione, - gestione dei diritti di accesso.
Interconnessione	- Hosting di funzionalità e interfacce ad altre reti e servizi.
Servizi di rete gestiti	- Registrazione e autorizzazione dei servizi di rete, - archiviazione ed elaborazione dei dati di comunicazione, localizzazione e traffico, - esposizione della rete e delle funzioni di rete ad applicazioni e servizi esterni.
Gestione e orchestrazione di funzioni di rete virtualizzate (NFV) e orchestrazione di rete (MANO), compresa l'infrastruttura di virtualizzazione	- Funzioni di gestione dell'orchestrazione e della configurazione di NFV indipendentemente dal tipo di implementazione (VM, container, microservizi), - funzioni di virtualizzazione per l'implementazione e l'uso di NFV, - funzione di selezione della porzione di rete ("Network Slice Selection Function", NSSF).
Rete di accesso radio	- Stazioni base che supportano la tecnologia 5G o superiore.
Sistemi di gestione e altri sistemi di supporto	- Monitoraggio del funzionamento e della gestione della rete di comunicazione mobile, compresa la parte di accesso (RAN/O-RAN), - sistemi per il rilevamento di eventi di sicurezza, anomalie, minacce e loro gestione (funzioni di sicurezza comprese SIEM/SOAR).
Intercettazione giuridica	- Funzioni di accesso al contenuto di comunicazione e dati sul traffico degli utenti da parte dell'autorità competente.