PROPUNERE

În temeiul articolului 116 alineatul (6) din Legea privind comunicațiile electronice (UL RS nr. 130/22 și 18/23 – ZDU-1O), Agenția pentru Rețele și Servicii de Comunicare a Republicii Slovenia, ținând seama de procedura de informare în conformitate cu Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului din 9 septembrie 2015 referitoare la procedura de furnizare de informații în domeniul reglementărilor tehnice și al normelor privind serviciile societății informaționale (JO L 241, 17.9.2015, p. 1), emite următoarele:

LEGEA GENERALĂ
privind cerințele și restricțiile de securitate suplimentare

Articolul 1
(Conținutul legii generale)

Prezenta lege general prevede:

1. orientări care trebuie urmate de operatorii de rețele de comunicații mobile (denumiți în continuare „operatori”) care furnizează aceste rețele entităților critice care sunt administratori de infrastructură critică în alte domenii de reglementare a infrastructurilor critice, astfel cum se specifică în legislația care reglementează domeniul infrastructurii critice (denumiți în continuare „administratori de infrastructură critică”), de furnizorii de servicii esențiale, astfel cum sunt stabiliți de legea care reglementează securitatea informațiilor (denumiți în continuare „furnizori de servicii esențiale”), organismelor administrației de stat, astfel cum sunt stabilite prin legea care reglementează securitatea informațiilor (denumite în continuare „organisme ale administrației de stat”) sau transportatorilor de părți esențiale ale sistemului de securitate al țării; și
2. elemente critice ale rețelei și ale sistemelor informatice asociate cu funcționalitățile lor menționate la articolul 116 alineatul (6) din Legea privind comunicațiile electronice (UL RS nr. 130/22 și 18/23 – ZDU-1O; denumită în continuare „legea”), astfel cum figurează în anexă, care face parte integrantă din prezenta lege generală și este elaborată în cooperare cu organismul responsabil cu securitatea informațiilor.

Articolul 2
(Semnificația termenilor)

(1) Termenii utilizați în prezenta lege generală înseamnă:

1. Un lanț de aprovizionare este întregul sistem de procese, persoane, organizare și distribuție implicate în proiectarea, producția, stocarea, distribuția și furnizarea, precum și instalarea și întreținerea componentelor elementelor critice de rețea instalate în rețeaua operatorului sau la furnizorul de servicii cloud care furnizează astfel de servicii operatorului.

2. Elementele critice ale rețelei sunt acele elemente de rețea, funcții, servicii și sisteme informatice de suport sub formă fizică, software sau virtualizată la operator sau la furnizorul de servicii cloud, astfel cum sunt enumerate în anexa la prezenta lege generală.

3. Entitățile critice sunt administratori de infrastructură critică în alte domenii de reglementare a infrastructurii critice stabilite în conformitate cu legea care reglementează domeniul infrastructurii critice, furnizorii de servicii esențiale în conformitate cu legea care reglementează securitatea informațiilor, organismele administrației de stat, astfel cum sunt stabilite de legea care reglementează securitatea informațiilor și transportatorii unor părți cheie ale sistemului de securitate al țării.

(2) Alți termeni utilizați în prezenta lege generală au același înțeles ca cel definit de lege și de Legea generală privind securitatea rețelelor, serviciilor și datelor.

Articolul 3
(Orientări generale)

(1) Operatorii din lanțul de aprovizionare al componentelor elementelor critice de rețea și al serviciilor de asistență de nivelul al treilea pentru aceste componente iau în considerare cel puțin următoarele orientări pe parcursul întregului ciclu de viață al acestor componente:

1. pentru un producător sau furnizor individual și pentru un furnizor de servicii de asistență de nivelul al treilea ca urmare a relațiilor și a acordurilor cu aceștia, efectuează o evaluare a riscurilor în ceea ce privește aprovizionarea și impactul potențial al persoanelor fizice sau juridice terțe în temeiul dreptului public sau privat (denumite în continuare „părți terțe”), compatibilitatea cu echipamentele altor producători, calitatea și siguranța produselor și potențialele efecte negative asupra funcționării serviciilor operatorului și a entităților critice;
2. că securitatea este încorporată și implementată deja în faza de proiectare și că contractele includ termene pentru eliminarea vulnerabilităților percepute;
3. că principalele elemente de securitate (disponibilitatea, confidențialitatea, integritatea și autenticitatea) sunt asigurate pe parcursul întregului ciclu de viață al utilizării lor;
4. că securitatea și furnizarea neîntreruptă a acestora sunt garantate și se confirmă faptul că aceasta susține elemente de securitate ridicate, în conformitate cu standardele recunoscute la nivel internațional (3GPP) și cu standardele tehnice europene (ETSI);
5. că orientările menționate la punctele 2-4 de la prezentul alineat pot fi verificate în documentația contractuală cu producătorul sau cu furnizorul;
6. pentru fiecare producător sau furnizor, riscurile asociate drepturilor de utilizare a tehnologiilor-cheie, care sunt necesare pentru fabricarea și utilizarea echipamentelor, precum și riscurile legate de furnizarea de echipamente, piese de schimb sau servicii de asistență de nivelul al treilea sunt, de asemenea, evaluate și luate în considerare;
7. că componentele utilizate nu au vulnerabilități critice cunoscute sau exploatate activ nerezolvate;
8. evitarea unui singur producător sau furnizor, în cazul în care acest lucru este fezabil din punct de vedere tehnic și durabil din punct de vedere economic, cu scopul de a reduce dependența și de a spori reziliența în cazul unor vulnerabilități ale componentelor critice, al unei defecțiuni catastrofale a rețelei sau al unei amenințări la adresa securității rețelelor și serviciilor entităților critice de către entități fizice sau juridice terțe de drept public sau privat.

(2) Atunci când furnizează echipamente, sisteme și servicii de informații și comunicații, operatorii respectă pe deplin orientările Agenției Uniunii Europene pentru Securitate Cibernetică (denumită în continuare „ENISA”) și reglementările valabile ale Uniunii Europene privind cerințele de securitate de bază atunci când achiziționează produse și servicii TIC sigure. Agenția publică pe site-ul său internet linkuri către documentele actuale ale ENISA și către reglementările UE din domeniul menționat anterior și le actualizează.

(3) În cadrul furnizării de componente ale elementelor critice de rețea sau se utilizează servicii de cloud, se acordă prioritate alegerii componentelor de la acei producători sau furnizori sau servicii de la furnizorii de servicii de cloud care au fost certificați de organisme de evaluare a conformității care au fost acreditate și, dacă este necesar, autorizate în temeiul articolului 60 alineatul (3) din Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (denumit în continuare „regulamentul”) pentru eliberarea certificatelor europene de securitate cibernetică la un anumit nivel de asigurare, astfel cum se stabilește la articolul 52 din regulament.

(4) În sensul alineatului anterior, operatorul verifică un site web special, instituit de ENISA în conformitate cu articolul 55 din regulament, destinat să informeze publicul cu privire la sistemele europene de certificare a securității cibernetice, la certificatele europene de securitate cibernetică și la declarațiile UE de conformitate, inclusiv informații referitoare la sistemele europene de certificare a securității cibernetice care nu mai sunt valabile sau revocate și expirate și cu privire la certificatele europene de securitate cibernetică și declarațiile UE de conformitate, precum și un registru de linkuri către informațiile privind securitatea cibernetică.

Articolul 4
(Evaluarea riscurilor)

(1) Atunci când determină riscul pe care îl prezintă producătorul sau furnizorul de componente și furnizorul de servicii de nivelul al treilea pentru elementele critice ale rețelei, operatorul ia în considerare următoarele aspecte de risc, pe care le evaluează.

(2) În evaluarea menționată la alineatul precedent, operatorul evaluează și ia în considerare cel puțin:

1. calitatea generală (inclusiv aspectele legate de siguranță) și fiabilitatea;
2. nivelul de utilizare a standardelor deschise și a interfețelor care împiedică dependența și blocarea produselor unui anumit producător sau furnizor;
3. respectarea standardelor tehnice internaționale și europene recunoscute (3GPP, ETSI) și a reglementărilor Uniunii Europene și a setărilor de securitate implicite în conformitate cu recomandările profesionale (Asociația GSMA);
4. nivelul de compatibilitate cu echipamentele terțe și cu funcțiile de rețea;
5. capacitatea de a oferi actualizări și personalizări;
6. procesul de gestionare a vulnerabilității, dezvăluirea acestora și procesul actualizat cu actualizări și remedieri;
7. disponibilitatea și transparența documentației privind:
   - funcțiile cheie și informațiile despre securitate și alte caracteristici ale componentei și posibile setări; și

- software-ul utilizat, inclusiv codul sursă deschisă (listă a materialelor software – SBOM);

8. nivelul de dependență de serviciile de asistență de nivelul al treilea în gestionarea și întreținerea echipamentelor, în cazul în care operatorul nu efectuează aceste servicii singur cu angajații săi;
9. evaluarea preliminară a conformității echipamentelor sau a unei entități care ar furniza un serviciu de asistență de nivelul al treilea de către organisme acreditate în Uniunea Europeană în conformitate cu sistemele europene de certificare de securitate cibernetică, prin care organismele acreditate sunt publicate în Jurnalul Oficial al Uniunii Europene.

(3) Operatorul documentează factorii de risc și rezultatele evaluării riscurilor pentru fiecare producător sau furnizor selectat sau furnizor de servicii de nivelul al treilea menționat la alineatele (2) și (3) din prezentul articol și le actualizează periodic.

Articolul 5
(Orientări generale privind exploatarea elementelor critice ale rețelei)

(1) Componentele elementelor critice ale rețelei, funcționarea acestora și setările implicite nu trebuie să conțină caracteristici tehnice care ar putea afecta negativ securitatea sau funcționarea entităților critice, printre altele din cauza sabotajului, a spionajului, a furtului de proprietate intelectuală sau a terorismului.

(2) Elementele critice ale rețelei sunt, în general, situate în Republica Slovenia sau, ținând seama de toate riscurile de securitate și asigurând un nivel ridicat de măsuri de securitate și dacă acest lucru nu este specificat altfel de reglementările aplicabile, în Uniunea Europeană. Operatorul informează Agenția pentru Rețele și Servicii de Comunicare din Republica Slovenia (denumită în continuare „agenția”) și organismul responsabil cu securitatea informațiilor cu privire la transferul preconizat al acestora cu cel puțin 30 de zile înainte de transferul în afara Uniunii Europene.

(3) Serviciile de asistență de nivelul al treilea pentru elementele critice ale rețelei sunt, în general, prestate în Republica Slovenia sau, ținând seama de toate riscurile de securitate și asigurând un nivel ridicat de măsuri de securitate și dacă acest lucru nu este specificat altfel de reglementările aplicabile, în Uniunea Europeană. Operatorul informează agenția și organismul responsabil cu securitatea informațiilor cu privire la transferul preconizat al serviciilor lor de asistență de nivelul al treilea cu cel puțin 30 de zile înainte de transferul în afara țărilor Uniunii Europene.

(4) Punerea în aplicare a serviciilor de asistență de la nivelul al treilea nu trebuie să pericliteze securitatea sau funcționarea serviciilor entităților critice sau securitatea națională.

(5) Operatorul stabilește și pune în aplicare în mod regulat procesul de identificare a elementelor critice ale rețelei. Acest lucru trebuie efectuat cel puțin o dată pe an sau atunci când sunt achiziționate componente ale elementelor critice ale rețelei.

(6) În cazul în care o componentă individuală reprezintă doar parțial un element critic al rețelei, aceasta este considerată ca făcând parte dintr-un element critic al rețelei.

(7) Operatorul menține o listă actualizată a tuturor componentelor elementelor critice ale rețelei, a funcțiilor, a locațiilor, a administratorilor și a operatorilor acestora, a furnizorilor lor de servicii de asistență de nivelul al treilea și a producătorilor sau furnizorilor acestora. La cerere, lista se pune la dispoziția agenției și a unui organism responsabil cu securitatea informațiilor.

Articolul 6
(Măsuri de securitate pentru furnizarea componentelor elementelor critice ale rețelei)

(1) Operatorul trebuie să cunoască întregul lanț de aprovizionare și riscurile asociate acestuia, inclusiv subcontractanții componentelor individuale ale elementelor critice ale rețelei care includ, de asemenea, chei de criptare, UICC/eUICC și alte elemente de securitate, a căror utilizare abuzivă ar putea pune în pericol securitatea entităților critice.

(2) Operatorul se asigură că cerințele de securitate dintre operator și producătorii sau furnizorii de componente ale elementelor critice ale rețelei sau furnizorii de servicii de asistență de nivelul al treilea sunt convenite și documentate prin contract și solicită producătorilor sau furnizorilor să respecte măsurile de securitate convenite de-a lungul întregului lanț de aprovizionare.

(3) Pentru a preveni exploatarea vulnerabilităților de către actorii răuvoitori în timp util, operatorul se asigură că producătorul sau furnizorul de componente ale unui element critic al rețelei se angajează contractual să informeze imediat operatorul cu privire la vulnerabilitatea detectată și la măsurile de reducere a riscurilor și oferă consiliere cu privire la măsurile de protecție sau de remediere pe care operatorul le poate lua ca răspuns la amenințare.

(4) Operatorul verifică, cel puțin o dată pe an, caracterul adecvat al drepturilor de acces la elementele critice ale rețelei sau le actualizează fără întârziere în conformitate cu schimbările intervenite în organizație sau în rândul furnizorilor de servicii de asistență de nivelul al treilea.

(5) Operatorul trebuie să prevină dependența sa de un furnizor individual sau de un furnizor de servicii de nivelul al treilea (și anume, „dependență de furnizor”), în cazul în care acest lucru este fezabil din punct de vedere tehnic și durabil din punct de vedere economic, cu scopul de a reduce dependența și de a spori reziliența în cazul vulnerabilităților componentelor critice, inclusiv prin evitarea contractelor pe termen lung cu producători, furnizori sau furnizori de servicii de asistență de nivelul al treilea sau prin posibilitatea de a le modifica cu scopul de a reduce perturbările în furnizarea de servicii către entitățile critice la cel mai scăzut nivel posibil.

Articolul 7
(Termeni contractuali cu producătorii, furnizorii sau furnizorii de servicii de asistență de nivelul al treilea)

Pentru a asigura un nivel ridicat de securitate, operatorul include cel puțin următoarele elemente în noile condiții contractuale cu producătorii, furnizorii sau furnizorii de servicii de asistență de nivelul al treilea:

1. o declarație a producătorului sau a furnizorului conform căreia componenta sau setările implicite ale acesteia nu au tehnologii de tip „uși secrete” nedocumentate sau niciun impact negativ asupra funcționării entităților critice;
2. un angajament al producătorului, al furnizorului sau al furnizorului de servicii de nivelul al treilea de a proteja datele cu care se familiarizează în timpul prestării de servicii sau al accesului la acestea în legătură cu furnizarea serviciului de acces;
3. angajamentul producătorului, al furnizorului sau al furnizorului de servicii de a informa imediat operatorul în cazul încălcării protecției datelor privind comunicațiile sau a datelor de transfer care afectează sau ar putea afecta operatorul sau entitățile critice menționate la articolul 1 punctul 1 din prezenta lege generală;
4. un angajament al producătorului, al furnizorului sau al furnizorului de servicii de nivelul al treilea de a notifica imediat operatorului orice incident de securitate și vulnerabilități care ar putea afecta securitatea rețelei, a serviciilor asociate sau a datelor operatorului;
5. un angajament al producătorului, al furnizorului sau al furnizorului de servicii de nivelul al treilea de a respecta standardele și normele de securitate stabilite de operator și de a lua măsurile de securitate adecvate pentru a asigura securitatea sistemelor informatice și a rețelelor, precum și datele operatorului sau ale entității critice;
6. capacitatea operatorului de a revizui în orice moment mediile, procedurile, măsurile de securitate și instrumentele utilizate de furnizorul de servicii de asistență de nivelul al treilea atunci când accesează rețeaua și datele operatorului;
7. responsabilitatea producătorului, a furnizorului sau a furnizorului de servicii de asistență de nivelul al treilea pentru daunele care ar fi cauzate de vulnerabilități identificate sau de utilizarea necorespunzătoare a componentelor elementelor critice ale rețelei, de setarea implicită a acestora sau în timpul furnizării de servicii de asistență de nivelul al treilea pe care producătorul, furnizorul sau furnizorul de sprijin de nivelul al treilea le-a neglijat sau le-a pus în aplicare în mod deliberat;
8. obligația de a instrui în mod regulat personalul producătorului sau al furnizorului sau al prestatorului de servicii de asistență de nivelul al treilea în domeniul securității datelor și al sistemelor și rețelelor informatice.

Articolul 8
(Norme privind accesul și utilizarea elementelor critice ale rețelei)

(1) Atunci când accesează fizic sau logic componentele elementelor critice ale rețelei, setările acestora și datele operatorului stocate, prelucrate sau modificate în acestea, operatorul se asigură că:

1. accesul este strict limitat la persoanele care au fost autorizate anterior;
2. toate lucrările asupra elementelor critice ale rețelei efectuate la fața locului sau prin acces de la distanță sunt controlate de operator;
3. autentificarea cu mai mulți factori se efectuează pentru utilizatorii cărora le sunt atribuite cele mai mari privilegii de drepturi pentru accesarea componentelor individuale ale elementelor critice ale rețelei, a setărilor acestora sau a datelor stocate sau prelucrate în acestea;
4. fiecare persoană autorizată căreia i se acordă accesul are un cont de utilizator unic și o parolă unică;
5. se utilizează numai parolele care sunt modificate în mod regulat sau imediat în cazul unei utilizări necorespunzătoare detectate și care conțin cel puțin 15 caractere și

includ litere majuscule și minuscule, numere și caractere speciale, în cazul în care software-ul permite acest lucru;
6. conceptul de toleranță zero sau încredere este pus în aplicare în ceea ce privește accesul, acolo unde este posibil;
7. securitatea conexiunii de comunicare de la utilizatorul autorizat la componentele individuale este protejată prin utilizarea criptării, ținând seama de cele mai recente evoluții tehnologice și de cele mai bune practici industriale în domeniul securității informațiilor sau recomandate de instituțiile înființate în domeniul securității informațiilor;
8. se efectuează o înregistrare indelebilă a accesului și a încercărilor de acces, care este păstrată timp de cel puțin șase luni, inclusiv o copie de rezervă, dar poate fi, de asemenea, pentru o perioadă mai lungă, atunci când analiza gestionării riscurilor și evaluarea nivelului acceptabil de riscuri arată că riscurile ar trebui gestionate în mod adecvat prin păstrarea evidențelor pentru o perioadă mai lungă;
9. înregistrarea și monitorizarea tuturor intervențiilor software asupra componentelor se efectuează acolo unde este posibil, inclusiv modificările de configurare. Înregistrările, inclusiv o copie de rezervă a acestor date, se păstrează atât timp cât se indică la punctul anterior;
10. accesul la componentele individuale și la datele stocate sau prelucrate pe acestea este limitat în timp și deschis numai pe durata activității necesare.

(2) În cazul accesului la componente individuale ale elementelor critice ale rețelei de către personalul sau angajații unui furnizor de servicii de asistență de nivelul al treilea, aceștia:
1. utilizează numai o stație de lucru intermediară dedicată securizată („server de salt”), care face obiectul unor controale de securitate periodice;
2. instalează pe o stație de lucru dedicată numai instrumentele, componentele și serviciile active absolut necesare pentru a accesa alte resurse din rețea care sunt absolut necesare și trebuie actualizate cu cele mai recente corecții de securitate;
3. utilizează operațiuni criptografice și chei securizate pe o stație de lucru dedicată, care trebuie să fie localizată în rețeaua operatorului și care se află sub controlul său unic;
4. fiecare acces este aprobat și activat manual de către operator și numai pe durata accesului;
5. toate accesările și activitățile sunt controlate fizic și înregistrate de operator;
6. utilizați autentificarea cu doi factori și parolele care au cel puțin 15 caractere și includ litere majuscule și minuscule, numere și caractere speciale, care se modifică pe baza riscurilor evaluate.

(3) Înainte de a transfera unui terț serviciul de gestionare, întreținere sau actualizare a elementelor critice ale rețelei sau a componentelor individuale ale acestora, operatorul verifică și se asigură că dispune de cel puțin aceleași mecanisme de securitate și procese de gestionare a securității sau de procese mai bune în comparație cu mecanismele și procesele sale. Acesta informează imediat entitatea critică în cauză, agenția și organismul responsabil cu securitatea informațiilor cu privire la intenția de a transfera.

(4) Operatorul verifică starea reală a proceselor de securitate înainte de începerea furnizării serviciilor și, ulterior, cel puțin o dată pe an. Operatorul ține evidența revizuirilor și controalelor interne privind furnizarea de servicii de asistență furnizate de terți și le păstrează pe durata prestării serviciilor și timp de un an de la încetarea acestora, dar nu mai mult de cinci ani.

PROPUNERE

DISPOZIȚIE TRANZITORIE ȘI FINALĂ

Articolul 9
(Dispoziții tranzitorii)

(1) Operatorul notifică agenției și organismului responsabil cu securitatea informațiilor amplasamentele existente ale elementelor critice ale rețelei în termen de 30 de zile de la intrarea în vigoare a prezentei legi generale.

(2) În termen de 30 de zile de la intrarea în vigoare a prezentei legi generale, operatorul informează agenția și organismul responsabil cu securitatea informațiilor cu privire la amplasamentele existente ale serviciilor de asistență de nivel al treilea pentru elementele critice ale rețelei.

(3) Agenția publică pentru prima dată documentele menționate la articolul 3 alineatul (2) din prezenta lege generală de la data intrării sale în vigoare.

Articolul 10
(Intrare în vigoare)

Prezenta lege generală intră în vigoare în a 30-a zi de la data publicării în Monitorul Oficial al Republicii Slovenia, prin care operatorii pot utiliza echipamentele și pot menține furnizarea de servicii de asistență de nivelul al treilea până la expirarea termenelor specificate la articolul 312 alineatele (2) și (3) din lege.

Nr. _____ mag. Marko Mišmaš

Ljubljana, la _____ director

EVA 2023-3150-0034

PROPUNERE

Anexă

Lista elementelor critice ale rețelei și a sistemelor informatice asociate:

Elemente critice ale rețelei	**Funcționalitățile rețelei și ale sistemelor informatice**
Gestionarea abonaților și mecanisme de criptare	- Gestionarea sesiunilor (voce și date), - autentificarea utilizatorilor și a echipamentelor cu rețeaua; - gestionarea și stocarea cheilor pentru autorizarea abonaților și a componentelor rețelei (UICC/eUICC, certificate digitale/HSM); - funcții de autentificare securizată, de protecție a integrității comunicațiilor (criptare) și de stocare a cheilor de utilizator, a componentelor de rețea și de gestionare; - gestionarea drepturilor de acces.
Interconectare	- Găzduirea caracteristicilor și interfețelor cu alte rețele și servicii.
Servicii de rețea gestionate	- Înregistrarea și autorizarea serviciilor de rețea; - stocarea și prelucrarea datelor privind comunicațiile, localizarea și traficul; - expunerea rețelei și a funcțiilor de rețea la aplicații și servicii externe.
Gestionarea și orchestrarea funcțiilor de rețea virtualizată (NFV) și orchestrarea rețelei (MANO), inclusiv infrastructura de virtualizare	- Funcțiile de gestionare a orchestrației și configurației NFV, indiferent de tipul de implementare (VM, container, microservicii); - funcțiile de virtualizare pentru implementarea și utilizarea NFV; - Funcția de selecție în rețea (NSSF);
Rețea de acces radio	- Stații de bază care acceptă tehnologia 5G sau superioară.
Sisteme de management și alte sisteme de asistență	- Monitorizarea funcționării și gestionării rețelei de comunicații mobile, inclusiv a părții de acces (RAN/O-RAN); - sisteme de detectare a evenimentelor de securitate, anomalii, amenințări și gestionarea acestora (funcții de securitate, inclusiv SIEM/SOAR).
Interceptare legală	- Funcțiile de acces la conținutul comunicațiilor și la datele privind traficul utilizatorilor de către autoritatea competentă.