Anexa nr. 1

DOMENIILE

vizate de măsurile de securitate

<u>Domeniul I. Politica de securitate şi managementul riscului</u>

Obiective de securitate

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1. să stabilească o politică de securitate adecvată;

2. să stabilească un management al riscului care:
   a) să stabilească domeniul de aplicare, precum şi criteriile de bază necesare procesului de management al riscului (criteriul de evaluare a riscului, criteriul de stabilire a impactului, criteriul de acceptare a riscului);
   b) să identifice riscurile, prin identificarea resurselor, amenințărilor, vulnerabilităților, măsurilor existente şi a consecințelor pe care incidentele de securitate le-ar putea avea asupra resurselor și să se asigure că personalul de conducere este informat în mod corespunzător despre aceste riscuri, dar și despre măsurile de reducere a lor; în cazul rețelelor definite la art. 2 lit. f) din Legea nr. 163/2021 privind adoptarea unor măsuri referitoare la infrastructuri informatice și de comunicații de interes național și condițiile implementării rețelelor 5G, se vor avea în vedere, totodată, potențiale riscuri cauzate de expunerea la terțe părți considerate a prezenta un grad de risc ridicat ori dependența de un singur producător;
   c) să analizeze riscurile prin estimarea impactului pe care îl poate avea concretizarea unei amenințări care exploatează o vulnerabilitate a unei resurse şi prin estimarea probabilității de apariție a incidentelor;
   d) să evalueze riscul;
   e) să evalueze opțiunile de tratare a riscului, să selecteze măsuri pentru tratarea riscului cu fixarea obiectivelor acestor măsuri şi să justifice riscurile acceptate care nu îndeplinesc criteriul de acceptare a riscului;
   f) să se asigure că riscurile reziduale sunt acceptate de personalul de conducere;

3. să stabilească o structură adecvată a rolurilor şi responsabilităţilor în asigurarea securităţii reţelelor şi serviciilor, să informeze personalul despre rolurile și responsabilitățile în asigurarea securităţii reţelelor şi serviciilor, precum și despre cazurile și modalitățile în care se pot contacta persoanele responsabile;

4. să stabilească o politică cu privire la cerinţele de securitate atât pentru achiziţionarea de produse şi servicii identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate (echipamente, servicii IT, software, interconectare, baze de date, facilităţi asociate etc.), cât şi pentru asigurarea întreţinerii sau gestiunii de către terţe părţi a acestor produse şi servicii;

5. să includă cerințe de securitate în contractele pentru achiziţionarea de la terţe părţi de produse şi servicii identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate şi pentru asigurarea întreţinerii sau gestiunii de către terţe părţi a acestor produse şi servicii, inclusiv în ceea ce privește confidențialitatea și transferul securizat al informației, să țină evidența incidentelor de securitate cauzate de terțe părți, să ia măsuri pentru a reduce riscurile reziduale care nu au fost adresate de terțele părți sau sunt rezultate din interacțiunea cu acestea;

6. în ceea ce privește rețelele definite la art. 2 lit. f) din Legea nr. 163/2021, să includă în politica privind cerinţele de securitate pentru achiziţionarea de la terţe părţi de produse şi servicii identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate şi pentru asigurarea întreţinerii sau gestiunii de către terţe părţi a acestor produse şi servicii cel puțin următoarele elemente:

a) referitor la echipamentele identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate, obligația achiziționării unor echipamente puse la dispoziție de terțele părți, precum și a proceselor și serviciilor acestora [procese TIC, servicii TIC, produse TIC, echipamente din componența rețelelor definite la art. 2 lit. f) din Legea nr. 163/2021, servicii cloud etc.] certificate în conformitate cu sistemele europene de certificare aplicabile, în cazul în care astfel de sisteme de certificare prevăzute de 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 (Regulamentul privind securitatea cibernetică) sunt obligatorii în temeiul dreptului național sau european;
b) obligația de a depune diligențele necesare pentru a se asigura că terții respectă standardele relevante în proiectarea și fabricarea echipamentelor, precum și în gestionarea ciclului de viață al acestora;
c) prezentarea documentelor justificative de către terți care să ateste că aceștia au depus diligențele necesare în vederea asigurării nivelului de calitate al proceselor interne de securitate aplicabile, inclusiv asigurarea securității prin proiectare (*security by design*), integrată în procesul de dezvoltare a produsului;
d) furnizarea de către terți a garanțiilor și documentelor justificative care să ateste că aceștia au depus diligențele necesare în ceea ce privește implementarea tuturor funcționalităților de securitate conform standardelor relevante și că în produsele pe care le pun la dispoziție nu există vulnerabilități introduse și/sau omise voit; aceștia vor informa imediat despre vulnerabilități de îndată ce acestea devin cunoscute;
e) obligația de a depune diligențele necesare pentru a se asigura că terții asigură protecția adecvată și nedivulgarea oricăror informații confidențiale despre beneficiarii echipamentelor, serviciilor, lucrărilor sau a altor informații confidențiale către alte entități;
f) obligația de a depune diligențele necesare pentru a se asigura că terții vor oferi asistență în investigarea și remedierea incidentelor de securitate și posibilitatea de a colabora în vederea efectuării unor eventuale teste periodice de securitate și de penetrare ale produselor pe care le pun la dispoziție.

Domeniul II. Securitatea resurselor umane

Obiective de securitate

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1. să stabilească un proces privind verificarea de fond a candidaţilor pentru angajare, a contractorilor şi a terţilor în conformitate cu legile aplicabile, reglementări şi etică, proporţionale cu riscurile percepute, și să efectueze, în baza procesului menționat, controale de verificare de fond a candidaţilor pentru angajare, a contractorilor şi a terţilor;

2. să se asigure că personalul are cunoştinţe suficiente de securitate şi este instruit permanent cu privire la securitatea reţelelor şi serviciilor, inclusiv prin implementarea unor programe de instruire

regulată în domeniul securității rețelelor și serviciilor de comunicații electronice, precum și să pună la dispoziția personalului materiale și documentații suport actualizate;

3. să stabilească un proces corespunzător de gestionare a schimbărilor de personal sau a modificărilor de roluri şi responsabilităţi, care să cuprindă inclusiv aspecte privind revocarea drepturilor de acces, predarea echipamentelor dacă nu mai sunt necesare, precum și instruirea personalului în cazul schimbărilor responsabilităților în cadrul organizației;

4. să stabilească un proces disciplinar pentru angajaţii care produc o încălcare a securităţii reţelelor sau serviciilor de comunicaţii electronice.

Domeniul III. Securitatea reţelelor şi serviciilor, a facilităţilor asociate şi a informaţiilor

Obiective de securitate

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1. să stabilească o securitate fizică și de mediu adecvată a reţelei şi a facilităților asociate, care să includă: stabilirea şi menţinerea unor măsuri de securitate care să protejeze în mod corespunzător împotriva accesului fizic neautorizat, distrugerilor provocate de incendii, inundaţii, cutremure, explozii, tulburări publice şi alte forme de dezastre naturale sau provocate de oameni;

2. în ceea ce privește rețelele definite la art. 2 lit. f) din Legea nr. 163/2021, să stabilească măsuri de securitate suplimentare pentru accesul fizic la rețea și la facilitățile asociate, în conformitate cu importanța obiectivului protejat; măsurile de securitate vor ține cont de riscurile specifice acestor rețele, inclusiv cele generate de accesul părților terțe;

3. să stabilească o securitate adecvată a utilităţilor suport, cum ar fi furnizarea de energie electrică, combustibil sau răcirea echipamentelor, cel puțin prin: implementarea unor măsuri prin care să se asigure securitatea adecvată a utilităţilor suport, dar și a facilităților conexe, proiectarea și dimensionarea acestora astfel încât să fie în acord cu cerințele și specificațiile producătorilor de echipamente;

4. să stabilească măsuri de securitate adecvate pentru accesul logic la reţea şi la sistemele informatice, care să prevadă cel puțin:

a) implementarea unor mecanisme de control al accesului logic pe baza unor identificatori unici;
b) managementul drepturilor de acces, definirea rolurilor, a drepturilor de acces și a responsabilităților, mecanismele de autentificare adecvate tipului de acces solicitat, precum și monitorizarea accesului, procese privind aprobarea excepțiilor și înregistrarea fraudelor;
c) măsuri de securitate privind accesul logic al terților, de la distanță, la resurse, aplicarea principiului „privilegiilor minime”, a principiului „separării sarcinilor”, monitorizarea continuă a accesului, aplicarea autentificării bazate pe tehnologii de ultimă generație.

5. în ceea ce privește rețelele definite la art. 2 lit. f) din Legea nr. 163/2021, se vor implementa măsuri de securitate suplimentare pentru accesul logic care vor ține cont de riscurile specifice ale acestor rețele. Controlul strict al accesului și/sau restricționarea accesului vor fi avute în vedere în cazul terților sau furnizorilor de servicii gestionate (entitățile care furnizează servicii legate de instalarea, gestionarea, funcționarea sau întreținerea produselor, rețelelor, infrastructurii, aplicațiilor TIC sau a oricăror alte rețele și sisteme informatice, prin intermediul asistenței sau al administrării active efectuate fie la sediul clienților, fie la distanță) care sunt considerați de risc ridicat sau care accesează din țări din afara Uniunii Europene rețelele și sistemele informatice;

6. să stabilească măsuri de securitate adecvate, pentru a asigura protecţia reţelelor şi serviciilor de comunicaţii electronice împotriva codurilor cu potenţial dăunător, codurilor mobile neautorizate şi a atacurilor informatice, inclusiv DoS/DDoS, malware;

7. să aplice măsuri de securitate adecvate în cazul managementului actualizărilor, corecțiilor software, dar și în cazul traficului de management și de semnalizare, în vederea prevenirii intervențiilor neautorizate în cadrul rețelei sau componentelor acesteia;

8. să asigure utilizarea adecvată a criptării datelor în timpul stocării sau a transmiterii lor prin rețea pentru a preveni incidentele de securitate și/sau pentru a minimiza impactul acestora asupra utilizatorilor finali sau a altor rețele sau servicii de comunicații electronice;

9. să asigure protecția adecvată a cheilor criptografice și a oricăror altor informații de autentificare pentru a nu fi divulgate sau alterate, iar accesul la cheile private să fie monitorizat și controlat.

Domeniul IV. Managementul operaţiunilor

Obiective de securitate

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1. să stabilească proceduri operaţionale şi responsabilităţi adecvate și să se asigure că toate sistemele necesare furnizării rețelelor și serviciilor de comunicații electronice sunt gestionate conform acestor proceduri operaționale;

2. să stabilească proceduri privind managementul schimbărilor efectuate în reţeaua de comunicaţii electronice, inclusiv schimbările software, și să se asigure că acestea sunt realizate conform procedurilor adoptate;

3. să întocmească și să păstreze cel puțin un an jurnale care să conţină informaţiile relevante referitoare la schimbările de la pct. 2, inclusiv în cazul schimbărilor software (evidența schimbărilor, a corecțiilor, a actualizărilor etc.);

4. să efectueze evaluări prealabile ale impactului potențial al unei schimbări de sistem;

5. să stabilească proceduri de gestionare a resurselor identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate și controlul configurării astfel încât disponibilitatea şi starea acestora să fie verificată, care să includă:

a) identificarea și inventarierea resurselor identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate, inclusiv cele ale unor terțe părți, întocmirea de registre actualizate care să conțină detalii despre tehnologiile și componentele puse în funcțiune, dependența între aceste resurse, precum și identificarea configurărilor sistemelor;

b) stabilirea proprietarilor resurselor identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate, definirea rolurilor, responsabilităților;

c) evaluarea de criticitate a resurselor identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate bazată pe evaluarea de risc.

Domeniul V. Managementul incidentelor

Obiective de securitate

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1. să stabilească procese şi proceduri pentru managementul incidentelor care afectează securitatea reţelelor şi serviciilor de comunicaţii electronice care să vizeze raportarea internă, evaluarea, răspunsul la incidente şi escaladarea acestora, inclusiv prin definirea rolurilor şi responsabilităţilor;

2. să se asigure de pregătirea adecvată, existența și disponibilitatea personalului pentru managementul incidentelor care afectează securitatea reţelelor şi serviciilor de comunicaţii electronice;

3. să stabilească și să implementeze procese și sisteme de detectare a incidentelor de securitate și a evenimentelor care pot conduce la incidente;

4. în ceea ce privește rețelele definite la art. 2 lit. f) din Legea nr. 163/2021, centrele de operațiuni de rețea și/sau centrele de operațiuni de securitate vor funcționa pe teritoriul național și/sau pe teritoriul Uniunii Europene; acestea ar trebui să asigure vizibilitatea și monitorizarea componentelor rețelei respective pentru a detecta evenimente de securitate și pentru a identifica și preveni amenințări;

5. să stabilească o procedură adecvată de raportare a incidentelor către Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM), precum şi către alte autorităţi responsabile şi să stabilească planuri de comunicare a incidentelor către alte părţi externe (furnizori de reţele şi servicii de comunicaţii electronice afectaţi, media, clienţi, parteneri de afaceri etc.);

6. să stabilească procese și proceduri pentru restabilirea prioritară a serviciilor ce contribuie la realizarea comunicațiilor de urgență.

Domeniul VI. Managementul continuităţii afacerii

Obiective de securitate

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1. să stabilească o strategie pentru asigurarea continuităţii furnizării reţelelor şi serviciilor de comunicaţii electronice în situaţiile generate de perturbări grave ale funcţionării reţelei sau serviciului; aceasta va include și măsuri privind asigurarea rezilienței lanțului de aprovizionare cu echipamente și software necesare furnizării rețelelor și serviciilor de comunicații;

2. să deţină capabilităţi de implementare a strategiei de continuitate şi să stabilească planuri de continuitate şi de recuperare;

3. în ceea ce privește rețelele definite la art. 2 lit. f) din Legea nr. 163/2021, planurile de continuitate şi de recuperare să aibă în vedere suplimentar:

- dependența de alte sectoare și servicii critice a căror afectare poate impacta direct sau indirect securitatea rețelelor și serviciilor;

- afectarea altor sectoare și servicii critice dependente de continuitatea furnizării rețelelor și serviciilor de comunicații electronice;

4. să stabilească o strategie pentru asigurarea accesului neîntrerupt la comunicațiile de urgență.

Domeniul VII. Monitorizare, testare şi audit

Obiective de securitate

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1. să stabilească politici de monitorizare a sistemelor, precum şi politici privind jurnalele de sistem care să asigure vizibilitate adecvată, să detecteze anomalii, să identifice și să prevină amenințări, inclusiv în ceea ce privește asigurarea comunicațiilor de urgență;

2. să stabilească politici pentru testarea, inclusiv prin exerciţii, a planurilor de continuitate şi de recuperare în cazul perturbărilor grave ale funcţionării reţelei sau serviciului, având în vedere scenarii realiste care să acopere cât mai multe situații posibile; în urma analizei rezultatelor vor fi luate măsurile corespunzătoare;

3. să stabilească politici pentru testarea echipamentelor, sistemelor, software-lor și corecțiilor software înainte de conectarea/punerea lor în funcţiune/implementarea lor;

4. să stabilească o politică adecvată pentru evaluarea şi testarea securităţii tuturor resurselor (echipamente, sisteme şi software etc.);

5. să stabilească o politică pentru monitorizarea conformităţii şi pentru audit, cu un proces de raportare a conformităţii şi de rezolvare a deficienţelor constatate în timpul auditului; în cazul rețelelor definite la art. 2 lit. f) din Legea nr. 163/2021, politica pentru monitorizarea conformității va cuprinde aplicarea măsurilor de securitate din standardele relevante.

Domeniul VIII. Conștientizarea amenințărilor

Obiective de securitate

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1. să stabilească și să implementeze procese de monitorizare, colectare și analiză continuă a informațiilor despre amenințările relevante la adresa securității rețelelor și serviciilor de comunicații electronice;

2. să ia măsuri adecvate de atenuare și prevenire a amenințărilor relevante la adresa securității rețelelor și serviciilor de comunicații electronice.