DEPARTAMENTUL DE STUDII PARLAMENTARE ŞI POLITICI UE
DIRECŢIA STUDII ŞI DOCUMENTARE LEGISLATIVĂ

LEGISLAȚIA PRIVIND SECURITATEA CIBERNETICĂ DINTR-O SERIE DE STATE MEMBRE ALE UNIUNII EUROPENE

studiu documentar

iunie 2022

Lucrările elaborate în cadrul Direcției studii și documentare legislativă au caracter documentar și nu reprezintă punctul de vedere al Camerei Deputaților.
Documentele legislative oficiale au fost consultate în limba de origine, iar traducerea informațiilor relevante selectate nu reprezintă o traducere oficială, fiind furnizată ca un mijloc de înțelegere a unui document original, scris în altă limbă.
Baza de date cuprinzând totalitatea studiilor elaborate de Direcția studii și documentare legislativă poate fi accesată prin intermediul paginii de Intranet a Camerei Deputaților la adresa:
http://www.cdep.ro/infoparl/dip.studii?par1=2021

Documentare și sinteză: Dan Alexandreanu
Consilier Parlamentar - Direcția studii și documentare legislativă
Palatul Parlamentului, str. Izvor nr.2-4, sect.5, București
Tel: 021.316.03.65; 021.414.13.50/ 51, Interior 1350/1349, camera 5070
E-mail: doc@cdep.ro

ABSTRACT

În decembrie 2020, Comisia Europeană și Serviciul European de Acțiune Externă (SEAE) au prezentat o nouă strategie de securitate cibernetică a UE. Scopul acestei strategii este acela de a consolida rezistența Europei la amenințările cibernetice și de a permite tuturor cetățenilor și întreprinderilor să se bucure și să profite din plin de servicii și de instrumente digitale fiabile. Noua strategie conține propuneri concrete pentru introducerea instrumentelor de reglementare, de investiții și de politică[1].

În martie 2021, Consiliul a adoptat o serie de concluzii privind strategia de securitate cibernetică, subliniind că, aceasta este esențială pentru construirea unei Europe reziliente, ecologice și digitale. Miniștrii UE au identificat autonomia strategică ca un obiectiv-cheie, menținând în același timp o economie deschisă. Ca parte a acestui fapt, capacitatea UE de a lua decizii autonome în domeniul securității cibernetice trebuie consolidată.

UE lucrează, de asemenea, la două propuneri legislative pentru a aborda riscurile actuale și viitoare *online* și *offline*:

- o directivă actualizată pentru îmbunătățirea protecției rețelelor și a sistemelor informatice;
- o nouă directivă privind rezistența organizațiilor critice.

Un Centru european pentru criminalitatea cibernetică a fost înființat în cadrul Europol pentru a sprijini statele membre în investigarea criminalității online și în desființarea rețelelor criminale.

Platforma multidisciplinară europeană împotriva amenințărilor criminale (EMPACT) este o inițiativă de securitate condusă de statele membre pentru a identifica, prioritiza și răspunde amenințărilor reprezentate de criminalitatea internațională organizată. Una dintre prioritățile principale ale acestei inițiative este lupta împotriva atacurilor cibernetice.

În plus, în mai 2019, Consiliul a stabilit un cadru legislativ care permite UE să introducă sancțiuni specifice pentru a descuraja și a răspunde atacurilor cibernetice care reprezintă o amenințare externă pentru UE sau statele membre.

Acest cadru legal permite ca UE să impună sancțiuni persoanelor sau organizațiilor responsabile de atacuri cibernetice și/sau tentative de atacuri cibernetice sau care contribuie în alt mod la acestea, oferind sprijin financiar, tehnic sau material pentru astfel de atacuri. Sancțiunile pot fi impuse și altor persoane și entități asociate acestor persoane și entități.

Ca urmare a măsurilor restrictive, printre altele:

- persoanele respective nu mai pot intra pe teritoriul UE;
- statele membre îngheață activele persoanelor și entităților în cauză.

[1] https://www.consilium.europa.eu/ro/policies/cybersecurity/

CUPRINS

LEGISLAȚIA PRIVIND SECURITATEA CIBERNETICĂ DINTR-O SERIE DE STATE MEMBRE ALE UE

AUSTRIA

Legea federală consolidată privind securitatea rețelelor și a sistemelor informatice(2022)[2] definește măsurile de securitate a rețelelor și a sistemelor operatorilor de servicii esențiale din sectoarele:

- energie;
- trafic;
- sistemul bancar;
- infrastructura pieței financiare;
- sănătate;
- alimentare cu apă potabilă;
- infrastructura digitală,
- precum și pentru furnizorii de servicii digitale și instituțiile administrației publice.

Cancelarul federal are următoarele sarcini strategice:

- coordonarea creării unei strategii și a unui raport anual privind securitatea rețelelor și a sistemelor informaționale;
- reprezentarea Austriei în grupul de cooperare, precum și în alte organisme de la nivel european și internațional pentru securitatea rețelelor și a sistemelor de informații, cărora le sunt atribuite sarcini strategice;
- coordonarea cooperării public-privat în domeniul securității rețelelor și sistemelor informaționale;
- funcționarea *GovCERT*[3] în condițiile prevăzute de lege;
- informarea publicului cu privire la un incident de securitate care afectează mai multe dintre sectoarele menționate;
- identificarea operatorilor de servicii esențiale în conformitate cu prevederile legale, crearea și actualizarea continuă a unei liste de servicii esențiale;
- consultarea cu autoritățile competente din alte state membre atunci când furnizorii de servicii digitale au sediul principal în Austria, dar rețeaua și sistemele lor de informații sunt situate într-un alt stat membru;

[2] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010536

[3] În acest scop, Echipa națională de răspuns în situații de urgență informatică și Echipele sectoriale de răspuns în situații de urgență informatică pentru operatorii de servicii esențiale și furnizorii de servicii digitale, precum și Echipa de răspuns în situații de urgență informatică a administrației publice (GovCERT) sprijină entitățile administrației publice în abordarea riscurilor și incidentelor de securitate.

- determinarea caracterului adecvat și autorizarea echipelor informatice de urgență în conformitate cu prevederile legale;
- publicarea și actualizarea unei liste a echipelor informatice de urgență într-o formă adecvată.

Cancelarul federal, de comun acord cu ministrul federal de interne, poate prevedea, prin ordonanță, următoarele:

- criterii pentru parametrii de funcționare, respectiv intervenții;
- reglementări mai detaliate pentru fiecare sector;
- adoptarea de măsuri de siguranță;
- adoptarea de excepții de la obligații pentru operatorii de servicii esențiale în conformitate prevederile legale.

Cancelarul federal - de comun acord cu ministrul federal de Interne și cu ministrul federal al Apărării Naționale – stabilește, prin ordonanțe, împărțirea atribuțiilor operatorilor din domeniul digital și al protecției datelor.

Ministrul federal de interne are următoarele atribuții operaționale:

- operarea punctului unic de contact (*SPOC*[4]) pentru securitatea rețelei și a sistemelor informatice;
- managementul organizațional al structurilor de coordonare *IKDOK*[5] și *OpKoord*[6];
- primirea și analiazrea rapoartelor privind riscurile și incidentele de securitate, pregătirea periodică a unui raport de situație relevant și transmiterea rapoartelor și a raportului de situație precum și de informații suplimentare relevante către autoritățile sau organismele naționale de profil;
- crearea și diseminarea informațiilor necesare pentru asigurarea securității rețelei și a sistemelor informatice, pentru prevenirea incidentelor de securitate;
- revizuirea măsurilor de securitate și respectarea obligațiilor de raportare;
- verificarea organismelor calificate pentru intervenții;
- informarea publicului cu privire la incidentele individuale de securitate;
- managementul și coordonarea managementului crizelor cibernetice la nivel operațional.

4 SPOC va acționa ca birou operațional de legătură pentru a asigura cooperarea transfrontalieră cu autoritățile competente din celelalte state membre ale Uniunii Europene, precum și între grupul de cooperare și rețeaua de CSIRT-uri.

5 Structura de Coordonare Operativă (IKDOK) este o structură interministerială de coordonare la nivel operațional în domeniul securității rețelelor și sistemelor informaționale formată din reprezentanți ai Cancelarului federal, Ministrului federal de interne, Ministrul federal al apărării și Ministrul federal de externe.

6 Structura de coordonare operativă (OpKoord) este o structură de coordonare la nivel operațional în domeniul securității rețelelor și a sistemelor informatice formată din IKDOK și echipele informatice de urgență.

O infracțiune administrativă se săvârșește de către persoana care:

- nu desemnează un punct de contact, nu anunță orice modificare luată sau nu poate fi contactată în termenul prevăzut de lege pentru intervenție;
- nu furnizează dovezi în conformitate cu prevederile legale;
- refuză inspecția;
- nu pune în aplicare ordinele oficiale în timp util;
- nu respectă obligația de raportare.

Infracțiunea administrativă se sancționează cu amendă de până la 50.000 de euro, iar în cazuri repetate de până la 100.000 de euro, fiind în sarcina autorităților administrative ale landurilor.

Competența locală pentru contravenții administrative se stabilește în funcție de sediul principal al operatorului de servicii esențiale sau al furnizorului de servicii digitale.

Nu este considerată contravenție administrativă o faptă penală de competența instanțelor de drept comun, care este sancționată cu o pedeapsă mai mare în temeiul altor dispoziții penale.

BELGIA

Legea privind cadrul de securitate a rețelelor și a sistemelor de informații de interes general pentru securitatea publică (2019)[7] urmărește transpunerea Directivei Europene (UE) nr. 2016/1148 a Parlamentului European și a Consiliului privind măsurile menite să asigure un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice din Uniunea Europeană.

Legea se aplică operatorilor de servicii esențiale, care au cel puțin o unitate pe teritoriul belgian și care desfășoară efectiv o activitate legată de furnizarea a cel puțin unui serviciu informatic esențial pe teritoriul belgian. De asemenea, legea se aplică și furnizorilor de servicii digitale care nu au un sediu pe teritoriul Uniunii Europene, atunci când prestează în Belgia servicii informatice.

Regele desemnează autoritatea responsabilă, ca autoritate națională de monitorizare și de coordonare a punerii în aplicare a respectivei legi. Autoritatea respectivă reprezintă punctul unic național de contact pentru securitatea rețelelor și a sistemelor informatice, pentru toți operatorii de servicii esențiale și furnizorii de servicii digitale, pentru Belgia.

Regele desemnează autoritatea responsabilă cu asigurarea rolului CSIRT național. Regele poate crea autorități sectoriale, formate din reprezentanți ai statului federal, ai comunităților și ai regiunilor, în conformitate cu procedurile prevăzute de Legea specială privind reformele instituționale. Se stabilește înființarea unui serviciu de inspecție pe sector sau, după caz, pe subsector, responsabil cu monitorizarea respectării prevederilor prezentei legi și actelor sale de punere în aplicare de către operatorii de servicii esențiali sau de către furnizorii

[7] https://etaamb.openjustice.be/fr/loi-du-07-avril-2019_n2019011507.html

de servicii digitale. Regele desemnează, pentru un anumit sector sau, după caz, subsector, serviciul de inspecție competent să efectueze inspecția.

Regele numește, prin decret aprobat de Consiliul de Miniștri, autoritatea responsabilă cu menținerea la zi a strategiei naționale existente în ceea ce privește securitatea rețelelor și a sistemelor informaționale. Strategia se actualizează, după consultarea autorităților de profil și, după caz, a autorităților de supraveghere a datelor cu caracter personal.

Strategia definește obiectivele de reglementare adecvate în vederea atingerii și menținerii unui nivel ridicat de securitate a rețelelor și a sistemelor informatice. Aceasta cuprinde, printre altele, următoarele aspecte:

a) obiectivele și prioritățile strategiei naționale de securitate a rețelelor și a sistemelor informaționale;
b) un cadru de guvernanță care să permită atingerea obiectivelor și priorităților strategiei naționale de securitate a rețelelor și a sistemelor informatice, inclusiv sarcinile și responsabilitățile organismelor publice și ale altor actori implicați;
c) inventarul măsurilor de pregătire, răspuns și redresare, inclusiv cooperarea dintre sectorul public și cel privat;
d) o privire de ansamblu asupra programelor de educație, conștientizare și formare în legătură cu strategia națională de securitate a rețelelor și a sistemelor informaționale;
e) o privire de ansamblu asupra planurilor de cercetare și dezvoltare aferente strategiei naționale de securitate a rețelelor și a sistemelor informatice;
f) un plan de identificare și de evaluare a riscurilor;
g) o listă a diferiților actori implicați în implementarea strategiei naționale de securitate a rețelelor și a sistemelor informaționale.

Sarcinile CSIRT sunt următoarele:

- urmărirea incidentelor la nivel național și internațional, inclusiv prelucrarea datelor cu caracter personal legate de urmărirea acestor incidente;
- activarea mecanismului de avertizare timpurie, diseminarea mesajelor de alertă și anunțuri, precum și diseminarea informațiilor privind riscurile si incidentele existente către părțile interesate;
- răspunsul la incidente;
- analiza dinamică a riscurilor și incidentelor și conștientizarea situației;
- detectarea, observarea și analiza problemelor de securitate informatică;
- promovarea adoptării și utilizării unor practici comune sau standardizate pentru procedurile de gestionare a riscurilor și incidentelor, precum și a sistemelor de clasificare a incidentelor, riscurilor și informațiilor;
- stabilirea de relații de cooperare cu sectorul privat, alte servicii administrative sau autorități publice;
- participarea la rețeaua CSIRT-urilor menționată la art. 12 din Directiva NIS.

Obligațiile CSIRT naționale sunt următoarele:

- garantează un nivel ridicat de disponibilitate a serviciilor sale de comunicații prin evitarea punctelor unice de defecțiune și dispune de mai multe mijloace de a fi contactat și de a contacta terțe persoane în orice moment;
- dispune de sedii si sisteme informatice amplasate pe site-uri securizate;
- asigură continuitatea afacerilor cu un sistem adecvat de gestionare a cererilor și de rutare pentru facilitarea transferurilor;
- participarea la reuniunile rețelelor CSIRT;
- se bazează pe o infrastructură a cărei continuitate este garantată;
- se asigură că toate canalele sale de comunicare sunt clar specificate și bine cunoscute partenerilor săi.

Toate măsurile luate trebuie să fie adecvate în vederea realizării obiectivelor definite de lege, să fie proporționale cu aceste obiective, și să respecte principiile obiectivității, transparenței și nediscriminării.

În îndeplinirea misiunilor sale, CSIRT folosește precauția necesară unei autorități publice, asigurându-se întotdeauna cu prioritate să nu perturbe funcționarea sistemului informatic, luând toate măsurile de precauție rezonabile pentru a nu se produce pagube materiale sistemului informatic.

BULGARIA

Legea privind securitatea cibernetică[8] reglementează activitățile privind:

h) organizarea, managementul și controlul securității cibernetice, inclusiv activități și proiecte de apărare cibernetică și criminalitate cibernetică;
i) întreprinderea măsurilor necesare pentru atingerea unui nivel general ridicat de rețea și securitatea informațiilor.
j) stabilirea atribuțiilor organelor competente în domeniul securității cibernetice.

Potrivit legii, securitatea cibernetică este definită ca o activitate de implementare a unui set de măsuri și derularea unor acțiuni prin care spațiul cibernetic este protejat de amenințări. Securitatea cibernetică include securitatea rețelelor și a informațiilor, contracararea criminalității cibernetice și apărarea rețelelor cibernetice.

Securitatea rețelelor și a informațiilor implică acea capacitate a rețelelor și sistemelor informatice de a se opune la un anumit nivel de impact unor variabile care afectează negativ existența, veridicitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate sau servicii conexe, oferite de accesibile prin aceste rețele și sisteme informatice.

[8] https://www.mlsp.government.bg/uploads/3/zakonodatelstvo/za-kibersigurnost.pdf

Președintele Agenției de stat pentru „Guvernul Electronic/ digitalizare” creează și gestionează un registru al serviciilor esențiale, care conține:

1. tipurile de servicii esențiale;
2. lista operatorilor de servicii esențiale și a serviciilor prestate de aceștia;
3. sfera de activitate;
4. numărul de utilizatori care se bazează pe serviciul oferit de operator;
5. sfera geografică a zonei care poate fi afectată de un incident.

Registrul este revizuit și actualizat la fiecare doi ani de organele administrative.

Conducerea și organizarea sistemului de securitate cibernetică se realizează de către Consiliul de Miniștri.

Strategia națională de securitate cibernetică reprezintă un cadru strategic al politicii de securitate cibernetică, care include:

1. scopuri, principii și priorități;
2. domenii de acțiune și măsuri privind:

    a) arhitectura sistemului de securitate cibernetică;
    b) securitatea rețelelor și a informațiilor;
    c) combaterea criminalității informatice;
    d) apărarea cibernetică;
    e) inteligența cibernetică;

3. interacțiunea dintre stat, mediul de afaceri și societate;
4. dezvoltarea și îmbunătățirea cadrului de reglementare;
5.creșterea gradului de conștientizare, cunoștințe și competențe;
stimulatoare de cercetare și inovare în domeniul securității cibernetice;
6. cooperarea internațională;
7. diplomația cibernetică;
8. interacțiunea la nivel tehnic, operațional și strategic.

Consiliul de securitate cibernetică este un organism consultativ, coordonat de Consiliul de Miniștri. Președintele Consiliului de securitate cibernetică este viceprim-ministrul.

Membrii Consiliului de Securitate Cibernetică sunt:

1. ministrul de interne;
2. ministrul apărării;
3. ministrul afacerilor externe;
4. ministrul de finanțe;
5. ministrul transporturilor, tehnologiilor informaționale și comunicațiilor;
6. ministrul energiei;
7. ministrul sănătății;
8. ministrul mediului și apei;

9. ministrul apărării;
10. secretarul general al MAI;
11. președintele Agenției de stat pentru securitate națională;
12. președintele Agenției de informații de stat;
13. directorul Serviciului de informații militare;
14. șeful Serviciului național de securitate;
15. președintele Agenției de stat pentru guvernare electronică;
16. secretarul Consiliului de securitate cibernetică;
17. secretarul Consiliului de securitate la Consiliul de Miniștri;
18. un reprezentant al Președintelui Republicii, desemnat în mod expres de acesta prin decret.

CEHIA

Legea privind securitatea cibernetică și actele conexe (2014)[9], cu completările ulterioare, reglementează drepturile și obligațiile persoanelor și competențele autorităților publice în domeniul securității cibernetice.

Potrivit legii, spațiul cibernetic este un mediu digital care permite crearea, prelucrarea și schimbul de informații, constând din sisteme informaționale, servicii și rețele de comunicații electronice. Un serviciu de bază reprezintă acel serviciu a cărui furnizare depinde de rețele de comunicații electronice sau de sisteme de informații și a cărui întrerupere ar putea avea un impact semnificativ asupra securității activităților sociale sau economice într-unul dintre aceste sectoare:

- energie;
- transport;
- bancar;
- infrastructura pieței financiare;
- asistență medicală;
- managementul apei;
- infrastructură digitală;
- industria chimică.

Autoritățile și persoanele cărora li se impun obligațiile de securitate cibernetică sunt:

- furnizorul serviciului de comunicații electronice și entitatea furnizoare a rețelei de comunicații electronice;
- autoritatea sau persoana care furnizează rețeaua semnificativă;
- administratorul și operatorul sistemului informatic al infrastructurii informaționale critice;
- administratorul și operatorul unui sistem informatic semnificativ;
- furnizor de servicii digitale.

Măsurile de securitate sunt:
a) organizatorice
b) tehnice.

[9] https://www.zakonyprolidi.cz/cs/2014-181

Dintre măsurile organizatorice se evidențiază:
- sistemul de management al securității informațiilor;
- managementul riscului;
- politica de securitate;
- securitatea organizatorică;
- stabilirea cerințelor de securitate pentru furnizori;
- managementul activelor;
- securitatea resurselor umane;
- managementul traficului și comunicațiilor;
- controlul accesului persoanelor;
- achiziție, dezvoltare și întreținere;
- gestionarea evenimentelor de securitate cibernetică și a incidentelor de securitate cibernetică;
- managementul continuității activității;
- control și audit.

Măsurile tehnice sunt:
- securitatea fizică;
- crearea unui instrument de protecție a integrității rețelelor de comunicații;
- crearea de instrumente de verificare a identității utilizatorilor;
- instrumente de gestionare a drepturilor de acces;
- instrumente de protecție împotriva codurilor neautorizate;
- instrumente de înregistrare a activității sistemului informațional sau de
- comunicare către utilizatori și administratorii acestuia;
- instrumente pentru detectarea evenimentelor de securitate cibernetică;
- instrumente pentru colectarea și evaluarea evenimentelor de securitate
- cibernetică;
- securitatea aplicației;
- mijloace criptografice;
- instrumente pentru a asigura nivelul de disponibilitate a informațiilor;
- siguranța sistemelor industriale și de control.

CROAȚIA

Legea privind securitatea cibernetică a operatorilor de servicii-cheie și a furnizorilor de servicii digitale[10] reglementează procedurile și măsurile pentru atingerea unui nivel comun înalt de securitate cibernetică a operatorilor de servicii-cheie și a furnizorilor de servicii digitale, competențele și autoritățile organismelor sectoriale competente, punctului național unic de contact, organismelor responsabile cu prevenirea și protecția împotriva incidentelor și a organismului tehnic pentru evaluarea conformității, supravegherea operatorilor cheie de servicii și a furnizorilor de servicii digitale.

[10] https://narodne-novine.nn.hr/clanci/sluzbeni/2018_07_64_1305.html

Legea transpune Directiva nr. 2016/1148 a Parlamentului European și a Consiliului privind măsurile pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor de informații în spațiul Uniunii.

Pentru a determina semnificația efectului negativ pe care un incident l-ar avea asupra furnizării unui serviciu cheie se iau în considerare următoarele criterii:

- numărul și tipul de utilizatori cărora entitatea le furnizează serviciul;
- existența dependenței altor activități sau domenii de serviciul respectiv;
- cota de piață a entității care furnizează serviciul;
- distribuția geografică a subiectului în prestarea serviciului;
- impactul posibil al incidentului, având în vedere gravitatea și durata acestuia, asupra activităților economice și sociale și asupra siguranței publice;
- importanța activității entității în menținerea unui nivel suficient de securitate a serviciului critic, ținând cont de disponibilitatea mijloacelor alternative de furnizare a serviciului respectiv;
- alte criterii sectoriale precum cantitatea serviciului prestat, ponderea în prestarea serviciului sau activele entității.

Serviciile cheie sunt:

- energetic;
- transport;
- bancar;
- infrastructurile pieței financiare;
- sectorul de sănătate;
- alimentare și distribuție cu apă;
- infrastructură digitală:
- servicii de afaceri pentru organisme guvernamentale.

Operatorii de servicii cheie și furnizorii de servicii digitale trebuie, pentru a asigura continuitatea furnizării acestor servicii, să ia măsuri pentru atingerea unui nivel ridicat de securitate cibernetică a serviciilor lor. Acesta vizează:

- protecția împotriva programelor *malware*;
- configurarea sistemului;
- gestionarea schimbărilor în sistem;
- gestionarea dispozitivelor hardware utilizate de sistem;
- protecția împotriva indisponibilității sistemului;
- managementul continuității activității;
- backup de stocare a datelor;
- dezvoltarea și întreținerea sistemului;
- management de proiect;
- verificări preventive ale vulnerabilității sistemului.

Măsurile prevăzute de lege vor consta cel puțin în:

- măsuri tehnice și organizatorice pentru managementul riscurilor, ținând cont de cele mai recente evoluții tehnice utilizate în cadrul celor mai bune practici de securitate în domeniul securității cibernetice;

• măsuri de prevenire și atenuare a efectelor incidentelor asupra securității rețelelor și a sistemelor informaționale.

Măsurile de management al riscului operatorilor trebuie să conțină:

- determinarea riscului de incidente;
- prevenirea, detectarea și rezolvarea incidentelor;
- atenuarea impactului incidentelor la minimum.

Măsurile de gestionare a riscurilor furnizorilor de servicii digitale includ:

- securitatea sistemelor și instalațiilor;
- rezolvarea incidentelor;
- managementul continuității activității;
- monitorizarea, auditarea și testarea;
- conformitatea cu standardele internaționale.

Structurile CSIRT competente la nivel sectorial îndeplinesc următoarele sarcini:

- urmărirea incidentelor;
- furnizarea de avertismente și anunțuri timpurii, precum și informează despre riscuri și incidente;
- realizarea unei analize dinamice a riscurilor și incidentelor și pregătirea unei imagini de ansamblu asupra situației din sector;
- efectuarea de verificări regulate de vulnerabilitate ale sistemelor de rețea și oferirea de informații operatorilor de servicii și furnizorilor de servicii digitale;
- primesc notificări de incidente;
- la solicitarea operatorilor cheie de servicii sau a furnizorilor de servicii digitale, analizează și răspunde la incidentele apărute;
- dacă circumstanțele permit, la primirea notificării despre incident, furnizează operatorului de servicii informații relevante cu privire la incident și, în special, informații care ar putea contribui la rezolvarea eficientă a incidentului;
- adoptă linii directoare pentru standardizarea și îmbunătățirea stării de implementare a obligației de a sesiza incidentele apărute;
- informează organul sectorial competent cu privire la incidentele apărute;
- în cooperare cu organismul sectorial competent, determină impactul transfrontalier al incidentelor;
- informează punctul unic național de contact cu privire la incidente, în conformitate cu orientările acestuia;
- furnizează punctului național unic de contact informații cu privire la principalele elemente ale procedurilor de soluționare a incidentelor pe care le desfășoară;
- cooperează cu alte CSIRT-uri la nivel național și internațional.

DANEMARCA

Legea privind Centrul pentru securitate cibernetică[11] prevede că principala sarcină a acestuia este aceea de a susține un nivel ridicat de securitate a informațiilor în infrastructura tehnologiei informației și comunicațiilor de care depind funcții importante din punct de vedere social.

Serviciul de securitate al Centrului pentru securitate cibernetică are sarcina de a detecta, analiza și contribui la tratarea incidentelor de securitate. În cazuri speciale, Centrul poate solicita companiilor cu caracter deosebit de important din punct de vedere social, regiunilor și municipiilor să fie conectate la serviciul de securitate a rețelei în scopul monitorizării comunicării în rețea. Solicitarea poate acoperi doar acele părți ale companiilor, regiunilor sau municipalităților care au un impact semnificativ asupra infrastructurii critice a Danemarcei. Centrul trebuie să evalueze cel puțin o dată la șase luni dacă o comandă notificată trebuie menținută.

Pentru a descoperi incidentele de securitate, unei persoane juridice sau fizice i se poate solicita să prezinte sau să dezvăluie informații despre utilizatorul unui cont de e-mail, adresă IP sau nume de domeniu. Ordinul respectiv nu poate fi dat dacă intervenția este disproporționată față de semnificația cauzei și de eventualele pierderi create. O decizie cu privire la un astfel de ordin va fi luată de către instanță la cererea Centrului pentru securitate cibernetică.

Centrul pentru securitate cibernetică poate efectua analize automate ale datelor de trafic, pachetelor de date și datelor staționare reglementate de lege. Analizele manuale ale datelor pot avea loc numai în următoarele cazuri:

1. pentru a detecta, analiza și sprijini abordarea incidentelor de securitate, datele de trafic pot fi analizate în măsura în care este necesar.
2. în caz de suspiciune rezonabilă a unui incident de securitate, pachetele de date și datele staționare pot fi analizate în măsura în care este necesar pentru a clarifica aspectele legate de incident.
3. în cadrul investigațiilor tehnice preventive de siguranța sistemelor, datele de trafic și datele staționare pot fi analizate în măsura în care este acest lucru e necesar pentru efectuarea investigațiilor.
4. ca parte a lucrărilor în curs de susținere a unui nivel ridicat de securitate a informațiilor în domeniul Ministerului Apărării, inclusiv verificarea dacă comunicarea conține materiale clasificate, date de trafic și pachete de date provenite de la autoritățile din zona Ministerul Apărării poate fi analizat.
5. ca parte a testelor tehnice și a configurației unităților de alarmă ale serviciului de securitate a rețelei, datele de trafic și datele de pachete pot fi analizate în măsura în care este necesar pentru realizarea testului. Analiza poate fi efectuată numai de angajații care se ocupă de sarcini

[11] https://www.retsinformation.dk/eli/lta/2019/836

tehnice operaționale și de dezvoltare pentru Centrul pentru securitate cibernetică.

Centrul poate transmite datele de trafic către:

- poliție, dacă există o suspiciune rezonabilă a unui incident de securitate;
- autoritatea sau compania afiliată de la care provin datele în cauză, dacă există o suspiciune rezonabilă a unui incident de securitate și dacă este necesar pentru îndeplinirea sarcinilor Centrului;
- autoritățile daneze, furnizorii de rețele și servicii publice de comunicații electronice și alte servicii de securitate a rețelei, precum și autoritățile și companiile în general în legătură cu emiterea de alerte de securitate, dacă există o suspiciune rezonabilă a unui incident de securitate.

Centrul pentru Securitate Cibernetică ia măsuri tehnice și organizatorice adecvate împotriva distrugerii, pierderii sau deteriorării accidentale și/sau ilegale a informațiilor și împotriva ca acestea să fie aduse la cunoștința unor persoane neautorizate, abuzate sau prelucrate în alt mod cu încălcarea legii.

ESTONIA

În sensul Legii privind securitatea cibernetică[12], un furnizor de servicii digitale este un furnizor care:

1. oferă un loc de tranzacționare pe internet;
2. oferă un motor de căutare bazat pe Internet;
3. oferă un serviciu de *cloud computing*.

În ceea ce privește Punctul unic de contact, în temeiul prevederilor art. 9 alin (1) din Directiva (UE) 2016/1148 a Parlamentul European și al Consiliului, acesta este gestionat de Agenția națională a sistemului informațional.

În asigurarea securității cibernetice se ține cont de următoarele principii:

- principiul personalității - asigurarea securității sistemului va fi organizată de furnizorul de servicii;
- principiul protecției cuprinzătoare - furnizorul de servicii identifică posibile amenințări la adresa sistemului și implementează măsuri organizatorice și tehnice adecvate pentru protecția acestuia;
- principiul reducerii efectelor nocive - în cazul unui incident cibernetic, furnizorul de servicii va lua măsurile necesare pentru a preveni răspândirea și eventuala răspândire a incidentului cibernetic în alt sistem și anunță autoritatea de supraveghere competentă;
- principiul cooperării - părțile cooperează pentru asigurarea securității cibernetice și soluționarea incidentelor cibernetice, ținând seama, după caz, de interconexiunea și interdependența sistemelor și serviciilor.

[12] https://www.riigiteataja.ee/akt/122052018001

Pentru prevenirea și rezolvarea incidentelor cibernetice, Consiliul pentru sistemul informațional de stat va coordona asigurarea securității cibernetice precum și prevenirea și rezolvarea incidentelor cibernetice.

Consiliul va inspecta domeniile din spațiul de adresă al Protocolului estonian de Internet și aferente codului de țară al Estoniei, va analiza riscurile care pun în pericol securitatea sistemelor și impactul acestora asupra securitatea statului, a societății și a sistemului. În vederea prevenirii și soluționării unui incident cibernetic, Consiliul are sarcina de a transmite alerte persoanelor care trebuie să implementeze măsurile de prevenire sau reducere a efectelor incidentului cibernetic.

Consiliul are dreptul de a transmite informații legate de prevenirea și soluționarea unui incident cibernetic unui stat străin sau Comitetului pentru securitatea rețelelor și informațiilor al Uniunii Europene sau unei alte organizații pentru îndeplinirea sarcinilor prevăzute de dreptul Uniunii Europene, atunci când informațiile nu pun în pericol securitatea națională sau procedurile penale. În plus, la transmiterea informațiilor, Consiliul trebuie să țină cont de interesele de afaceri ale furnizorului de servicii sau ale furnizorului de servicii digitale și se ghidează după obligația de a păstra secretele de afaceri.

Registrul incidentelor cibernetice este o bază de date deținută de Consiliul sistemului informațional de stat în care sunt introduse date care descriu producerea unui incident cibernetic, în scopul ținerii evidenței incidentelor cibernetice și analizării acestora în vederea rezolvării și transmiterii de alerte.

Registrul are acces restricționat, iar informațiile din registru sunt destinate uzului intern, dacă legislația nu prevede altfel. Acesta se înființează prin decizie a ministrului competent.

Legea privind securitatea cibernetică va fi modificată de la 1 ianuarie 2023, prin introducerea unui nou standard de securitate a informațiilor din Estonia (E-ITS), care va înlocui actualul sistem de securitate de referință (ISKE)[13]. E-ITS este un standard de securitate a informațiilor în limba estonă și în conformitate cu spațiul legal din Estonia, care este în conformitate cu standardul internațional. E-ITS ajută la promovarea nivelului de securitate a informațiilor a instituțiilor din sectorul public, precum și a companiilor private, securitatea informațiilor devenind mai accesibilă și pentru organizațiile mai mici.

Practic, fiecare organizație poate alege modulele de securitate adecvate în funcție de dimensiunea și complexitatea sistemelor sale. Acest lucru permite reutilizarea celor mai bune practici de securitate a informațiilor și, de asemenea, economisește bani în domeniul securității informațiilor, adică permite tuturor să asigure o mai mare securitate a sistemelor lor la un cost mai mic.

În plus, modificările care vor fi adoptate permit ministrului întreprinderilor și tehnologiei informației să desemneze Consiliul pentru sistemul informațional de stat drept centru național de coordonare pentru industrie, tehnologie și cercetare în domeniul securității cibernetice și Autoritatea pentru protecția consumatorului și supravegherea tehnică drept organism național de certificare a securității cibernetice.

[13] https://www.ria.ee/et/uudised/mkm-valitsus-ajakohastab-kuberruumi-kaitse-eesmargil-kuberturvalisuse-seadust.html

FINLANDA

În 2019, Guvernul a aprobat strategia de securitate cibernetică a Finlandei, care stabilește obiective naționale pentru dezvoltarea mediului cibernetic și securizarea funcțiilor vitale aferente.

Principalele trei direcții strategice sunt[14]:

- cooperarea internațională;
- o mai bună coordonare a managementului securității cibernetice;
- planificarea, pregătirea și dezvoltarea expertizei în domeniul securității cibernetice.

Noua strategie de securitate cibernetică se bazează pe principiile generale ale strategiei de securitate cibernetică din anul 2013. Strategia și implementarea acesteia fac parte din implementarea strategiei UE de securitate cibernetică. Necesitatea actualizării strategiei de securitate cibernetică a fost dictată de schimbările semnificative produse în mediul de operare și zonele de dezvoltare specifice.

Principalele măsuri strategice sunt:

- asigurarea de resurse informaționale și servicii digitale pentru funcțiile vitale ale societății. Nivelurile țintă necesare pentru managementul continuității activității naționale sunt stabilite atât la nivelul activităților conexe, cât și la nivelul lanțurilor de servicii.
- îmbunătățirea și armonizarea managementului impus de apărarea securității naționale, în conformitate cu standardele critice de securitate. Pentru servicii se urmărește verificarea, testarea, evaluarea și implementarea produselor și a soluțiilor complete legate de funcțiile critice.
- cooperarea în domeniul securității cibernetice între autorități va fi dezvoltată în noile domenii informaționale apărute. Domeniile-cheie pentru dezvoltare sunt apărarea cibernetică și lupta împotriva amenințărilor cibernetice ce pot afecta securitatea națională. În plus, se are în vedere modificarea legislației privind combaterea criminalității cibernetice pentru a se permite prevenirea eficientă împotriva acestor acțiuni, precum și investigarea eficientă a amenințărilor apărute.
- Centrul de securitate cibernetică va elabora o imagine situațională 24/7 și va încuraja cooperarea dintre autorități și comunitatea de afaceri.
- în ceea ce privește funcțiile vitale ale societății, va fi sprijinită furnizarea de servicii de afaceri critice și dezvoltarea managementului privind continuitatea afacerilor. Sunt stabilite autorități responsabile, care au obiective clare pentru dezvoltarea securității cibernetice. Autoritățile publice pot contribui la obiectivele de securitate cibernetică incluzându-le în acorduri comerciale, care trebuie, însă, clarificate din punct de vedere legislativ.

[14] https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/

FRANȚA

Strategia națională pentru siguranța digitală prevede următoarele obiective[15]:

- implementarea de capacități științifice și tehnice și de resurse industriale necesare pentru protecția informațiilor suverane, a securității cibernetice și pentru dezvoltarea unei economii digitale de încredere.
- asigurarea utilizării în folosul statului a afacerilor și activităților cetățenilor, împreună cu o monitorizare activă a siguranței tehnologiilor utilizate. Având în vedere evoluțiile tehnologice majore, cum ar fi telecomunicațiile mobile de generație 5G sau rețelele definite de software, Franța va analiza natura și capacitățile echipamentelor hardware și software instalate la baza rețelelor sale de comunicații electronice, urmărind protejarea secretului corespondenței, viața privată a cetățenilor săi și rezistența acestor infrastructuri la atacurile cibernetice, continuând să-și adapteze cadrul de reglementare la noile tehnologii emergente.
- accelerarea consolidării securității sistemelor informaționale de stat.
- pregătirea organizațiilor pentru o eventuală criză digitală severă.

Prerogativele aparțin CERT-EU (capacitatea de răspuns la incidente informatice a instituțiilor, entităților și agențiilor din Uniunea Europeană) și NCIRC (capacitate de răspuns la incidentele informatice ale Organizației Tratatul Atlanticului de Nord) pentru a asigura apărarea cibernetică a instituțiilor respective.

Legea nr. 2018-133 privind diverse prevederi de adaptare la dreptul Uniunii Europene în domeniul securității cibernetice transpune Directiva NIS nr. 2016/1148[16].

Legea face astfel posibilă extinderea la toate categoriile de operatori a unui număr de obligații în materie de securitate a rețelelor și a sistemelor informaționale. Legea menționează faptul că securitatea rețelelor și a sistemelor informaționale constă în capacitatea acestora de a rezista, la un anumit nivel de încredere, acțiunilor care compromit disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate și a serviciilor aferente pe care aceste rețele și sisteme informaționale le oferă sau le fac accesibile.

Legea creează două noi categorii de actori: operatorii de servicii esențiale (OSE) și furnizorii de servicii digitale (DSP).

- operatorii de servicii esențiale sunt reprezentați de orice entitate publică sau privată care furnizează un serviciu esențial pentru menținerea activităților societale și/sau economice critice, dependente de rețele și sistemele informatice și al cărei serviciu ar putea fi grav afectat de un incident de securitate a rețelei.

[15] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf
[16] https://www.linklaters.com/en/insights/publications/2018/march/cyber-securite

Acești operatori vor fi stabiliți de către primul-ministru, în diverse sectoare precum:

- energie;
- transport;
- sistemul bancar;
- infrastructuri ale pieței financiare;
- sănătate;
- infrastructuri digitale.

Aceste OSE vor fi obligate:

i. să ia măsuri tehnice pentru a gestiona în amonte riscurile care amenință securitatea rețelelor;
ii. să prevină incidentele care compromit securitatea;
iii. să anunțe Agenția națională pentru securitatea sistemelor informaționale (ANSSI) despre acele incidente care au un impact semnificativ asupra securității rețelei.

În caz contrar, operatorii pot fi sancționați cu amendă penală cuprinsă între 75.000 și 125.000 de euro.

- furnizorii de servicii digitale reprezintă persoanele juridice care furnizează un serviciu digital, acest lucru acoperind trei tipuri de servicii digitale:

(i) motoarele de căutare online;
(ii) piețele online;
(iii) serviciile de *cloud computing*.

Acești furnizori sunt supuse unor obligații similare cu cele ale OSE. DSP-urile care au cel puțin 50 de angajați și care au o cifră de afaceri anuală de peste 10 milioane de euro trebuie să garanteze un nivel satisfăcător de securitate a sistemelor informaționale prin identificarea riscurilor, evitarea incidentelor și recurgerea la măsuri preventive.

În cazul în care DSP-urile nu au notificat ANSSI cu privire la incidentele de securitate a rețelei care au un impact semnificativ asupra furnizării serviciului respectiv, amendă penală este cuprinsă între 50.000 și 100.000 de euro.

GRECIA

Legea nr. 4577/2018 impune obligații importante pentru securitatea sistemelor și a rețelelor entităților din domeniile:

- energie;
- transport;
- bănci;
- infrastructură financiară;
- sănătate;
- alimentare cu apă;

- infrastructură digitală;
- comerț electronic;
- serviciile societății informaționale[17].

Legea stabilește Planul național de securitate cibernetică și desemnează Autoritatea națională de securitate cibernetică din cadrul Ministerului politicii digitale, telecomunicațiilor și informației, drept structura cu rol de supraveghere și reglementare în domeniu. De asemenea, legea prevede înființarea unei echipe de răspuns la incidentele de securitate informatică (CSIRT).

De asemenea, sunt stabilite obligații importante de securitate cibernetică pentru următoarele categorii de companii:

- operatorii de servicii esențiale care își desfășoară activitatea în domeniile menționate mai sus;
- furnizori de servicii digitale, în special întreprinderi de comerț electronic și, în general, servicii digitale, motoare de căutare și furnizori de *cloud computing*.

Întreprinderile care intră în sfera de aplicare a legii au următoarele obligații de bază în ceea ce privește securitatea sistemelor lor:

- adoptă masuri tehnice și organizatorice pentru securitatea rețelelor și sistemelor informatice;
- adoptă măsuri pentru prevenirea și minimizarea impactului incidentelor care afectează securitatea rețelelor și a sistemelor informaționale;
- anunță Autoritatea națională de securitate cibernetică și CSIRT cu privire la incidentele cu impact grav asupra continuității afacerii. Notificarea trebuie făcută fără întârzieri nejustificate și să fie însoțită de informații suplimentare cu privire la gravitatea incidentului relevant;
- cooperează cu autoritățile competente.

Autoritatea națională de securitate cibernetică are următoarele atribuții principale:

- evaluarea conformității întreprinderilor care se află sub incidența Legii nr. 4577/2018;
- notificarea companiilor responsabile pentru ca acestea să furnizeze informațiile necesare, inclusiv politicile de securitate;
- notificarea companiilor responsabile de corectarea oricărei încălcări a criteriilor de conformitate.

În urma avizului Autorității naționale de securitate cibernetică, ministrul de profil poate impune următoarele sancțiuni, în cazul încălcării prevederilor legale:

[17] https://www.platis-anastassiadis.com/en_gr/law-alerts/l-4577-2018-new-cybersecurity-obligations-for-essential-and-digital-services

- amendă de până la 15.000 de euro în situația lipsei notificării sau întârzierii trimiterii acesteia;
- amendă de până la 200.000 de euro în cazul neluării măsurilor organizatorice/tehnice adecvate pentru gestionarea riscurilor la adresa securității rețelei și a sistemului;
- amendă de până la 50.000 de euro în caz de nefurnizare sau întârziere nejustificată a furnizării informațiilor, la cererea Autorității naționale de securitate cibernetică.

GERMANIA

A doua lege privind creșterea securității sistemelor de tehnologie a informației[18] a intrat în vigoare în anul 2021. Acest lucru a conferit Oficiului federal pentru securitatea informației (BSI) noi competențe, care îi consolidează semnificativ activitatea ca autoritate federală de securitate cibernetică.

BSI gestionează următoarele aspecte:

- *detectare și apărare* - BSI are competențe sporite pentru a detecta lacunele de securitate și pentru a iniția măsuri împotriva atacurilor cibernetice. Îndeplinind rolul de centru de competență central pentru securitatea informațiilor, BSI poate astfel modela o digitizare sigură și, printre altele, poate defini standarde minime obligatorii pentru autoritățile federale, care pot fi monitorizate mai eficient;

- *securitatea cibernetică* în rețelele de comunicații mobile - legea conține o serie de prevederi care interzic utilizarea componentelor critice pentru a proteja ordinea publică sau securitatea în Germania. Operatorii de rețea trebuie să îndeplinească, de asemenea, cerințe de securitate ridicate, iar componentele critice trebuie să fie certificate. Printre altele, legea asigură securitatea informațiilor în rețelele mobile 5G;

- *protecția consumatorilor* - BSI va fi un centru de consiliere independent și neutru pentru consumatori cu privire la problemele de securitate IT la nivel federal, protecția consumatorilor devenind astfel o sarcină a BSI. Introducerea unei etichete uniforme de securitate IT pentru cetățeni are scopul de a face securitatea IT mai transparentă și de a identifica în mod clar produsele care sunt deja conforme cu anumite standarde de securitate;

- *securitate pentru companii* - grupul de infrastructuri critice a fost extins pentru a include și sectorul de eliminare a deșeurilor municipale. În plus, alte companii de interes public special (de exemplu, producătorii de armament sau companiile cu o importanță economică deosebit de mare) vor trebui, de asemenea, să implementeze anumite măsuri de securitate IT în viitor și vor fi incluse în schimbul de informații cu încredere cu BSI.

- *autoritate națională pentru certificarea securității cibernetice* - în conformitate cu prevederile legale, BSI are rolul de autoritate națională pentru certificarea securității cibernetice în sensul art. 58 alin. 1 din Regulamentul (UE) nr. 2019/881. Aceasta este responsabilă în special de monitorizarea și punerea în aplicare a reglementărilor în cadrul schemelor europene de certificare a

[18] https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1652954229494

securității cibernetice. Activitățile de supraveghere și certificare trebuie să fie strict separate de alte activități și trebuie să se desfășoare în mod independent.

ITALIA

Legea nr. 109/2021 privind securitatea cibernetică[19] definește sistemul național de securitate cibernetică, care este condus de Președintele Consiliului de Miniștri. Primul ministru este responsabil pentru:

- numirea și revocarea directorului general și a directorului general adjunct al Agenției naționale de securitate cibernetică (ACN) după informarea președintelui COPASIR (Comisia parlamentară pentru securitatea Republicii);
- adoptarea strategiei naționale de securitate cibernetică, după consultarea Comitetului interministerial pentru securitate cibernetică (CIC), organism cu funcție de consiliere;
- propune și supraveghează domeniul politicilor de securitate cibernetică, în scopul protejării securității naționale în spațiul cibernetic.

Agenția națională de securitate cibernetică a fost înființată pentru a proteja interesele naționale în domeniul securității cibernetice, are personalitate juridică de drept public și autonomie de reglementare administrativă, patrimonială, organizatorică, contabilă și financiară, în limitele prevederilor legale. ACN are până la un număr maxim de 8 birouri de nivel de conducere generală, precum și un număr de maximum 30 de secții de nivel de conducere, în limita resurselor disponibile. Agenția poate solicita în baza anumitor convenții și cu respectarea domeniilor de competență primară, colaborarea cu alte organe de stat, administrațiile locale, cu forțele armate, forțele de poliție sau alte structuri publice pentru îndeplinirea sarcinilor sale instituționale. Principalele sarcini ale agenției sunt:

- promovarea implementării acțiunilor comune menite să asigure securitatea cibernetică și reziliența pentru dezvoltarea digitalizării țării, a sistemului de producție și a administrațiilor publice;
- pregătește strategia națională de securitate cibernetică;
- realizează toate activitățile necesare pentru a sprijini funcționarea Nucleului de securitate cibernetică;
- dezvoltă capacităților naționale de prevenire, monitorizare, detectare și atenuare, pentru a face față incidentelor de securitate cibernetică și atacurilor cibernetice, inclusiv prin echipa de răspuns la incidente de securitate informatică (CSIRT) și pornirea operațională a Centrului național de evaluare și certificare;
- promovează definirea și menținerea unui cadru juridic național actualizat și coerent în domeniul securității cibernetice, ținând cont și de orientările și evoluțiile din arena internațională;

[19] https://focus.namirial.it/cyber-security-legge/#:~:text=%C3%88%20stata%20pubblicata%20in%20Gazzetta,82

- contribuie la creșterea securității sistemelor de tehnologie a informației și comunicațiilor (TIC) ale subiecților incluși în perimetrul național de securitate cibernetică, administrațiilor publice, operatorilor de servicii esențiale (OSE) și furnizorilor de servicii digitale (FSD);
- sprijină dezvoltarea competențelor industriale, tehnologice și științifice, promovând proiecte de inovare și dezvoltare, urmărind în același timp stimularea creșterii forței de muncă naționale în domeniul securității cibernetice în vederea obținerii autonomiei strategice naționale în acest sector;
- asumarea funcțiilor de interlocutor național unic pentru entitățile publice și private în domeniul măsurilor de securitate și activităților de inspecție în domeniile securității cibernetice naționale, securității rețelelor și sistemelor informaționale (potrivit prevederilor Directivei NIS) și securității rețelelor de comunicații electronice;
- realizează activități de comunicare și promovare a conștientizării stării de fapt în domeniul securității cibernetice, pentru a contribui la dezvoltarea unei culturi naționale pe această temă.

Comitetul interministerial pentru securitate cibernetică are următoarele atribuții:

- are funcții de consiliere, propunere și supraveghere a politicilor de securitate cibernetică, în scopul protejării securității naționale în domeniu;
- propune Președintelui Consiliului de Miniștri orientările generale care trebuie urmate în cadrul politicilor naționale de securitate cibernetică;
- exercită o supraveghere ridicată asupra implementării strategiei naționale de securitate cibernetică;
- promovează adoptarea inițiativelor necesare pentru a favoriza colaborarea eficientă, la nivel național și internațional, între subiecții instituționali și operatorii privați interesați de securitatea cibernetică, precum și pentru schimbul de informații și pentru adoptarea de bune practici și măsuri direcționate în scopul de a obține cele mai bune practici în domeniul securității cibernetice, precum și în ceea ce privește dezvoltarea industrială, tehnologică și științifică;
- își exprimă opinia cu privire la bugetul și bilanțul final al Agenției naționale de securitate cibernetică.

Nucleul de securitate cibernetică a fost creat pentru a-l sprijini pe președintele Consiliului de Miniștri în materia securității cibernetice, în ceea ce privește aspectele legate de prevenirea și pregătirea oricăror situații de criză și pentru activarea procedurilor de alertă, fiind compus din:

- consilierul militar al Președintelui Consiliului de Miniștri;
- un reprezentant al DIS (Departamentul de informații pentru securitate);
- un reprezentant al AISE (Agenția de informații externe și securitate);
- un reprezentant al AISI (Agenția de informare și securitate internă);

- un reprezentant al fiecăruia dintre ministerele reprezentate în Comitet, al Ministerului cercetării și al Departamentului de protecție civilă al Președinției Consiliului de Miniștri.

Nucleul are următoarele atribuții:

- formulează propuneri de inițiative pe tema securității cibernetice în țară, în cadrul contextului internațional în materie;
- promovează programarea și planificarea operațională a răspunsului la situațiile de criză cibernetică de către administrațiile și operatorii privați;
- promovează și coordonează desfășurarea de exerciții interministeriale și participă la exerciții internaționale privind simularea evenimentelor cibernetice în scopul creșterii rezistenței țării;
- evaluează și promovează, împreună cu administrațiile competente, procedurile de schimburi de informații, inclusiv cu operatorii privați interesați, în scopul emiterii de alarme legate de evenimente cibernetice și pentru managementul crizelor.

LETONIA

Viziunea politicii de securitate cibernetică este reprezentată de un spațiu cibernetic sigur, deschis, gratuit și de încredere, cu servicii garantate sigure, fiabile și neîntrerupte, esențiale pentru stat și societate, drepturile omului trebuind să fie respectate atât în mediul fizic, cât și în cel virtual[20].

Potrivit prevederilor strategiei privind securitatea cibernetică, Letonia trebuie să profite de mediul digital pentru a asigura economia și bunăstarea socială, reducând în același timp nivelul general al riscurilor de securitate cibernetică, fără a restricționa fluxul de tehnologie, comunicații și date.

Scopul politicii de securitate cibernetică pentru perioada 2019-2022 este reprezentat de consolidarea și dezvoltarea capacităților de apărare cibernetică prin creșterea rezistenței la atacurile cibernetice și conștientizarea publicului cu privire la amenințările din spațiul cibernetic.

Pentru atingerea scopului propus sunt urmărite:

- atenuarea riscurilor de securitate cibernetică;
- dezvoltarea capacităților naționale de apărare cibernetică;
- securitatea infrastructurilor TIC și a sistemelor informatice;
- creșterea gradului de conștientizare a publicului cu privire la riscurile cibernetice;
- lupta împotriva criminalității informatice.

[20] https://likumi.lv/ta/id/220962-informacijas-tehnologiju-drosibas-likums

Principiile de bază ale securității cibernetice sunt următoarele:

- securitatea cibernetică nu este un scop în sine, ci o parte integrantă a securității naționale;
- baza funcționării statului, societății și economiei moderne, promovarea securității cibernetice la nivel internațional în cooperare cu aliații și partenerii necesari pentru atingerea obiectivelor naționale de securitate cibernetică;
- implicarea societății civile, a sectorului privat, reprezentanților publici și academicienilor;
- securitatea cibernetică este asigurată cu respectarea drepturilor omului;
- anticiparea timpurie, investigarea și prevenirea atacurilor cibernetice;
- securitatea cibernetică începe cu responsabilitatea individuală pentru utilizarea în siguranță a structurii TIC.

Potrivit prevederilor Legii privind securitatea tehnologiei informației[21], instituțiile de prevenire a incidentelor de securitate în domeniul tehnologiei informației promovează securitatea în domeniu, în Letonia. Sarcinile instituțiilor de prevenire a incidentelor de securitate sunt îndeplinite de:

1. Serviciul de informații și securitate militară în raport cu Ministerul Apărării, instituțiile subordonate acestuia, împreună cu Forțele armate naționale;
2. Institutul de matematică și informatică al Universității din Letonia în legătură cu instituțiile guvernamentale de stat si locale, cu unele excepții, precum și cu persoanele juridice de drept privat.

Institutul de matematică și informatică îndeplinește sarcinile specificate de lege și își exercită competențele sub autoritatea Ministerului Apărării, în conformitate cu actele normative, prevederile acordului de delegare și fondurile alocate de la bugetul de stat. Atunci când iau decizii administrative, Institutul respectă cerințele Legii privind structura administrației publice.

Instituțiile guvernamentale de stat și locale și persoanele juridice de drept privat au obligația de a coopera cu instituțiile de prevenire a incidentelor de securitate, furnizându-le informațiile necesare și respectând cerințele legale.

Institutul:

- menține o reprezentare unitară a activităților care se desfășoară în spațiul informatic electronic;
- oferă sprijin în prevenirea unui incident de securitate sau coordonează acțiunile de prevenire a acestuia;
- oferă recomandări necesare pentru prevenirea riscurilor actuale din domeniul tehnologiei informației, în conformitate cu amenințările actuale într-un mod accesibil publicului;
- desfășoară lucrări de cercetare, organizează evenimente educaționale, instruire și exerciții în domeniul securității tehnologiei informației;
- acordă sprijin instituțiilor statului în activitățile de protejare a securității naționale, precum și în ceea ce privește detectarea și

[21] https://likumi.lv/ta/id/220962-informacijas-tehnologiju-drosibas-likums

investigarea infracțiunilor din domeniul tehnologiei informației, cu respectarea restricțiilor privind prelucrarea datelor specificate în actele normative;
- supraveghează îndeplinirea obligațiilor prevăzute de lege, de către instituțiile guvernamentale de stat și locale, furnizorii de servicii de bază, furnizorii de servicii digitale și structurile de comunicații electronice;
- cooperează cu instituții/unități de prevenire a incidentelor de securitate recunoscute la nivel internațional.

Instituțiile de prevenire a incidentelor de securitate au dreptul:
- să solicite și să primească de la instituțiile guvernamentale de stat și locale, precum și de la persoanele juridice de drept privat, informații privind cerințele de securitate ale tehnologiei informației (inclusiv în ceea ce privește rețelele și sistemele informaționale) și informații tehnice referitoare la un incident de securitate care a avut loc sau este în curs de desfășurare (informații privind amploarea incidentului, fișierele software afectate, descrierea vulnerabilităților, măsurile tehnice luate pentru a preveni incidentul, informații despre activitățile dăunătoare sau alte informații tehnice, inclusiv adrese IP);
- să obțină un flux de date online de la instituțiile guvernamentale de stat și locale și de la persoane juridice de drept privat, de comun acord;
- să efectueze inspecții ale infrastructurii critice;
- să ia decizii (și să emită acte administrative) pentru a asigura îndeplinirea obligațiilor prevăzute de lege pentru instituțiile administrației publice de stat și locale, precum și pentru persoanele juridice de drept privat.

LITUANIA

Principiile securității cibernetice, enunțate de Legea privind securitatea cibernetică sunt următoarele[22]:

1. nediscriminarea în spațiul cibernetic;
2. managementul riscului de securitate cibernetică - măsurile de securitate cibernetică aplicate trebuie să asigure gestionarea riscurilor care sunt evaluate periodic de către entitățile de securitate cibernetică;
3. proporționalitatea securității cibernetice - măsurile legale, organizatorice și tehnice aplicabile de securitate cibernetică nu trebuie să restrângă activitățile entităților în spațiul cibernetic, dincolo de ceea ce este necesar;
4. interes public primordial - măsurile de securitate cibernetică aplicate trebuie să asigure în primul rând protecția interesului public, dar nu trebuie să încalce drepturile consumatorilor individuali sau să

[22] https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/15e540727ac211e89188e16a6495e98c

restrângă în mod disproporționat libertatea acestora în spațiul cibernetic;

5. standardizare și neutralitate tehnologică - în implementarea măsurilor de securitate cibernetică, actorii securității cibernetice sunt încurajați să respecte standardele și specificațiile naționale, ale Uniunii Europene și alte standarde internaționale de securitate cibernetică pentru sistemele de comunicații și informații, fără a solicita sau prioritiza vreun tip specific de tehnologie;
6. subsidiaritate - securitatea cibernetică a sistemelor de comunicații și informații și a serviciilor furnizate de acestea revine în responsabilitatea entităților de securitate cibernetică care operează și prestează servicii prin aceste sisteme. În domeniile care intră în competența exclusivă a actorilor de securitate cibernetică, autoritățile de formulare și de implementare a politicii de securitate cibernetică iau măsuri numai atunci când securitatea cibernetică a sistemelor de comunicații și informații și a serviciilor furnizate de acestea nu pot fi asigurate de entitățile de securitate cibernetică care operează aceste sisteme.

Consiliul de securitate cibernetică este un organism consultativ permanent, colegial, independent care analizează starea securității cibernetice în Republica Lituania și oferă diferitelor instituții forme de implementare a politicilor de securitate cibernetică, iar entităților de securitate cibernetică, instituțiilor de cercetare și celor de afaceri care operează în domeniu, propuneri de îmbunătățire a securității cibernetice.

Consiliul de securitate cibernetică este prezidat de un reprezentant al Ministerului Apărării Naționale, principalele atribuții fiind următoarele:

- înaintează propuneri entităților din sectorul securității cibernetice cu privire la prioritățile de securitate cibernetică, direcțiile de dezvoltare, rezultatele urmărite și metodele de implementare ale acestora;
- înaintează propuneri entităților din sectorul securității cibernetice cu privire la posibilitățile de cooperare dintre sectorul public, cel de afaceri și știință în domeniul asigurării securității cibernetice;
- analizează tendințele de îmbunătățire a securității cibernetice, furnizează concluzii și propuneri entităților din sectorul securității cibernetice privind gestionarea incidentelor cibernetice;
- oferă recomandări cu privire la consolidarea securității cibernetice.

Centrul național de securitate cibernetică este o instituție aflată în subordinea Ministerului Apărării Naționale. Acesta:

- monitorizează conformitatea entităților de securitate cibernetică și a sistemelor de comunicații și informații cu cerințele organizatorice și tehnice de securitate cibernetică aplicabile entităților de securitate cibernetică și investighează starea securității cibernetice;
- oferă instrucțiuni de securitate cibernetică și furnizează informațiile necesare efectuării evaluării de conformitate a entităților de securitate cibernetică și a sistemelor de comunicații și informații gestionate de

acestea, cu cerințele organizatorice și tehnice de securitate cibernetică aplicabile structurilor de securitate cibernetică și a stării de securitate cibernetică;

- aplică măsuri tehnice pentru a evalua rezistența resurselor informaționale de stat și a infrastructurilor informaționale critice la incidente cibernetice;
- emite instrucțiuni legate de asigurarea securității cibernetice și eliminarea deficiențelor de securitate cibernetică identificate, stabilește un termen limită pentru îndeplinirea acestor instrucțiuni societăților care gestionează resursele informaționale ale statului, administratorilor de infrastructură informațională critică, rețelelor publice de comunicații, furnizorilor de servicii de comunicații și celor care oferă servicii de găzduire a informațiilor electronice;
- instruiește entitățile de securitate cibernetică, cu excepția furnizorilor de servicii digitale, efectuează un audit independent de securitate al sistemelor de comunicații și informații sau al serviciilor furnizate de acestea pe cheltuiala lor și prezintă rezultatele unui astfel de audit, dacă nu se respectă cerințele organizatorice și tehnice de securitate cibernetică;
- monitorizează incidentele cibernetice la nivel național și efectuează analize de risc în spațiul cibernetic și în legătură cu incidentele cibernetice;
- în conformitate cu planul de implementare a măsurilor tehnice de securitate cibernetică coordonat cu entitățile care gestionează resursele informaționale de stat sau administratorii infrastructurii informaționale critice, în conformitate cu procedura stabilită de ministrul apărării naționale, implementează și gestionează măsuri de securitate cibernetică pentru resursele informaţionale ale statului şi de importanţă deosebită în infrastructurile informaţionale.
- aplică măsurile de securitate cibernetică necesare în timpul unui incident cibernetic;
- participă la managementul crizelor de securitate cibernetică;
- informează publicul despre incidentele cibernetice individuale sau solicită entității de securitate cibernetică să facă acest lucru;
- prelucrează datele cu caracter personal necesare îndeplinirii funcțiilor Centrului în domeniul asigurării securității cibernetice, cooperând cu organizațiile internaționale în domeniu.

Măsurile implementate cu fondurile Centrului național de securitate cibernetică sunt folosite exclusiv pentru asigurarea securității cibernetice.

Măsurile tehnice de securitate cibernetică instalate pe cheltuiala Centrului național de securitate cibernetică sunt întreținute tehnic, iar reparațiile acestora se efectuează pe cheltuiala Centrului.

ȚĂRILE DE JOS

Prezentarea generală a legislației și reglementărilor privind securitatea cibernetică se regăsesc în răspunsul guvernului la raportul WRR[23] „Pregătirea pentru perturbarea digitală” și răspunsul Agenției pentru securitate cibernetică (2020).

Legea privind securitatea rețelelor și a sistemelor informatice[24] se aplică:

- furnizorilor unui serviciu esențial sau categoriilor de astfel de furnizori;
- alți furnizori vitali sau categorii de astfel de furnizori.
- Domeniile vizate sunt:
- energie;
- telecomunicații;
- transport;
- energie nucleară;
- alimentare cu apă;
- societăți financiare;
- asistență medicală.

Furnizorul de servicii esențiale și furnizorul de servicii digitale iau măsuri tehnice și organizatorice adecvate și proporționale pentru a gestiona riscurile la adresa securității rețelei și a sistemelor lor de informații.

Măsurile furnizorului de servicii digitale iau în considerare următoarele aspecte:

- securitatea sistemelor și instalațiilor;
- gestionarea incidentelor;
- managementul continuității activității;
- supraveghere, control și testare;
- respectarea standardelor internaționale.

În cazul producerii de incidente, notificarea acestora trebuie să cuprindă, conform legii, următoarele aspecte:

- natura și amploarea incidentului;
- ora probabilă a începerii incidentului;
- posibilele consecințe ale incidentului în și în afara Țărilor de Jos;
- un prognostic al timpului de recuperare;
- dacă este posibil, măsurile luate sau care urmează să fie luate de către furnizor pentru a limita consecințele incidentului sau pentru a preveni repetarea acestuia;
- datele de contact ale ofițerului responsabil cu întocmirea raportului.

[23] https://open.overheid.nl/repository/ronl-ec4dde7f-d0b3-46dc-83f7-174c42584100/1/pdf/tk-bijlage-overzicht-wet-en-regelgeving-cybersecurity.pdf
[24] https://wetten.overheid.nl/BWBR0041515/2022-05-01

Dacă este solicitat, furnizorul care a făcut o notificare menționată de lege va furniza imediat ministrului de resort toate celelalte informații necesare pentru:

- sprijinirea furnizorului de servicii în luarea de măsuri pentru garantarea sau restabilirea continuității serviciilor sale;
- estimarea riscurilor pentru rețele și sistemele informatice.

Pentru a stabili dacă un incident are consecințe semnificative, se iau în considerare următoarele aspecte:

- numărul de utilizatori afectați de întreruperea serviciului;
- durata incidentului;
- întinderea ariei geografice afectate de incident.
- amploarea perturbării funcționării serviciului;
- amploarea consecințelor asupra activităților economice și sociale.

Autoritatea competentă poate aplica contravenientului o amendă administrativă în cazul încălcării prevederilor legale menționate. Amenda este cuprinsă între 1 și 5 milioane de euro.

POLONIA

Sistemul național de securitate cibernetică cuprinde[25]:

- operatorii de servicii esențiale;
- furnizorii de servicii digitale;
- CSIRT MON[26];
- CSIRT NASK[27];
- CSIRT GOV[28];
- echipe sectoriale de securitate cibernetică;
- unitățile din sectorul finanțelor publice;
- institute de cercetare;
- Banca națională a Poloniei;
- Banca națională de economii;
- Biroul de inspecție tehnică;
- agenția pentru servicii de navigație aeriană;
- centrul polonez de acreditare;
- centrul național pentru protecția mediului și gospodărirea apelor, precum și centrele voievodale;
- societăți comerciale care îndeplinesc sarcini de utilitate publică;

[25] https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/U/D20181560Lj.pdf
[26] Echipa de răspuns la incidente de securitate, condusă de ministrul apărării naționale.
[27] Echipa de răspuns la incidente de securitate, condusă de Institutul național de cercetare.
[28] Echipa de răspuns la incidente de securitate, condusă de șeful Agenției de securitate internă.

- entități care furnizează servicii de securitate cibernetică;
- autoritățile competente de securitate cibernetică;
- Punctul unic de contact pentru securitate cibernetică, etc.

Operatorii de servicii esențiale asigură:

1) evaluarea sistematică a riscului de incident și gestionarea acestui risc;
2) implementarea unor măsuri adecvate și proporționale cu riscul evaluat, din punct de vedere tehnic și organizatoric, ținând cont de cea mai recentă stare a cunoștințelor, inclusiv:

i. întreținerea și funcționarea în siguranță a sistemului informațional;
ii. securitatea fizică și de mediu, inclusiv controlul accesului;
iii. securitatea și continuitatea furnizării serviciilor de care depinde performanța serviciului-cheie,
iv. implementarea, documentarea și menținerea planurilor de acțiune care să permită furnizarea continuă și neîntreruptă a serviciului esențial și asigurarea confidențialității, integrității, disponibilității și autenticitatea informațiilor;
v. acoperirea sistemului informatic utilizat pentru furnizarea serviciului cu un sistem continuu de monitorizare.

3) colectarea de informații despre amenințările și vulnerabilitățile securității cibernetice, incidente ale sistemului informatic utilizat pentru furnizarea serviciului cheie;
4) managementul incidentelor;
5) aplicarea măsurilor de prevenire și reducere a impactului incidentelor asupra securității sistemului informatic utilizat pentru serviciul-cheie, inclusiv:

i. utilizarea unor mecanisme care asigură confidențialitatea și integritatea datelor prelucrate în sistem;
ii. actualizarea software-ului;
iii. protecția împotriva modificărilor neautorizate din sistemul informatic;
iv. luarea de măsuri imediate la descoperirea unei vulnerabilități sau amenințări la adresa securității cibernetice;

6) utilizarea mijloacelor de comunicare care să permită comunicarea corectă și sigură în cadrul sistemului național de securitate cibernetică.
În cazul unui incident, operatorul asigură rezolvarea acestuia prin[29]:

- clasificarea incidentelor pe baza criteriilor specificate de Consiliul ministrului prin regulament;
- dacă incidentul este clasificat drept grav - raportarea către CSIRT competent în cel mult 24 de ore de la momentul detectării,
- cooperarea cu CSIRT ca entitate cu funcție de gestionare a incidentelor, împreună cu asigurarea accesului adecvat la informații,
- eliminarea vulnerabilităților sistemului.

[29] https://cyberpolicy.nask.pl/ustawa-o-krajowym-systemie-cyberbezpieczenstwa/

Atunci când este desemnată o echipă sectorială de securitate cibernetică, operatorul transmite suplimentar un raport echipei, cooperează cu aceasta prin transmiterea datelor necesare și oferă echipei acces la informații despre incidentele înregistrate.

Raportul de incident trebuie să includă:

- informații de identificare (detalii de contact ale entității raportoare, detalii ale persoanei raportoare, detalii ale persoanei autorizate să prezinte situația existentă);
- descrierea impactului incidentului asupra furnizării serviciului-cheie (descrierea serviciului, numărul de utilizatori, domeniul geografic, impactul incidentului, cauza incidentului, cursul și efectele sale);
- informații pentru CSIRT relevant despre impactul posibil al incidentului asupra unui număr mai mare de state membre ale UE;
- în cazul unui incident care ar putea avea un impact asupra furnizării unui serviciu cheie - descrierea cauzelor, cursului și efectelor incidentului;
- informații despre acțiunile preventive și corective întreprinse.

Directiva NIS a oferit statelor membre flexibilitate în ceea ce privește numărul de CSIRT înființate. Legea poloneză desemnează trei CSIRT la nivel național:

- CSIRT NASK în structurile Institutului național de cercetare;
- CSIRT GOV în structurile Agenției de securitate;
- CSIRT MON în structurile Ministerului Apărării Naționale.

Fiecare CSIRT național are o zonare clar definită.

- CSIRT MON coordonează gestionarea incidentelor semnalate de entitățile din subordinea ministrului Apărării Naționale și de întreprinderile de importanță economică și de apărare deosebită.
- CSIRT GOV coordonează incidentele raportate de administrația guvernamentală, Banca Națională a Poloniei, Banca Națională de Economii și operatorii de infrastructură critică.
- CSIRT NASK coordonează incidentele raportate de alte entități, inclusiv operatori de servicii-cheie, furnizori de servicii digitale și administrația locală.

Persoane fizice - cetățenii pot raporta incidente și către CSIRT NASK. În plus, în cazul incidentelor teroriste, sunt competente CSIRT MON și CSIRT GOV (în conformitate cu prevederile Legii privind activitățile antiteroriste și ale Legii privind Serviciul de contrainformații militare și Serviciul de informații militare). În cazul incidentelor legate de apărarea națională, competența revine CSIRT MON.

Toate cele trei CSIRT la nivel național cooperează cu autoritățile competente, ministrul competent pentru informatizare și Comisarul pentru securitate cibernetică.

În plus, sarcinile lor includ:

- monitorizarea amenințărilor și incidentelor de securitate cibernetică la nivel național;
- evaluarea riscurilor la nivel de țară;
- furnizarea de informații privind incidentele și riscurile altor entități incluse în sistemul național de securitate cibernetică;
- emiterea de mesaje despre amenințările identificate la adresa securității cibernetice;

- răspunsul la incidentele raportate;
- coordonarea gestionării incidentelor critice (după calificarea prealabilă a acestora drept incidente critice);
- în cazuri justificate, examinarea unui dispozitiv sau software informatic în scopul identificării unei vulnerabilități, utilizarea acestuia putând amenința integritatea, confidențialitatea, responsabilitatea, autenticitatea sau disponibilitatea datelor prelucrate, ceea ce poate afecta securitatea publică sau un interes important al statului;
- depunerea cererilor de „recomandări privind utilizarea dispozitivelor sau software-ului informatic" pentru entitățile sistemului național de securitate cibernetică în ceea ce privește impactul acestora asupra securității publice sau a unui interes important al statului;
- cooperarea cu echipele sectoriale de securitate cibernetică, atât în sfera de coordonare a gestionării incidentelor grave și critice, cât și în sfera schimbului de informații care să permită contracararea amenințărilor la adresa securității cibernetice;
- cooperarea cu alte țări UE în schimbul de informații cu privire la incidente grave și semnificative;
- transmiterea către Punctul unic de contact (ministrul responsabil cu informatizarea) a unei liste a incidentelor (grave și semnificative) raportate în anul calendaristic precedent;
- elaborarea în comun și transmiterea către ministrul competent pentru informatizare a unei părți din Raportul privind amenințările la adresa securității naționale menționat la art. 5a alineat. 1 din Legea din 26 aprilie 2007 privind managementul crizelor privind securitatea cibernetică.

PORTUGALIA

Legea privind securitatea spațiului cibernetic[30], de transpunere a Directivei (UE) nr. 2016/1148 a Parlamentului European și a Consiliului privind măsurile de asigurare a unui nivel comun ridicat de securitate a rețelelor și a sistemelor informaționale se aplică:

a) administrației publice;
b) operatorilor de infrastructură critică;
c) operatorilor de servicii esențiale;
d) furnizorilor de servicii digitale;
e) orice alte entități care utilizează rețele și sisteme de informații.

În sensul legii, fac parte din administrația publică:

- statul;
- regiunile autonome;
- autoritățile locale;
- entitățile administrative independente;
- institute publice;

[30] https://dre.pt/dre/detalhe/lei/46-2018-116029384

- companiile publice;
- asociațiile obștești.

Consiliul Superior pentru securitatea *cyberspace*-ului este organul specific care îl consultă pe primul-ministru în problemele legate de securitatea spațiului cibernetic.

Consiliul *cyberspace* are următoarea componență:

- ministrul de resort, care prezidează consiliul;
- șeful Autorității naționale de securitate, care îl poate înlocui pe ministrul de resort;
- Secretarul general al Sistemului de securitate internă;
- Secretarul general al Sistemului informațional al Portugaliei;
- doi deputați numiți de Adunarea Republicii prin metoda d'Hondt;
- directorul Serviciului de informații de securitate;
- directorul Serviciului de informare strategică a apărării;
- coordonatorul Centrului național de securitate cibernetică;
- un reprezentant din zona de administrare electorală, etc.

În componența Consiliului mai sunt incluși un reprezentant al guvernului Regiunii autonome Azore și unul al guvernului Regiunii autonome Madeira.

Echipa națională de răspuns la incidente de securitate informatică este *CERT.PT,* care funcționează la Centrul național de securitate cibernetică.

Această structură are următoarele atribuții:

- exercită coordonarea operațională ca răspuns la incidente, în conlucrare cu echipele sectoriale de răspuns la incidentele de securitate IT existente;
- monitorizează incidentele cu implicații naționale;
- activează mecanismele de avertizare timpurie;
- intervine în reacția, analiza și atenuarea incidentelor;
- realizează analiza dinamică a riscului;
- asigură cooperarea cu entități publice și private;
- promovează adoptarea și utilizarea practicilor comune sau standardizate;
- participă la forumurile naționale de cooperare în domeniul securității informatice.

Încălcarea prevederilor legale constituie contravenții administrative. Constituie infracțiuni foarte grave:

- nerespectarea obligației de implementare a cerințelor de securitate;
- nerespectarea instrucțiunilor de securitate cibernetică emise de Centrul național de securitate cibernetică;
- nerespectarea obligației de a sesiza Centrul național de securitate cibernetică în legătură cu incidentele apărute;

- nerespectarea obligației de a notifica Centrul național de securitate cibernetică a identificării ca furnizor de servicii digitale.

Infracțiunile administrative menționate se pedepsesc cu amendă de la 5.000 la 25.000 euro, în cazul persoanelor fizice și cu 10.000 - 50.000 euro, în cazul persoanelor juridice.

Veniturile din amenzi revin la:

a) 60% pentru stat;

b) 40% pentru Centrul național de securitate cibernetică.

SLOVACIA

Conform prevederilor Legii privind securitatea cibernetică și modificările aduse anumitor legi (2018)[31], Biroul pentru securitate cibernetică:

- gestionează și coordonează performanța administrației de stat,
- stabilește standarde, proceduri operaționale, emite o metodologie și o politică de conduită în spațiul cibernetic;
- stabilește principiile pentru prevenirea și tratarea incidentelor de securitate cibernetică;
- pregătește o strategie națională de securitate cibernetică și un raport anual privind starea securității cibernetice în Republica Slovacă, în cooperare cu autoritățile competente ale statului;
- este Punctul național de contact pentru securitatea cibernetică în străinătate și asigură cooperarea cu punctele unice de contact ale statelor membre ale Uniunii Europene și ale Organizației Tratatului Atlanticului de Nord;
- îndeplinește obligațiile de notificare și raportare față de organismele relevante ale Uniunii Europene și ale Organizației Tratatului Atlanticului de Nord și participă și sprijină stabilirea de parteneriate la nivel național și internațional în domeniul securității cibernetice;
- asigură apartenența Republicii Slovace la grupul de cooperare și la rețeaua CSIRT-urilor,
- în cooperare cu Ministerul afacerilor externe și afacerilor europene al Republicii Slovace, dezvoltă cooperarea internațională și monitorizează efectele activităților de securitate cibernetică asupra intereselor de politică externă ale Republicii Slovace și ale partenerilor din cadrul Uniunii Europene și ale Organizației Tratatului Atlanticului de Nord;
- cooperează cu autoritățile centrale, cu alte organe ale administrației de stat și cu unitățile CSIRT, cu operatorii de servicii de bază și cu furnizorii de servicii digitale în îndeplinirea sarcinilor legale;

[31] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/

- administrează și operează sistemul informatic unificat de securitate cibernetică.

La notificarea Autorității centrale sau din proprie inițiativă, furnizorul de servicii de bază și cel de servicii digitale stabilesc:

1. serviciul de bază al entității, pe care îl include în lista serviciilor de bază;
2. serviciul digital, pe care îl include în lista serviciilor digitale.

Sistemul informațional unificat de securitate cibernetică este un sistem informatic gestionat și operat de Birou, care servește la coordonarea, înregistrarea și controlul efectiv al performanței administrației de stat în domeniul securității cibernetice și al unităților CSIRT. Acest sistem este destinat, de asemenea, procesării și evaluării datelor și informațiilor privind starea securității cibernetice și servește pentru planificarea crizelor în timp de pace, managementul statului în situații de criză, altele decât starea de război.

Sistemul cuprinde un sistem de comunicare pentru raportarea și rezolvarea incidentelor de securitate cibernetică și un sistem central de avertizare timpurie. Sistemul informațional unificat este format dintr-o parte publică și o parte non-publică, iar accesul la acesta este gratuit. Partea publică a sistemului conține:

- registrul autorităților centrale;
- lista serviciilor de bază;
- registrul furnizorilor de servicii de bază;
- lista de servicii digitale;
- registrul furnizorilor de servicii digitale;
- registrul incidentelor de securitate cibernetică;
- lista CSIRT-urilor acreditate;
- metodologii, orientări, standarde, politici și comunicări;
- informații și date necesare pentru utilizarea sistemului unic de informații în domeniul securității cibernetice,
- alerte și avertismente, precum și alte informații pentru a minimiza, a preveni sau a remedia consecințele unui incident de securitate cibernetică.

Sistemul de comunicare pentru raportarea și rezolvarea incidentelor de securitate cibernetică este un sistem de comunicare care asigură achiziția, concentrarea, analiza și evaluarea sistematică a informațiilor privind incidentele de securitate cibernetică.

Sistemul central de avertizare timpurie este un sistem informatic care asigură schimbul în timp util de informații privind amenințările, incidentele de securitate cibernetică și riscurile asociate acestora între Birou și entitățile de profil. Acesta are acces direct la partea nepublică a sistemului informatic unificat de securitate cibernetică în timp real, în măsura specificată de Birou sau în baza unei reglementări speciale.

Orice persoană care este obligată în temeiul legii să furnizeze informații, date și rapoarte prin sistemul informatic unificat de securitate cibernetică, în mod gratuit și fără întârziere.

SLOVENIA

Legea reglementează domeniul securității informațiilor și măsurile pentru atingerea unui nivel înalt de securitate a rețelelor și a sistemelor de informații din Republica Slovenia, care sunt esențiale pentru buna funcționare a statului și activităților economice ale statului[32]. Acesta stabilește cerințe minime de securitate și cerințe de notificare a incidentelor pentru cei responsabili. De asemenea, reglementează competențele, sarcinile, organizarea și funcționarea autorității naționale competente pentru securitatea informațiilor, punctele unice de contact pentru securitatea informațiilor, echipele naționale de rezolvare a incidentelor de securitate, etc.

Persoanele răspunzătoare conform legii sunt:

- furnizori de servicii esențiale;
- furnizorii de servicii digitale;
- organele administrației de stat care gestionează sistemele informaționale și părți ale rețelei sau furnizează servicii de informare necesare bunei funcționări a statului sau pentru asigurarea securității naționale.

Furnizorii de servicii esențiale sunt entități care își desfășoară activitatea în următoarele domenii:

1. energie
2. infrastructură digitală
3. alimentarea și distribuția apei potabile
4. sănătate
5. trafic
6. sistemul bancar
7. infrastructura pieței financiare
8. aprovizionarea cu alimente
9. protecția mediului.

Furnizorii de servicii esențiale trebuie să asigure un nivel înalt de securitate a rețelelor și sistemelor informaționale, trebuie să realizeze și să mențină un sistem documentat de management al securității informațiilor și un sistem de management al continuității activității, care trebuie să includă cel puțin:

- o analiză a managementului riscului cu o evaluare a nivelului acceptabil de risc;
- politica de continuitate a afacerii cu planul de management al acesteia;
- o listă a sistemelor de informare cheie, de control și monitorizare a rețelelor și a datelor asociate care sunt de importanță deosebită pentru funcționarea serviciilor esențiale;
- planul de reînnoire și restabilire a sistemelor informaționale menționate mai sus;
- planul de răspuns la incidente cu un protocol național de notificare CSIRT;

[32] http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707

- planul de măsuri de securitate pentru a asigura integritatea, confidențialitatea și disponibilitatea rețelelor și a sistemelor informatice care țin seama de specificitățile sectoriale.

Furnizorii de servicii digitale identifică și adoptă măsuri tehnice și organizatorice adecvate și proporționale pentru a gestiona riscurile de securitate ale rețelelor și sistemelor de informații pe care le utilizează, pentru a furniza aceste servicii în UE. Ținând cont de stadiul tehnicii, aceste măsuri trebuie să asigure un nivel de securitate al rețelelor și sistemelor informaționale adecvat riscului existent. Acestea iau în considerare următoarele elemente:

- securitatea sistemelor și instalațiilor;
- managementul incidentelor;
- managementul continuității afacerii, monitorizarea, auditarea și testarea;
- conformitatea cu standardele internaționale.

Furnizorii de servicii digitale iau măsuri corespunzătoare pentru a preveni și a reduce impactul incidentelor care pun în pericol securitatea rețelelor și sistemelor lor de informații în ceea ce privește serviciile pe care le furnizează în UE, pentru a asigura continuitatea acestor servicii.

Furnizorii de servicii digitale notifică CSIRT național, fără o întârziere nejustificată, orice incident care are un impact semnificativ asupra furnizării acelor servicii pe care le oferă în UE. Notificarea include informații pe baza cărora CSIRT național poate determina semnificația potențialului impact transfrontalier. Obligația de a raporta un incident se aplică numai atunci când furnizorul de servicii digitale are acces la informațiile necesare pentru a evalua impactul incidentului.

CSIRT națională notifică incidentul autorității naționale competente, care deține o listă a incidentelor produse. Autoritatea națională competentă informează imediat poliția și Centrul național de gestionare a crizelor cu privire la un incident care ar putea avea un impact mai mare sau ar putea provoca o deteriorare a stabilității securității naționale a Republicii Slovenia pe termen lung.

La determinarea gradului de impact al incidentului se iau în considerare următorii parametri:

- numărul de utilizatori afectați de incident, în special utilizatorii dependenți de servicii în furnizarea propriilor servicii;
- durata incidentului;
- distribuția geografică în ceea ce privește zona afectată de incident;
- măsura în care funcționarea serviciului este perturbată;
- amploarea impactului asupra activităților economice și sociale.

Persoanei juridice (societate mică) care furnizează servicii i se pot aplica sancțiuni, respectiv amendă de la 500 la 10.000 euro, iar unei persoane juridice (societate mare) o amendă de la 10.000 la 50.000 euro, dacă nu îndeplinesc atribuțiile stabilite de lege.

SUEDIA

Eforturile de securitate cibernetică sunt necesare pentru a permite societății să funcționeze și să se dezvolte în conformitate cu obiectivele diferitelor domenii de politică. Transformarea digitală înseamnă că în proporție din ce în ce mai mare, toate activitățile din societate depind în diferite grade de rețelele și sistemele informaționale și, prin urmare, de securitatea cibernetică[33].

Strategia de securitate cibernetică se bazează pe obiectivele stabilite pentru securitatea Suediei:

- protejarea vieții și a sănătății populației;
- funcționarea societății pentru a susține valori fundamentale precum democrația, statul de drept și drepturile și libertățile omului;
- Suedia trebuie să devină un lider mondial în valorificarea oportunităților oferite de transformarea digitală.

Cadrul legal este reprezentat de cerințele de securitate a informațiilor prevăzute în Ordonanța (2015:1052) privind măsuri ale autorităților responsabile de pregătire și supraveghere pentru situații de urgență, Legea arhivelor (1990:782), Legea datelor cu caracter personal (1998:204) și Legea comunicațiilor (2003:389).

Pentru a reduce vulnerabilitățile și pentru a promova obiectivele de securitate și IT ale Suediei, evaluările guvernului privesc:

- asigurarea unei abordări sistematice și cuprinzătoare în eforturile de securitate cibernetică;
- îmbunătățirea securității rețelelor, a produselor și a sistemului cibernetic, în general;
- îmbunătățirea capacității de a preveni, detecta și gestiona atacurile cibernetice și alte incidente IT;
- creșterea posibilității de prevenire și combatere a criminalității informatice;
- creșterea cunoștințelor și promovarea expertizei în domeniu;
- consolidarea cooperării internaționale;
- asigurarea că activitățile au nevoie de o monitorizare continuă, cu nevoi speciale de protecție;
- asigurarea dezvoltării și consolidării continue a unui sistem eficient de apărare cibernetică fără întreruperi, cu capacitatea de a preveni, detecta și gestiona atacuri cibernetice, atât pentru activitățile militare, cât și cele civile.

[33] https://www.government.se/4ada5d/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213

SPANIA

Prin Ordinul PRA/33/2018 a fost reglementată activitatea Consiliului național de securitate cibernetică[34].

Consiliul exercită următoarele atribuții:

1. propune liniile directoare pentru planificarea și coordonarea politicii de securitate națională referitoare la securitatea cibernetică.
2. contribuie la consolidarea bunei funcționări a Sistemului național de securitate în domeniul securității cibernetice.
3. verifică gradul de conformitate cu Strategia de securitate națională și propune, după caz, revizuirea acesteia, în raport cu securitatea cibernetică.
4. contribuie la pregătirea propunerilor de reglementare pentru consolidarea Sistemului național de securitate.
5. consolidează relațiile cu administrațiile publice implicate în domeniul securității cibernetice, precum și coordonarea, colaborarea și cooperarea între sectorul public și cel privat.
6. efectuează evaluarea riscurilor și amenințărilor, analizează posibilele scenarii de criză, în special cele susceptibile să conducă la o situație de interes pentru securitatea națională, în domeniul securității cibernetice, și evaluează rezultatele privind acestora, în coordonare cu organele și autoritățile competente.

Decretul regal nr. 12/2018[35] se aplică:

a) serviciilor esențiale dependente de rețelele și sistemele informatice cuprinse în sectoarele strategice definite în anexa la Legea 8/2011, care stabilește măsuri de protecție a infrastructurilor critice.
b) serviciilor digitale, care sunt piețele online, motoarele de căutare online și serviciile de *cloud computing*.

Autoritățile competente au următoarele atribuții:

a. supraveghează respectarea de către operatorii de servicii esențiale și furnizorii de servicii digitale a obligațiilor determinate, în conformitate cu prevederile legale.
b. stabilește canale de comunicare adecvate cu operatorii de servicii esențiale și cu furnizorii de servicii digitale care, după caz, vor fi dezvoltate prin regulament.
c. coordonarea cu CSIRT-urile de referință prin protocoale de acțiune care, după caz, vor fi elaborate prin regulament.
d. primește sesizări despre incidente IT, prin intermediul CSIRT-urilor de referință.

[34] https://www.boe.es/buscar/act.php?id=BOE-A-2018-799
[35] https://www.boe.es/buscar/act.php?id=BOE-A-2018-12257

e. informează Punctul unic de contact cu privire la sesizările de incidente prezentate în cuprinsul legii.
f. informează, după caz, publicul cu privire la anumite incidente, atunci când difuzarea acestor informații este necesară pentru a evita alte incidente mai grave.
g. cooperează, în sfera de aplicare a prezentului decret regal-lege, cu autoritățile competente în materie de protecție a datelor cu caracter personal, securitate publică, securitate cetățenească și securitate națională, precum și cu autoritățile sectoriale corespunzătoare.
h. stabilește obligații specifice de garantare a securității rețelelor și sistemelor informatice și de notificare a incidentelor.
i. promovează utilizarea standardelor și specificațiilor tehnice.

Echipele de răspuns la incidente de securitate informatică (CSIRT) de referință în domeniul securității rețelelor și sistemelor informatice sunt următoarele:

a) în ceea ce privește relațiile cu operatorii de servicii esențiale:

1. CCN-CERT - Centrul criptologic național;

2. INCIBE-CERT - Institutul național de securitate cibernetică din Spania;

3. ESPDEF-CERT - Ministerul Apărării, care va coopera cu CCN-CERT și INCIBE-CERT în acele situații pe care le consideră în sprijinul operatorilor de servicii esențiale.

Obligațiile furnizorilor de servicii digitale sunt comune cu cele menționate în alte state.

Pentru săvârșirea de infracțiuni se pot aplica următoarele sancțiuni:

a. pentru săvârșirea de infracțiuni foarte grave, amendă de la 500.001 la 1.000.000 euro.
b. pentru săvârșirea de infracțiuni grave, amendă de la 100.001 la 500.000 euro.
c. pentru săvârșirea de contravenții, amendă de până la 100.000 euro.

În stabilirea cuantumului sancțiunilor, organul competent va ține cont de următoarele criterii:

- gradul de vinovăție sau existența intenției.
- continuitatea sau persistența comportamentului inadecvat.
- natura și cuantumul prejudiciului cauzat.
- recidiva, prin săvârșirea în ultimul an a mai multor infracțiuni de aceeași natură, atunci când aceasta a fost declarată prin rezoluție fermă în procedură administrativă.
- numărul de utilizatori afectați.
- volumul de facturare al persoanei responsabile.
- acțiunile întreprinse de responsabil pentru atenuarea efectelor sau consecințelor infracțiunii, etc.

UNGARIA

Ciberspațiul reprezintă fenomenul combinat de interconectare globală, sisteme informatice electronice descentralizate și în continuă creștere, precum și procesele societale și economice care apar în și prin aceste sisteme în formă de date și informații[36].

Numărul tot mai mare și diversele surse de amenințări care apar în spațiul cibernetic, precum și ordinul crescând de mărime al consecințelor lor indică faptul că numărul și eficiența utilizatorilor publici și non-publici a crescut rapid în ultimul deceniu, existând actori care utilizează spațiul cibernetic pentru a obține ilegal date sau informații critice, pentru a perturba sistemele de comunicare și informare.

Securitatea cibernetică este activitatea continuă și planificată de acțiuni politice, juridice, economice, măsuri educaționale, de conștientizare și tehnice pentru gestionarea riscurilor în spațiul cibernetic.

Ungaria deține deja majoritatea instrumentelor necesare pentru a-și îndeplini obiectivele strategice:

a) inventarierea și coordonarea organizațiilor guvernamentale responsabile pentru securitatea spațiului cibernetic maghiar, înființarea unor sisteme eficiente de cooperare;
b) trecerea în revistă a societății civile, organizațiilor de afaceri și academice responsabile pentru securitatea spațiului cibernetic maghiar;
c) inventarierea infrastructurilor informaționale critice și a activelor critice ca active naționale de date și asigurarea protecției acestora;
d) funcționarea instituțiilor guvernamentale specializate;
e) asigurarea unui cadru de reglementare;
f) participarea la cooperarea internațională și regională la nivel politic;
g) stabilirea unui cadru de sprijin pentru cercetare și dezvoltare, educație și conștientizare din partea publicului;
h) stabilirea sistemelor de motivare a afacerilor;
i) integrarea aspectelor de securitate cibernetică în dezvoltările tehnice aflate în subordinea statului.

[36] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Hungary

BIBLIOGRAFIE

- https://www.bundeskanzleramt.gv.at/themen/cybersicherheit/oesterreichische-strategie-fuer-cybersicherheit.html
- https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010536
- https://economie.fgov.be/fr/file/2154/download?token=bWnBTZgR
- https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_FR_DP2.pdf
- https://etaamb.openjustice.be/fr/loi-du-07-avril-2019_n2019011507.html
- https://www.zakonyprolidi.cz/cs/2017-205
- https://cybersecurity.cz/law.html
- https://nukib.cz/cs/infoservis/aktuality/1742-nukib-vydava-prvni-dve-cloudove-vyhlasky/
- https://www.mvcr.cz/clanek/egovernment-cloud.aspx
- https://www2.deloitte.com/hr/hr/pages/audit/articles/kiberneticka-sigurnost.html
- https://www.zakon.hr/z/1041/Zakon-o-kiberneti%C4%8Dkoj-sigurnosti-operatora-klju%C4%8Dnih-usluga-i-davatelja-digitalnih-usluga
- https://rdd.gov.hr/UserDocsImages/dokumenti/Strategija_e-Hrvatska_2020.pdf
- https://narodne-novine.nn.hr/clanci/sluzbeni/full/2018_07_64_1305.html
- https://www.fmn.dk/da/nyheder/2019/2019/telesektoren-styrker-samfundets-robusthed-med-ny-sektorstrategi-for-cyber--og-informationssikkerhed/
- https://digst.dk/strategier/cyber-og-informationssikkerhed/
- https://vm.fi/documents/10623/307681/Digitaalisen+turvallisuuden+kansainv%C3%A4linen+vertailu/7aafe82e-86e7-7450-358c-f1adfeecb3e5/Digitaalisen+turvallisuuden+kansainv%C3%A4linen+vertailu.pdf
- https://trustpair.fr/blog/cybersecurity-act-la-loi-europeenne-sur-la-cybersecurite/

- https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045294275
- https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf
- https://www.linklaters.com/en/insights/publications/2018/march/cyber-securite
- https://www.numerique.gouv.fr/uploads/Strategie-nationale-pour-le-cloud.pdf
- https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=B32CFA9B-74D2-411D-A501-82041939FC67&filename=1002%20-%20Le%20Gouvernement%20annonce%20sa%20strat%C3%A9gie%20nationale%20pour%20le%20Cloud.pdf
- https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2022/01/1617_-_dossier_de_presse_-_strategie_nationale_pour_le_cloud_.pdf
- https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Greece_2019.pdf
- https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1652954229494
- https://www.reuters.com/article/deutschland-digitalisierung-idDEKBN1X820Y
- http://copyrightblog.kluweriplaw.com/2018/09/15/italy-adopts-first-rules-cloud-service-providers-possible-next-steps-including-eu-level/#:~:text=Starting%20from%2020th%20November,Privacy%20and%20Protection%20of%20data).
- https://docs.italia.it/italia/cloud-italia/strategia-cloud-italia-docs/it/stabile/index.html
- https://www.heraldo.es/noticias/aragon/2022/04/20/aragon-tendra-una-ley-cloud-pionera-en-europa-con-ayudas-a-empresas-y-mas-formacion-de-profesionales-1568448.html
- https://aecconsultoras.com/noticias-sectoriales/aragon-aprueba-el-proyecto-de-ley-de-tecnologias-en-la-nube-para-acelerar-la-transformacion-digital/
- https://www.consilium.europa.eu/hu/policies/cybersecurity/
- https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010536
- https://etaamb.openjustice.be/fr/loi-du-07-avril-2019_n2019011507.html

- https://www.mlsp.government.bg/uploads/3/zakonodatelstvo/za-kibersigurnost.pdf
- https://www.zakonyprolidi.cz/cs/2014-181
- https://narodne-novine.nn.hr/clanci/sluzbeni/2018_07_64_1305.html
- https://www.retsinformation.dk/eli/lta/2019/836
- https://www.riigiteataja.ee/akt/122052018001
- https://www.ria.ee/et/uudised/mkm-valitsus-ajakohastab-kuberruumi-kaitse-eesmargil-kuberturvalisuse-seadust.html
- https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/
- https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf
- https://www.linklaters.com/en/insights/publications/2018/march/cyber-securite
- https://www.platis-anastassiadis.com/en_gr/law-alerts/l-4577-2018-new-cybersecurity-obligations-for-essential-and-digital-services
- https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1652954229494
- https://focus.namirial.it/cyber-security-legge/#:~:text=%C3%88%20stata%20pubblicata%20in%20Gazzetta,82
- https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/15e540727ac211e89188e16a6495e98c
- https://open.overheid.nl/repository/ronl-ec4dde7f-d0b3-46dc-83f7-174c42584100/1/pdf/tk-bijlage-overzicht-wet-en-regelgeving-cybersecurity.pdf
- https://wetten.overheid.nl/BWBR0041515/2022-05-01
- https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/U/D20181560Lj.pdf
- https://dre.pt/dre/detalhe/lei/46-2018-116029384
- https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/
- https://www.boe.es/buscar/act.php?id=BOE-A-2018-799
- https://www.boe.es/buscar/act.php?id=BOE-A-2018-12257

- https://net.jogtar.hu/jogszabaly?docid=A2100805.KOR
- https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf
- https://likumi.lv/ta/id/220962-informacijas-tehnologiju-drosibas-likums
- https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf
- https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=173&modo=2&nota=0&tab=2
- https://www.gov.si/assets/ministrstva/MJU/DID/Strategija-kibernetske-varnosti.pdf
- http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707
- https://rechtenoverheid.nl/files/2013-09/Sjerps_Cloud%20Computing%20en%20Gegevensbescherming.pdf
- https://www.cncs.gov.pt/pt/estrategia-nacional/
- https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Narodna-strategia-kybernetickej-bezpecnosti.pdf
- https://www.slov-lex.sk/legislativne-procesy/-/SK/LP/2017/260/pripomienky/COO-2145-1000-3-1952023