DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

ORDIN

privind aprobarea politicilor de confidențialitate și transparență ale Platformei Naționale pentru Raportarea Incidentelor de Securitate Cibernetică

Decembrie 2023

Având în vedere dispozițiile Art. 20 (3) și Art. 52 (3) al Legii nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, și Art. 5 lit. c) pct. 12 și Art. 7 alin. (3) și alin. (4) din Ordonanța de urgență a Guvernului nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, aprobată cu modificări și completări prin Legea nr. 11/2022,

Directorul Directoratului Național de Securitate Cibernetică emite prezentul ordin:

Art. 1 Se aprobă politicile de confidențialitate și transparență ale Platformei Naționale pentru Raportarea Incidentelor de Securitate Cibernetică, denumită în continuare ”PNRISC” sau ”platforma”, prevăzute în anexa la prezentul Ordin.

Art. 2 Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

ANEXA

Politicile de confidențialitate și transparență ale PNRISC

Art. 1 Aplicabilitate

Prezentele politici de confidențialitate și transparență ale PNRISC stabilesc cadrul legal pentru exercitarea activităților de colectare și procesare a datelor și informațiilor privind incidentele de securitate cibernetică ce fac obiectul raportării în platformă, precum și liniile directoare menite a asigura confidențialitatea și transparența atunci când se partajează date și informații care fac obiectul raportării către autoritățile competente, prevăzute la art. 10 alin (1) din Legea 58/2023.

Art. 2 Principii ale partajării datelor

(1) Partajarea datelor prin intermediul PNRISC se face în conformitate cu prevederile art. 23 din Legea 58/2023 privind responsabilitățile autorităților competente de a asigura coordonarea managementului incidentelor de securitate cibernetică, respectiv de a acorda sprijin, la cerere, proprietarilor, administratorilor, posesorilor și/sau utilizatorilor de rețele și sisteme informatice aflate în domeniul lor de competență, activitate sau responsabilitate, în scopul adoptării de măsuri reactive de primă urgență pentru remedierea efectelor incidentelor de securitate cibernetică.

(2) Partajarea datelor prin intermediul PNRISC respectă principiul colaborării, cooperării și coordonării constând în realizarea, în mod conjugat, de către persoanele fizice sau juridice responsabile, a tuturor activităților care să asigure securitatea și/sau apărarea sistemelor, rețelelor și serviciilor informatice care fac obiectul Legii 58/2023.

(3) Partajarea datelor și informațiilor prin intermediul PNRISC respectă principiul necesității și proporționalității, respectiv se vor partaja numai datele necesar a fi cunoscute de autoritățile competente, în conformitate cu atribuțiile și domeniile de competență ale acestora, conform legii.

(4) Partajarea datelor și informațiilor prin intermediul PNRISC respectă nevoia de asigurare a confidențialității, în vederea protejării intereselor persoanelor prevăzute la art. 3 alin. (1) din Legea nr.58/2023, care au obligația de a notifica incidentele de securitate cibernetică prin intermediul PNRISC.

(5) Autoritățile competente stabilite prin art. 10 din Legea 58/2023 au acces, în temeiul art. 20 alin.(2) din Legea 58/2023, în vederea asigurării managementului incidentelor, rezilienței în spațiul cibernetic și îndeplinirii responsabilităților care le revin, la următoarele categorii de date din PNRISC:

a) Directoratul Național de Securitate Cibernetică (DNSC), la toate raportările de incidente de securitate cibernetică care privesc spațiul cibernetic civil;

b) Ministerul Cercetării, Inovării și Digitalizării (MCID), la raportările de incidente de securitate cibernetică ce afectează sau pot afecta rețelele și sistemele informatice proprii;

c) Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM), la raportările de incidente de securitate cibernetică ce afectează sau pot afecta rețelele și sistemele informatice proprii și a celor prevăzute la art. 3 alin. (1) lit b) din Legea 58/2023 și a spectrului de frecvențe radio neguvernamental;

d) Ministerul Afacerilor Externe (MAE), la raportările de incidente de securitate cibernetică ce afectează sau pot afecta rețelele și sistemele informatice din responsabilitate;

e) Ministerul Apărării Naționale (MApN), la raportările de incidente de securitate cibernetică ce afectează sau pot afecta rețelele și sistemele informatice care susțin capabilitățile militare de apărare;

f) Ministerul Afacerilor Interne (MAI), la raportările de incidente de securitate cibernetică ce afectează sau pot afecta rețelele și sistemele informatice din domeniul său de competență;

g) Serviciul Român de Informații (SRI), la raportările de incidente de securitate cibernetică ce afectează sau pot afecta rețelele și sistemele informatice proprii, precum și raportările privind orice alte incidente asociate unor amenințări, riscuri și vulnerabilități la adresa securității naționale a României care pot sprijini îndeplinirea atribuțiilor de autoritate competentă la nivel național în domeniul cyberintelligence;

h) Serviciul de Informații Externe (SIE), la raportările de incidente de securitate cibernetică care reprezintă amenințări, riscuri și vulnerabilități cibernetice la adresa rețelelor și sistemelor informatice din responsabilitate;

i) Serviciul de Telecomunicații Speciale (STS), la raportările de incidente de securitate cibernetică ce afectează sau pot afecta infrastructurile, rețelele, sistemele, serviciile proprii și spectrul de frecvențe radio proprii, precum și pentru cele reglementate prin legi speciale;

j) Serviciul de Protecție și Pază (SPP), la raportările de incidente de securitate cibernetică ce afectează sau pot afecta pentru infrastructurile, rețelele, sistemele și serviciile proprii, precum și cele care pot afecta securitatea demnitarilor;

k) Oficiul Registrului Național al Informațiilor Secrete de Stat (ORNISS), la raportările de incidente de securitate cibernetică ce afectează sau pot afecta rețelele și sistemele informatice proprii, precum și cele care afectează sau pot afecta securitatea informațiilor clasificate.

(6) Autoritatile competente menționate la alin. (5) pot avea acces suplimentar, individual sau în comun, la:

a) informații cu caracter general sau statistic în format anonimizat (tendințe, tipuri de atacuri, tehnici, tactici și proceduri identificate, vulnerabilități frecvent exploatate, sectoare afectate, indicatori de compromitere) provenite din PNRISC, în vederea prevenirii, informării și fundamentării luării deciziilor, conform competențelor proprii;

b) seturile de date care vizează în mod direct autoritățile sau care pot afecta starea de securitate a acestora.

Art. 3 Confidențialitatea, integritatea și disponibilitatea

(1) Pentru îndeplinirea responsabilităților care le revin, autoritățile care au acces la PNRISC asigură confidențialitatea, integritatea și disponibilitatea datelor partajate.

(2) Autoritățile care au acces la PNRISC tratează toate datele primite ca fiind confidențiale și acordă accesul la date doar personalului autorizat în acest sens pentru a-și îndeplini îndatoririle de serviciu.

(3) În cazul unei încălcări a confidențialității sau afectări a integrității ori disponibilității, autoritatea competentă care a detectat încălcarea notifică imediat Directoratul Național de Securitate Cibernetică și aplică toate măsurile necesare pentru a atenua sau remedia situația.

Art. 4 Transparența

(1) DNSC păstrează un jurnal al tuturor activităților de partajare a datelor efectuate prin intermediul PNRISC, incluzând data începerii partajării, tipul de date partajate, precum și identitatea autorității competente ce are acces la date.

(2) DNSC revizuiește periodic activitățile de partajare a datelor prin PNRISC pentru a asigura conformitatea cu aceste politici.

(3) DNSC publică un raport anual de transparență privind activitățile de raportare și partajare datelor și informațiilor prin intermediul PNRISC, fără a dezvălui informații sensibile sau confidențiale.

Art. 5 Măsuri minimale de asigurare a confidențialității, integrității și disponibilității datelor partajate prin PNRISC

(1) Datele și informațiile raportate și partajate prin intermediul PNRISC sunt protejate din punct de vedere al confidențialității, integrității și disponibilității cel puțin prin aplicarea următoarelor măsuri:

a. Separarea logică a informațiilor introduse în PNRISC;

b. Jurnalizarea accesului, a activităților utilizatorilor și a activităților de administrare a PNRISC;

c. Efectuarea accesului utilizatorilor pe bază de roluri;

d. Folosirea autentificării multi-factor;

e. Salvarea fișierelor jurnal incremental într-o zonă „read-only”, în vederea realizării analizei lor periodice în scopul identificării unor eventuale riscuri;

f. Implementarea unei politici de backup și reziliență;

g. Auditare de securitate anuală a platformei;

h. Verificarea și validarea periodică a politicii de „cookies” a platformei;

i. Testare de securitate după fiecare actualizare majoră, sau în funcție de necesități.

(2) DNSC are obligația de a implementa și a verifica masurile de protecție prevăzute la alin. (1).

Art. 6 Scop și păstrare

(1) Datele și informațiile raportate și partajate prin intermediul PNRISC se vor utiliza exclusiv în scopul consolidării securității cibernetice, în condițiile Legii 58/2023.

(2) Datele și informațiile din PNRISC nu se păstrează mai mult decât este necesar pentru a atinge scopul pentru care au fost partajate. După atingerea scopului, datele vor fi șterse în siguranță.

Art. 7 Supraveghere și responsabilitate

(1) Rolul de supraveghere, monitorizare și revizuire a practicilor de gestionare și partajare a datelor și informațiilor prin intermediul PNRISC și asigurare a conformității cu aceaste politici este îndeplinit de un expert din cadrul uneia dintre autoritățile competente prevăzute la art. 10 alin (1) din Legea 58/2023,

(2) Expertul prevăzut la alin. (1) este desemnat de către Directorul DNSC cu avizul Consiliului Operativ de Securitate Cibernetică (COSC).

(3) Expertul desemnat nu poate efectua niciun fel de alte activități de serviciu legate de PNRISC, cu excepția celor de la alin.1.

(4) Expertul desemnat întocmește și înaintează către COSC un raport anual privind transparența și confidențialitatea PNRISC. Raportul va include, după caz, recomandări și propuneri de îmbunătățire a măsurilor privind transparența și confidențialitatea PNRISC.

(5) Autoritățile competente au obligația să implementeze în cel mai scurt timp recomandările și propunerile de îmbunătățire transmise prin intermediul raportului anual și să înștiințeze COSC cu privire la măsurile adoptate.

FINALUL DOCUMENTULUI