HOTĂRÎRE GUVERN Nr. 201 din 28.03.2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică

Publicat : 07.04.2017 în Monitorul Oficial Nr. 109-118 art Nr : 277

Baza legală

- Legea nr. 467-XV din 21 noiembrie 2003 cu privire la informatizare şi la resursele informaţionale de stat
- Legea nr. 71-XVI din 22 martie 2007 cu privire la registre
- Programului naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, aprobat prin Hotărîrea Guvernului nr. 811 din 29 octombrie 2015

Guvernul HOTĂRĂŞTE

- Cancelaria de Stat, ministerele şi alte autorităţi administrative centrale subordonate Guvernului şi structurile organizaţionale din sfera lor de competenţă, autoritățile administrative autonome și unităţile cu autonomie financiară, în termen de pînă la 31 decembre 2017, vor asigura implementarea Cerințelor minime obligatorii de securitate cibernetică

Cerințele minime, după domeniul de aplicare, sînt de două categorii:

- nivelul 1 – de securitate cibernetică de bază (utilizare TIC în activitatea instituției);
- nivelul 2 – de securitate cibernetică avansată (utilizare TIC în activitatea instituției și prestare servicii bazate pe TIC).

I. DISPOZIȚII GENERALE

- *autentificare multifactorială* – autentificare cu cel puțin doi factori de autentificare independenți;
- *cerințe minime obligatorii de securitate cibernetică* – sistemul de management al securității cibernetice – toate politicile, procedurile, planurile, procesele, practicile, rolurile, responsabilitățile, resursele și structurile care sînt folosite pentru a proteja și păstra intactă informaţia;
- *paravan de protecție (firewall)* – un dispozitiv sau o serie de dispozitive configurate în așa fel încît să filtreze, să cripteze sau să intermedieze traficul dintre diferite domenii de securitate pe baza unor reguli predefinite;
- *actualizare* – procedeu de modificare a unor fișiere și aplicații ale calculatorului sau crearea unor noi;
- *protecție malware* – măsură tehnică de securitate, efectuată prin folosirea de programe antivirus, în scopul protecției cibernetice;
- *antispyware* – măsură tehnică de securitate, efectuată prin folosire de programe, în scop de prevenire a intruziunii cibernetice;
- *test de penetrare* – evaluare a securității cibernetice a unui sistem împotriva diferitor tipuri de atacuri.

II. ORGANIZAREA SISTEMULUI INTERN DE SC

- Conducătorul autorității poartă răspundere pentru asigurarea securității cibernetice în instituție.
- Conducătorul autorității desemnează, prin act administrativ, persoana (subdiviziunea) responsabilă de punerea în aplicare a sistemului de management al securității cibernetice în instituție și prezintă M TIC informația respectivă în termen de cinci zile lucrătoare de la desemnarea acesteia.

Persoana responsabilă are următoarele atribuții:

- organizează SMSC în instituție;
- participă, cel puțin o dată pe an, la cursurile de formare organizate de M TIC privind securitatea cibernetică și, respectiv, organizează cursuri pentru angajații instituției;
- asigură elaborarea, implementarea și respectarea prevederilor următoarelor documente (revizuit cel puțin o dată pe an):
  - planul de acțiuni pentru asigurarea SC al instituției,
  - politica de securitate cibernetică a instituției,
  - planul de instruire și responsabilizare în SC a personalului,
  - regulamentele interne de securitate cibernetică,
  - procedurile de recuperare.

Politica de SC, în calitate de document instituțional, include:

- scopul și obiectivele;
- principiile de organizare internă a managementului de securitate cibernetică;
- analiza situației și vulnerabilităților (disponibilitate, integritate și confidențialitate a datelor, precum și analiza riscurilor și căilor de remediere);
- declaraţia managementului instituției de susţinere a scopului şi principiilor securităţii cibernetice în instituție.

Planul de instruire și responsabilizare în SCa personalului instituției include:

- instruirea privind etica cibernetică (programe/cursuri de formare în domeniul securității cibernetice);
- măsurile de securitate internă privind activitatea personalului (autorizație de acces, stabilirea drepturilor, obligațiilor, restricțiilor, responsabilizarea angajaților, monitorizarea, proceduri de asistență ale utilizatorilor în cazuri de urgență);
- măsurile de securitate privind activitatea personalului/companiilor externe cooptate (coordonarea responsabilităților, acorduri de nedivulgare, autorizație de acces, monitorizare, planul de contingență (intervenție) pentru suspendarea operațiunilor de externalizare).

Regulamentele interne de securitate cibernetică prevăd:

- dezvoltarea, actualizarea, modificarea, mentenanța sistemelor informaționale;
- gestionarea activelor și facilităților de comunicații electronice și tehnologia informației;
- stocarea copiilor de rezervă ale datelor, precum şi ale procedurilor de control;
- păstrarea datelor de acces, de jurnalizare a activităților;
- monitorizarea securităţii sistemului;
- regulile de gestionare a evenimentelor de securitate;
- procedurile de utilizare a datelor în cazuri excepționale (de urgență) ;
- procedurile de evaluare a securității cibernetice.

Procedurile de recuperare includ:

- stabilirea procedurilor privind copierea de rezervă și de recuperare în cazul unui incident de securitate cibernetică;
- descrierea acțiunilor măsurabile de recuperare;
- atribuirea responsabilităților pentru restabilirea funcționalităților;
- stabilirea procedurilor de notificare.

III. CERINȚELE MINIME OBLIGATORII DE SECURITATE CIBERNETICĂ DE NIVELUL 1 (UTILIZAREA TIC ÎN ACTIVITATEA INSTITUȚIEI)

Controlul accesului

1) drepturile, obligațiile, restricțiile și responsabilitățile utilizatorilor urmează a fi stabilite de către persoana responsabilă de proces și comunicat într-o formă stabilită responsabilului/subdiviziunii de securitate cibernetică;

2) persoana care desfășoară activități de administrare a sistemului utilizează conturi diferite pentru funcții de administrare și funcții de utilizator;

3) fiecare cont de utilizator este asociat cu o persoană anumită. În cazul în care sistemul prevede neadmiterea utilizării acestor conturi de către alte persoane, atunci sistemul trebuie să includă mijloace tehnice speciale, care să nu admită utilizarea acestor conturi de către persoane terțe;

4) în cazul în care sistemul nu este utilizat pentru autentificarea multifactorială, adică nu este un atribut de o natură statică (de exemplu, simbolic, un mesaj de cod-text de unică folosință), dar este un atribut de altă natură, utilizatorii sistemului trebuie să utilizeze o parolă;

5) utilizatorul sistemului trebuie să folosească în calitate de parolă o combinație din numere (0-9), caractere latine (minuscule și majuscule) și simboluri speciale (!#%), constituită din numărul minim de caractere, stabilit prin regulamentul intern de securitate, dar nu mai puțin de 7 caractere;

6) se interzice stocarea electronică și transportarea în formă necriptată a parolelor utilizatorilor sistemului, inclusiv a procesului de autentificare a utilizatorilor. Se admite transportarea acestora prin rețea publică necriptată doar în cazul utilizării unei parole de o singură folosință, cu o valabilitate de 48 de ore de la momentul transmiterii acestora;

7) sistemul trebuie să dispună de mecanisme de gestiune a parolelor, precum şi să asigure autentificarea şi identificarea utilizatorului pentru o perioadă limitată de timp;

8) nu se admite utilizarea în echipamentele și produsele program a parolelor implicite (de la producător);

9) datele despre activitățile în sistem (jurnalizarea) se stochează în timp real şi se păstrează pe perioada stabilită prin regulamentul intern de securitate, dar nu mai puțin de 6 luni;

10) orice activitate în sistem trebuie să poată fi identificată într-un anumit cont de utilizator sau adresă IP;

11) managementul drepturilor de utilizator trebuie să asigure ca fiecare utilizator să poată face uz doar de drepturile sale. Verificarea activităților în sistem se realizează periodic, la etape de timp stabilite conform regulamentului intern de securitate, dar nu mai rar de o dată la 6 luni;

12) managementul controlului accesului trebuie să fie setat ca să permită acces autorizat din rețea externă prin Internet doar cu o parolă de o singură folosință, inclusiv prin semnătura electronică din cadrul serviciului electronic guvernamental de autentificare şi control al accesului (MPass).

Securitatea fizică

- delimitarea clară a perimetrului rezervat diferitor grupuri de echipamente IT, alcătuirea planurilor camerelor de servere și a rețelelor;
- asigurarea condițiilor de încălzire, ventilare și aer condiționat a încăperilor specializate;
- asigurarea accesului în spațiile specializate strict conform competențelor;
- asigurarea securității energetice prin utilizarea unor dispozitive conforme normativelor în vigoare și cu protecție la suprasarcină;
- asigurarea mentenanței adecvate, conform cerințelor tehnice;
- evidența echipamentelor și produselor program, utilizare în cadrul instituției.

Securitatea operațională

1) echipamentele și produsele program trebuie să fie protejate ca să asigure operaționalitatea sistemelor;
2) pe calculatoarele conectate la reţeaua Internet trebuie să fie instalat cel puțin (SO cu actualizările curente aplicate; program antivirus activat și actualizat; firewall activat; blocare automată a sistemului în caz de neutilizare a acestuia - screen saver, log-off);
3) controlul tehnic se efectuează periodic, conform regulamentului intern de securitate, și vizează:
4) aplicarea cerințelor de securitatea cibernetică la utilizarea rețelelor:
5) elaborarea planului de continuitate, care va asigura restaurarea caracteristicilor sistemului și a datelor în caz de incident de securitate, care să includă:
6) stabilirea mecanismului de scoaterea din uz a echipamentelor, distrugerea datelor ce le conțin și reutilizarea lor;
7) stabilirea cerințelor de securitate și restricții pentru echipamentele personale utilizate în cadrul instituției.

Schimbul securizat de date și de comunicări

- aplicarea ghidului de utilizare a serviciilor sistemului de poștă electronică, aprobat ca document tehnic pentru toate autoritățile sus-menționate, și obligarea personalului privind:
  a) verificarea chenarului cu adrese înainte de expediere a corespondenței și a destinatarului, pentru a evita erorile;
  b) precauția față de conținutul mesajelor recepționate, verificarea datelor expeditorului/companiei, în mod special a celor de la expeditori necunoscuți, privind eventuala falsificare a identității pentru a ascunde adevărata sa origine;
  c) verificarea și scanarea antivirus a anexelor la mesaje recepționate și a extensiilor acestora;
- interzicerea:
  a) redirecționării automate a mesajelor din poșta de serviciu spre alte conturi personale/private;
  b) utilizării poștei electronice de serviciu pentru a expedia sau redirecționa mesaje considerate obscene, amenințătoare, ofensatoare, calomnioase, defăimătoare, rasiste, pornografice, de hărțuire, de ură, remarci discriminatorii și alte mesaje antisociale;
  c) transmiterii/retransmiterii în lanț a mesajelor cu divers conținut irelevant pentru activitatea de serviciu;
  d) utilizării poștei electronice de serviciu pentru obţinerea unui cîștig material, în scopuri personale, politice sau de alt gen;
  e) distribuirii materialelor protejate de drepturi de autor;
  f) transmiterea informațiilor confidențiale prin mesaje electronice nesecurizate;
  g) utilizarea poștei electronice de serviciu pentru răspîndirea virușilor de calculator, de infiltrare în sisteme, deteriorare sau distrugere a datelor, produselor program și echipamentelor ori care duc la degradarea sau perturbarea performanței rețelei;
  h) ascunderea și încercarea de a ascunde identitatea atunci cînd este trimis un mesaj prin poșta electronică de serviciu;
- limitarea accesului personalului la conținut obscen și antisocial, a descărcării conținutului protejat de drepturi de autor, utilizarea neconformă a informațiilor de serviciu și distribuirea lor, descărcarea materialelor din surse necunoscute, precum și alte activități ce contravin obiectivelor instituției.

V. CERINȚELE MINIME OBLIGATORII DE ASIGURARE A SECURITĂȚII CIBERNETICE LA ACHIZIȚIA SISTEMELOR INFORMAȚIONALE NOI SAU ACTUALIZAREA CELOR EXISTENTE

Achiziții de sisteme informaționale automatizate noi

1) suportul anumitor sisteme de securitate și de mentenanță (inclusiv înlăturarea lacunelor de securitate ale sistemului, într-o perioadă prestabilită);

2) transmiterea către instituție a dreptului de autor asupra codului-sursă a produselor program;

3) stabilirea perioadei de timp în care se efectuează actualizările propriu- zise;

4) sistemul de securitate cibernetică poate prevedea caracteristici mai stricte decît cele prevăzute în prezentele Cerințe, dar în măsura în care nu intră în conflict cu legislația în vigoare;

5) înainte de achiziționarea unui nou sistem sau dezvoltarea celui existent, instituția elaborează și aprobă politica de securitate și se asigură că sistemele noi, pe parcursul dezvoltării lor, vor fi conforme prezentelor Cerințe;

6) înainte de a pune în funcțiune un nou sistem, instituția trebuie să se asigure de funcționalitatea caracteristicilor de securitate ale acestuia conform cerințelor prestabilite, prin efectuarea de o terţă parte a testelelor respective;

7) instituţia asigură efectuarea periodică a auditului de securitate a sistemului, în conformitate cu documentaţia tehnică aprobată;

8) dezvoltarea și testarea sistemului nu trebuie să fie sau să prezinte un pericol pentru integritatea datelor stocate în sistem.

VI. CERINȚE DE SECURITATE LA EXTERNALIZAREA ADMINISTRĂRII/MENTENANȚEI SISTEMELOR

Contract cu furnizorul extern de servicii

1) reglementările interne de securitate cibernetică ale instituției pe care trebuie să le urmeze prestatorul de servicii în realizarea prevederilor contractuale;

2) serviciile externalizate;

3) cerințele precise pentru volumul și calitatea serviciilor externalizate documentate ca Service Level Agreement (SLA);

4) drepturile și obligațiile instituției și prestatorului de servicii externalizate:

a) dreptul instituției de a monitoriza continuu calitatea serviciilor furnizate;
b) dreptul instituției de a înainta prestatorului extern de servicii un titlu executoriu cu privire la aspectele legate de externalizarea de bună-credință, de înaltă calitate, executarea la timp și corectă a legilor și a regulamentelor;
c) dreptul instituției de a înainta prestatorului extern de servicii o cerere scrisă motivată pentru încetarea imediată a contractului de externalizare, în cazul în care instituția a constatat că prestatorul extern de servicii nu respectă cerințele contractului de externalizare privind valoarea sau calitatea serviciului;
d) obligația prestatorului extern de servicii de a furniza instituției informația privind monitorizarea continuă a calității serviciilor de externalizare prestate;
e) dreptul de audit al prestatorului de serviciu, dacă au fost notificate nonconformități critice.

VII. RĂSPUNSUL LA INCIDENTE, CONTINUITATEA PROCESELOR ȘI RECUPERAREA

24. Planul de răspuns la incidente stabilește că:

1) instituția trebuie să elaboreze și să pună în aplicare planul de răspuns de incidente cibernetice;

2) în cazul unor încălcări ale securității cibernetice, persoana responsabilă/subdiviziunea asigură imediata notificare, înregistrare și verificare a incidentelor de securitate cibernetică și punerea în aplicare a măsurilor de contracarare a acestora, conform procedurilor stabilite.

25. Continuitatea activității și procedurile de recuperare în caz de dezastru trebuie să prevadă:

1) implementarea procedurilor de efectuare a copiilor de rezervă și a celor de recuperare;

2) elaborarea și implementarea obiectivelor de recuperare, conform obiectivelor momentului de recuperare (OMR) și perioadei de recuperare (OPR).

26. Conformitatea cu cerințele interne și externe de securitate cibernetică stipulează că:

1) instituția actualizează planul său de acțiuni pentru asigurarea securității cibernetice, care precizează măsurile puse în aplicare și cele planificate;

2) instituția asigură conformitatea sa cu cerințele externe de securitate cibernetică, prevăzute de legislație.