INCIDENTUL DE SECURITATE

I. Consideraţii generale. Definirea informaţiei clasificate compromise şi a incidentului de securitate

Punctul de plecare în definirea incidentului de securitate îl reprezintă înţelesul dat de art. 3 din *Standardele naţionale de protecţie a informaţiilor clasificate în România*, aprobate prin HG nr. 585/2002, termenilor ***informaţie clasificată compromisă***, respectiv ***incident de securitate***.

Informaţia clasificată compromisă este *informaţia care şi-a pierdut integritatea, a fost rătăcită, pierdută ori accesată, total sau parţial de persoane neautorizate*. Compromiterea poate fi accidentală sau deliberată şi poate determina una sau mai multe dintre consecinţele menţionate (ex. informaţia poate fi rătăcită şi în acelaşi timp accesată de persoane neautorizate).

Pentru a se stabili dacă informaţia a fost compromisă este necesar să se aibă în vedere semnificaţiile compromiterii. Spre exemplu, pierderea integrităţii, respectiv alterarea informaţiei clasificate înseamnă atât pierderea suportului material, cât şi pierderea confidenţialităţii, disponibilităţii, autenticităţii informaţiei clasificate (mai ales în cazul celor în format electronic).

Incidentul de securitate este *orice acţiune sau inacţiune contrară reglementărilor de securitate a cărei consecinţă a determinat sau este de natură să determine compromiterea informaţiilor clasificate*.

Prin urmare, orice manifestare prin care o persoană **acţionează neconform dispoziţiilor legale în materia protecţiei informaţiilor clasificate**, fie că acestea impun sau interzic o anumită conduită, fapt care determină sau este de natură să determine compromiterea unei astfel de informaţii, constituie incident de securitate (ex. diseminarea sau distrugerea neautorizată; nerespectarea normelor privind evidenţa, întocmirea, păstrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea şi distrugerea informaţiilor clasificate).

Pentru ca acţiunea sau inacţiunea contrară reglementărilor de securitate să constituie incident de securitate, este necesar ca aceasta să ***determine sau să fie de natură să determine compromiterea informaţiei clasificate.***

Întrucât prima dintre posibilele urmări ale incidentului de securitate, respectiv aceea de a fi determinat compromiterea informaţiei clasificate nu ridică probleme, se va insista asupra celeilalte ipoteze, respectiv cea în care acţiunea sau inacţiunea ***este de natură să determine compromiterea***.

Astfel, chiar dacă rezultatul incidentului de securitate nu s-a "consumat" (informaţia nu şi-a pierdut integritatea, nu a fost rătăcită, pierdută etc.), **starea de pericol la adresa valorilor sociale ocrotite s-a produs** (subliniem că valorile sociale protejate prin aplicarea dispoziţiilor legale în domeniul protecţiei informaţiilor clasificate secret de stat sunt **securitatea naţională** şi **apărarea ţării**).

De aceea orice acţiune sau inacţiune care ***este de natură să determine compromiterea*** informaţiilor clasificate trebuie tratată ca incident de securitate, în primul rând pentru că legea prevede astfel în mod expres şi în al doilea rând pentru că numai cercetarea administrativă poate stabili împrejurările în care s-a produs incidentul şi urmările sale. Altfel spus, există posibilitatea ca, aparent, informaţia să nu fi fost compromisă, în vreme ce, în realitate, consecinţele incidentului s-au produs (ex. un document clasificat secret de stat uitat într-o încăpere neprotejată, situată în afara zonelor de securitate, este găsit după câteva ore; chiar şi în acest caz sunt necesare cercetări pentru a se stabili dacă, în respectivul interval de timp, relativ scurt, documentul a fost accesat de o persoană neautorizată).

II. Premise ale producerii incidentelor de securitate

Incidentele de securitate pot să apară pe fondul existenţei unor deficienţe în respectarea dispoziţiilor legale în domeniul protecţiei informaţiilor clasificate, care favorizează sau potenţează producerea incidentelor, constituind **premise** ale acestora. Enumerăm, cu titlu exemplificativ, unele dintre aceste disfuncţii:

- nerespectarea normelor care prevăd componentele protecţiei informaţiilor clasificate: protecţia juridică, protecţia prin măsuri procedurale, protecţia fizică, protecţia personalului care are acces la informaţii clasificate ori este desemnat să asigure securitatea acestora, protecţia surselor generatoare de informaţii. Altfel spus, implementarea şi respectarea măsurilor de protecţie a informaţiilor clasificate pe toate aceste componente constituie o garanţie împotriva producerii incidentelor de securitate;
- transportul informaţiilor clasificate realizat de către persoane juridice neautorizate ori expedierea documentelor şi materialelor care conţin astfel de informaţii prin poştă, în condiţiile în care dispoziţiile art. 81 alin. (1) din *Standardele naţionale de protecţie a informaţiilor clasificate în România*, aprobate prin HG nr. 585/2002, reglementează obligaţia ca transportul să se realizeze prin intermediul unităţii specializate a SRI;

- tergiversarea îndeplinirii obligaţiilor prevăzute de art. 18 din *Standardele naţionale de protecţie a informaţiilor clasificate în România*, aprobate prin HG nr. 585/2002. Astfel, informaţiile secrete de stat şi secrete de serviciu stabilite astfel potrivit HCM nr. 19/1972 nu sunt înregistrate şi sunt gestionate în condiţii improprii, iar nerespectarea dispoziţiilor art. 18 alin. (1) şi (2), care ar determina inventarierea, aducerea sub incidenţa noilor reglementări în materia protecţiei informaţiilor clasificate şi asigurarea securităţii acestor informaţii, constituie deficienţe des întâlnite în practică. În acest context, subliniem că nerespectarea termenului de 12 luni stabilit de art. 18 alin. (1) nu înseamnă că deţinătorii informaţiilor secrete de stat şi secrete de serviciu

stabilite astfel potrivit HCM nr. 19/1972 sunt exoneraţi de obligaţia aducerii la îndeplinire a procedurii de încadrare în noi clase şi niveluri de secretizare, ci, dimpotrivă, reprezintă o circumstanţă agravantă, care **va fi avută în vedere în contextul constatării contravenţiei la art. 18 şi al aplicării sancţiunii prevăzute de Standardele naţionale**;

- compromisuri în privinţa întocmirii şi implementării programelor de prevenire a scurgerii de informaţii clasificate (ex. superficialitatea în întocmirea programelor, transmiterea acestora în mod repetat şi fără a se ţine cont de observaţiile comunicate în mod oficial de Serviciul Român de Informaţii cu ocazia restituirii, întârzierea implementării concrete a măsurilor prevăzute în programe etc.);

- gestionarea în condiţii de risc, cu încălcarea normelor privind evidenţa, întocmirea, păstrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea şi distrugerea informaţiilor clasificate. Nerespectarea dispoziţiilor menţionate constituie unele dintre situaţiile des întâlnite în practică şi care determină compromiterea informaţiilor clasificate;

- de asemenea, reprezintă premise de producere a incidentelor de securitate supraclasificarea şi, mai ales, subclasificarea informaţiilor (ex. subclasificarea determină ca măsurile de securitate să nu fie dimensionate corect, în raport cu clasa ori nivelul real de secretizare a informaţiilor);

- nerespectarea prevederilor *Standardelor naţionale de protecţie a informaţiilor clasificate în România*, aprobate prin HG nr.585/2002, de către persoanele juridice care participă la procedurile de negociere şi derulare a unor contracte clasificate;

- nerespectarea exigenţelor în materia INFOSEC (utilizarea de suporţi de memorie neautorizaţi, conectarea la medii intranet / internet etc).

Enumerarea circumstanţelor care constituie sau pot constitui premise de producere a incidentelor de securitate este doar exemplificativă, în esenţă orice încălcare a dispoziţiilor legale în vigoare putând avea drept consecinţă compromiterea informaţiilor clasificate.

Cu toate acestea supunem atenţiei câteva situaţii concrete care au generat incidente de securitate urmate de compromiterea informaţiei, la nivelul unor entităţi care gestionează informaţii secrete de stat, astfel:

- documente secrete de stat de nivel "strict secret", primite de o instituţie publică centrală de la alţi emitenţi, în scopul îndepliniri atribuţiilor legale specifice acesteia, au fost distruse fără îndeplinirea procedurilor legale prealabile şi contrar cerinţei exprese a emitentului, consemnată pe document;

- *documente secrete de stat, nivel "strict secret", neînregistrate la nivelul instituţiei, au fost predate de către reprezentanţii structurii de securitate, pe baza condicii de predare - primire, unei persoane neautorizate în acel moment pentru a accesa informaţii clasificate; ulterior, documentele nu au fost returnate biroului;*

- informaţii de acelaşi nivel au fost gestionate în exteriorul zonei de securitate clasa I sau chiar la domiciliul unui utilizator, cu toate că informaţia nu trebuia să părăsească sistemul de protecţie al instituţiei deţinătoare;

- transportul unor documente secrete de stat s-a realizat cu mijloace proprii ale unui operator economic naţional între sediile acestuia - şi nu prin intermediul poştei speciale - la acţiune participând inclusiv personal neautorizat;

- documente clasificate au fost multiplicate în exteriorul sediului unei societăţi, la un centru comercial specializat;

- documente clasificate gestionate de un organ de specialitate al administraţiei publice centrale au fost puse la dispoziţia unor case de avocatură fără ca la nivelul acestora să fie implementate măsuri protective;

- *informaţii secrete de stat au fost vehiculate în cadrul unui contract fără obţinerea Certificatului de securitate industrială, de către personal al firmei prestatoare neautorizat la nivelul maxim de secretizare a informaţiilor gestionate. În speţă, documente clasificate au fost puse la dispoziţia unei firme specializată în domeniul arhivistic împreună cu fondul arhivistic neclasificat, cu încălcarea dispoziţiilor legale în domeniul protecţiei informaţiilor clasificate*;

- contrar exigenţelor INFOSEC, sisteme informatice dedicate procesării / stocării informaţiilor clasificate inclusiv secret de stat au fost conectate la reţele de comunicaţii de tip *intranet* sau *internet*, existând astfel posibilitatea compromiterii informaţiei, fie ca urmare a unui atac cibernetic, în cazul conectării la *internet*, fie prin accesare neautorizată, în situaţia *intranet* utilizat deopotrivă de personal neautorizat pentru acces la informaţii secrete de stat;

- *la sistemul informatic şi de comunicaţii (SIC) pe care sunt stocate/procesate informaţii secrete de stat, au fost conectaţi suporţi de memorie externă care nu figurau în evidenţe ca fiind dedicaţi pentru stocarea/transferul informaţiilor astfel clasificate; verificările efectuate au relevat că au fost accesate documente clasificate, conţinutul acestora fiind salvat pe suporturile de memorie în cauză.*

- *un suport de memorie de tip "stick", dedicat stocării / transferului informaţiilor clasificate "secrete de serviciu" a fost pierdut de un angajat al unei autorităţi*

naţionale, în condiţii incerte; suportul de memorie a fost scos din instituţie, cu încălcarea normelor ce reglementează gestiunea informaţiilor în format electronic şi a modului de manipulare a acestora; cercetarea administrativă a reliefat o serie de disfuncţii care au favorizat producerea acestui incident de securitate: lipsa funcţiei de administrator de securitate pentru implementarea măsurilor de securitate specifice echipamentelor informatice care gestionează informaţii clasificate; îndeplinirea cu superficialitate a atribuţiilor pe linia protecţiei informaţiilor clasificate de către membrii structurii de securitate;

- *Informaţii clasificate "secrete de serviciu" au fost transmise prin email atât unui consultant din cadrul unei case de avocatură cât şi unui reprezentant al societăţii mamă, cu sediul în afara teritoriului României;*

- documente clasificate au fost păstrate în arhive neclasificate ale unui organ specializat al administraţiei publice centrale şi implicit accesate de personal neautorizat. *Reprezentanţii instituţiei în cauză au menţionat că existenţa acestor documente nu era cunoscută, în condiţiile în care ultima persoană care le-a gestionat a ieşit la pensie în 2000, fără a fi încheiat un proces verbal de predare - primire a arhivei.*

- pe fondul stării de lichidare a unor operatori economici de stat, arhive conţinând documente clasificate în baza legislaţiei anterioare anului 2002 au fost practic abandonate şi expuse astfel compromiterii, fie prin degradare, fie prin acces neautorizat.

III. Cercetarea incidentelor de securitate. Responsabilităţi

1. Înştiinţarea conducătorului unităţii şi a instituţiilor competente;.

Pornind de la premisa că în practică nu conducătorul unităţii este cel care descoperă producerea unui incident de securitate, un rol important revine şefilor structurilor de securitate care au, în primul rând, obligaţia de a-l încunoştinţa pe conducător despre producerea unui astfel de eveniment, orice compromis putând genera urmări deosebit de grave.

La rândul lor, conform art. 88 din *Standarde*, conducătorii unităţilor deţinătoare de informaţii secrete de stat au obligaţia de ***a înştiinţa***, în scris, instituţiile prevăzute la art. 25 din Legea nr. 182/2002, potrivit competenţelor, prin cel mai operativ sistem de comunicare, despre compromiterea unor astfel de informaţii.

Este obligatoriu ca înştiinţarea să conţină:

a) prezentarea informaţiilor compromise, respectiv clasificarea, marcarea, conţinutul, data emiterii, numărul de înregistrare şi de exemplare, emitentul şi persoana sau compartimentul care le-a gestionat;

b) o scurtă prezentare a împrejurărilor în care a avut loc compromiterea, inclusiv data constatării, perioada în care informaţiile au fost expuse compromiterii şi persoanele neautorizate care au avut sau ar fi putut avea acces la acestea, dacă sunt cunoscute;

c) precizări cu privire la eventuala informare a emitentului.

La solicitarea instituţiilor competente, ***înştiinţările preliminare*** vor fi completate pe măsura derulării cercetărilor (prevăzute la art. 90) iar documentele privind evaluarea prejudiciilor şi activităţile care urmează a fi întreprinse ca urmare a compromiterii vor fi prezentate aceloraşi instituţii. Structura/funcţionarul de securitate are obligaţia de a ţine evidenţa cazurilor de încălcare a reglementărilor de securitate, a documentelor de cercetare şi a măsurilor de soluţionare şi să le pună la dispoziţia autorităţilor desemnate de securitate, conform competenţelor ce le revin.

2. ***Cercetarea incidentului - scopul, modalitatea de realizare, persoanele implicate, conlucrarea cu reprezentanţii autorităţilor desemnate de securitate, finalizarea cercetării***

În conformitate cu prevederile art. 90 din *Standarde*, orice încălcare a reglementărilor de securitate ***va fi cercetată*** pentru a se stabili:

a) dacă informaţiile respective au fost compromise;

b) dacă persoanele neautorizate care au avut sau ar fi putut avea acces la informaţii secrete de stat prezintă suficientă încredere şi loialitate, astfel încât rezultatul compromiterii să nu creeze prejudicii;

c) măsurile de remediere - corective, disciplinare sau juridice - care sunt recomandate.

În aplicarea acestor dispoziţii, pentru atingerea scopului prevăzut de normele menţionate, cercetarea trebuie să se desfăşoare după un anumit algoritm, prima măsură care trebuie dispusă fiind desemnarea, de către conducătorul instituţiei, a unei comisii din care trebuie să facă parte şeful structurii/funcţionarul de securitate şi care să stabilească circumstanţele producerii incidentului.

În acest sens, este necesar să se urmărească circuitul documentului din momentul intrării în unitate, în cazul informaţiilor primite de la alţi emitenţi, respectiv din momentul întocmirii, în cazul informaţiilor proprii, fapt pentru care trebuie consultate registrele de evidenţă şi condicile de predare-primire a documentelor clasificate.

Ulterior, sunt necesare cercetări pentru identificarea persoanelor care au avut acces la informaţia clasificată compromisă (mai ales a ultimei persoane care a gestionat informaţia) şi pentru stabilirea deficienţelor în aplicarea dispoziţiilor legale care au determinat producerea incidentului de securitate.

În astfel de situaţii se va dovedi importanţa deosebită a respectării principiului necesităţii de a cunoaşte şi a normelor privind evidenţa şi transmiterea documentelor clasificate între utilizatori.

Din practica evaluării incidentelor de securitate produse la nivelul unor entităţi din zona de competenţă a SRI în calitate de ADS, a rezultat că, în unele situaţii, cercetările incidentelor de securitate se realizează în mod formal sau nu îndeplinesc toate cerinţele legale, astfel:

- Nu sunt clarificate împrejurările incidentului de securitate;
- Concluziile cercetării se limitează la simpla constatare a compromiterii urmată de declasificare;

- Măsurile corective nu sunt corect dimensionate şi nu sunt de natură să remedieze disfuncţionalităţile sistemului protectiv;

- Nu se clarifică situaţia tuturor informaţiilor care au făcut obiectul incidentului;

- Nu sunt notificaţi alţi eventuali posesori ai informaţiei clasificate compromise;

- Verificările nu au stabilit responsabilităţile pentru producerea incidentului de securitate care a generat compromiterea unor informaţii secrete de stat;

Pe toată durata cercetării este recomandată colaborarea cu reprezentanţii autorităţilor desemnate de securitate competente, care vor acorda sprijinul necesar în limitele atribuţiilor prevăzute de lege, în cadrul activităţilor de asistenţă specializată.

În final, supunem atenţiei faptul că **cercetarea nu se poate considera încheiată decât atunci când rezultatul ei este prezentat de comisie conducătorului unităţii care va dispune asupra măsurilor adecvate, care includ, în cazul suspiciunilor privind fapte care ar putea constitui infracţiuni la regimul secretului de stat, sesizarea organele de urmărire penală, cărora le vor fi puse la dispoziţie datele şi materialele necesare probării faptelor, în condiţiile legii**.