Incidente de securitate

Cercetarea de securitate. Măsuri de reacție și politici anticipative

Evenimente, incidente și încălcări de securitate

Reacție și anticipare. ISO 27002

Definiții. ISO 27002

Evenimentul de securitate a informațiilor este situația identificată în legătură cu un sistem, un serviciu sau o rețea care indică o posibilă încălcare a politicii de securitate a informațiilor, un eșec al măsurilor de protecție, eșecul controalelor sau o situație ignorată anterior, dar relevantă din punct de vedere al securității.

Incidentul privind securitatea informației reprezintă un eveniment sau o serie de evenimente legate sau identificate de securitate a informației care au o probabilitate semnificativă de a compromite activitățile/operațiunile organizației, de a provoca daune activelor acesteia și de a aduce amenințări la securitatea informației.

Încălcarea securității informațiilor este compromiterea securității informațiilor care duce la distrugerea nedorită, pierderea, modificarea, dezvăluirea sau accesul la informațiile protejate transmise, stocate sau prelucrate în alt mod.

Evenimente și incidente de securitate

ISO 27002, care tratează gestionarea incidentelor de securitate a informațiilor, face o **distincție** importantă între un eveniment de securitate a informațiilor și un incident de securitate a informațiilor:

- ❖un eveniment nu este neapărat un incident, în timp ce un incident va începe întotdeauna ca un eveniment;
- ❖există o serie de evenimente (fie așteptate, fie neașteptate), care pot să nu compromită în mod semnificativ integritatea, disponibilitatea sau confidențialitatea informațiilor organizației;
- ❖evenimentele sunt raportate; incidentele sunt gestionate – ceea ce înseamnă că trebuie să existe o decizie, pentru fiecare eveniment, dacă este sau nu un incident;
- ❖un eveniment poate compromite securitatea datelor sau punctele slabe asociate sistemelor informaționale;
- ❖oricât de bun ar fi SMSI, vor exista evenimente de securitate a informațiilor (accidentale sau deliberate, rău intenționate sau pentru distracția unui hacker).

Ceea ce contează este că organizația are o metodă testată și minuțioasă pentru a răspunde la inevitabil. Numai în acest fel organizația poate asigura disponibilitatea și integritatea datelor sale.
ISO/IEC 27035 este codul de practică care se ocupă în mod specific de gestionarea incidentelor și de crearea unei echipe de răspuns la incident de securitate a informațiilor [1].

Mecanismul de raportare a incidentelor (ISO 27002)

Organizația trebuie să ofere un **mecanism de control** pentru ca personalul să raporteze evenimentele observate sau suspectate de securitate a informațiilor prin canale adecvate în timp util.

Scopul acestui mecanism este sprijinirea raportării la timp, consecventă și eficientă a evenimentelor de securitate a datelor și informațiilor care pot fi identificate de personal. Evenimentele de securitate a informațiilor includ incidente, încălcări și vulnerabilități.

Responsabilități:

- tot personalul și utilizatorii trebuie să fie conștienți de responsabilitatea lor de a raporta evenimentele de securitate a informațiilor cât mai repede posibil pentru a preveni sau a minimiza efectul incidentelor de securitate a informațiilor;
- personalul trebuie să cunoască, de asemenea, procedura de raportare a evenimentelor de securitate a informațiilor și punctul de contact la care ar trebui raportate evenimentele.
- mecanismul de raportare ar trebui să fie cât mai ușor, accesibil și disponibil posibil;
- personalul și utilizatorii trebuie sfătuiți să nu încerce să dovedească vulnerabilitățile suspectate de securitate a informațiilor. Testarea vulnerabilităților poate fi interpretată ca o potențială utilizare greșită a sistemului și poate provoca, de asemenea, daune sistemului sau serviciului informațional și poate să distrugă sau să ascundă dovezile digitale. În cele din urmă, acest lucru poate duce la răspunderea juridică pentru persoana care efectuează testarea.

Situații de raportare

Situațiile care trebuie luate în considerare pentru raportarea evenimentelor de securitate a informațiilor includ:

(a)controale ineficiente de securitate a informațiilor;

(b)încălcarea așteptărilor privind confidențialitatea, integritatea sau disponibilitatea informațiilor;

(c)erori umane;

(d)nerespectarea politicii de securitate a informațiilor, politicilor specifice temei sau standardelor aplicabile;

(e)încălcări ale măsurilor de securitate fizică;

(f)modificări ale sistemului care nu au trecut prin procesul de management al schimbării;

(g)defecțiuni sau alte comportamente anormale ale sistemului software sau hardware;

(h)încălcări de acces;

(i)vulnerabilități;

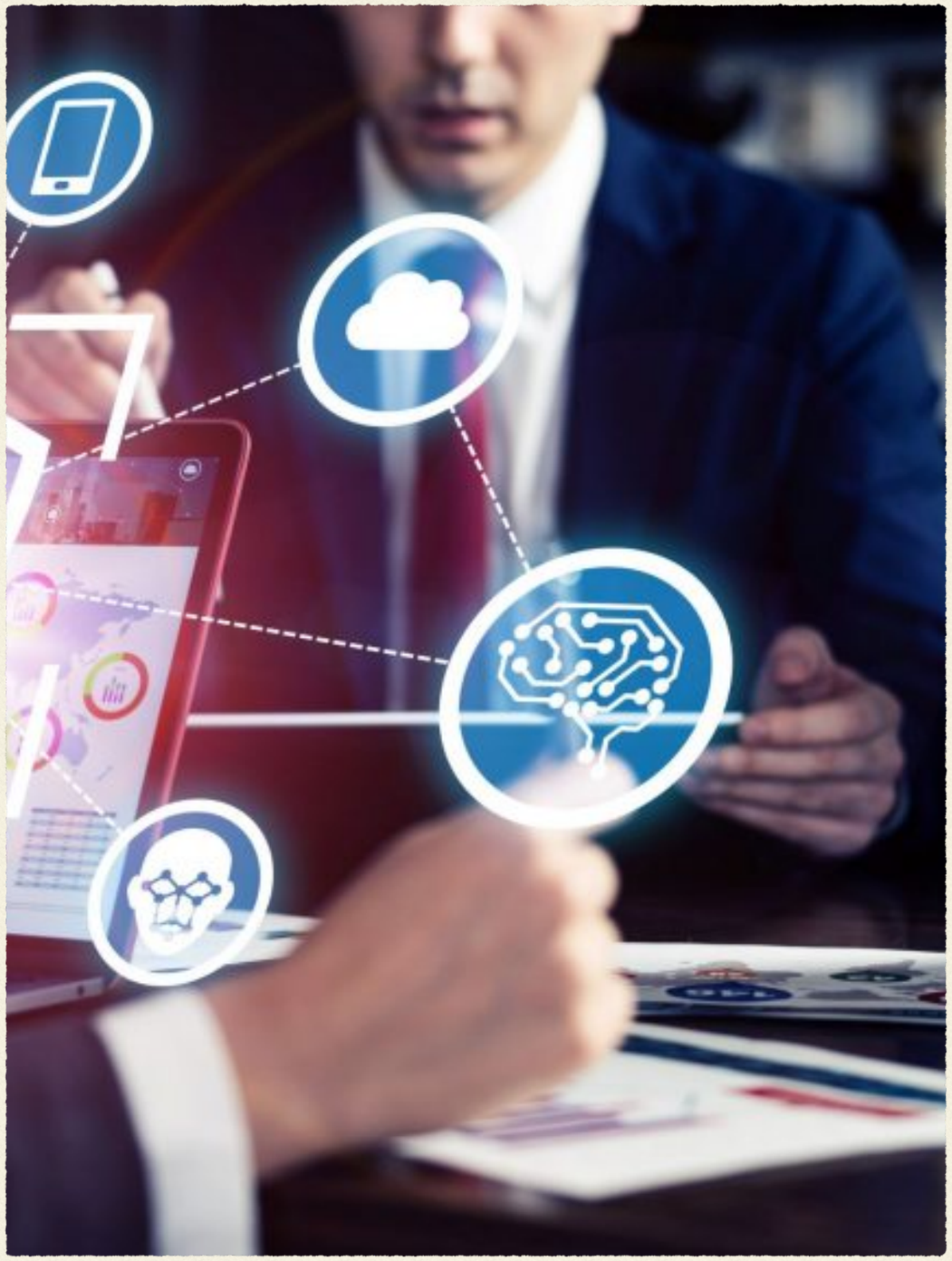
(j)infecție cu malware suspectată.

ISO/IEC 27035

ISO/IEC 27035: 2023 este dedicat managementului incidentelor de securitate a informațiilor, cuprinzând concepte de bază, principii și procese cu activități cheie de management al acestora.

Oferă o abordare structurată pentru pregătirea, detectarea, raportarea, evaluarea și răspunsul la incidente și aplicarea lecțiilor învățate.

Îndrumările sunt aplicabile tuturor organizațiilor, indiferent de tip, dimensiune și natura afacerii în raport cu situația de risc pentru securitatea datelor, fiind utile și firmelor externe care furnizează servicii de gestionare a incidentelor de securitate a datelor și informației.



Planificarea și pregătirea managementului incidentelor

ISO 27002 (5.24) stabilește că planificarea și pregătirea gestionării incidentelor de securitate a datelor și informației **se realizează prin**:

- definirea, stabilirea și comunicarea proceselor, rolurilor și responsabilităților de gestionare a incidentelor de securitate a informațiilor;
- asigurarea unui răspuns rapid, eficient, consecvent și ordonat la incidentele de securitate a informațiilor, inclusiv comunicarea cu privire la evenimentele de securitate a informațiilor.

Roluri și responsabilități:

(1)stabilirea unei metode de raportare a evenimentelor de securitate a informațiilor, inclusiv punct de contact;
(2)stabilirea unui proces de management al incidentelor:
    (a)trebuie să ofere organizației capacitatea de a gestiona incidentele de securitate a informațiilor;
    (b)să aibă capacitatea de administrare, documentare, detectare, triaj, prioritizare, analiza, comunicare și coordonare a părților interesate;
(3)stabilirea unui proces de răspuns la incident:
    (a)oferă organizației capacitatea de a evalua, de a răspunde și de a învăța din incidentele de securitate a informațiilor;
    (b)personalul care răspunde la incidente trebuie pregătit, certificat și dezvoltat profesional continuu;
(4)doar personalul competent trebuie să gestioneze problemele legate de incidentele de securitate a informațiilor din cadrul organizației:
    (a)personalul trebuie să primească documentație privind procedurile;
    (b)este necesară instruirea periodică;
(5)procedurile trebuie comunicate efectiv părților interne și externe relevante.

Proceduri de gestionare a incidentelor

(1)**evaluarea** evenimentelor de securitate conform criteriilor pentru ceea ce constituie un incident de securitate a datelor și informației;

(2)întocmirea unui **PLAN DE MANAGEMENT** al evenimentelor și incidentelor de securitate a datelor, prin mijloace umane sau automate:

(a)**monitorizarea** (jurnalizarea și înregistrarea activităților din sistemele informatice; utilizatorii trebuie să nu aibă posibilitatea de șterge logurile propriilor activități în activele de procesare a datelor) - se realizează conform capitolelor 8.15 și 8.16 din ISO27002;

(b)**detectarea** - trebuie identificate comportamentele anormale și detectate potențialele incidente (cap. 8.16),

(c)**clasificarea** - evaluarea evenimentelor de securitate, conform unei scheme de clasificare și prioritizare, pentru a decide dacă acestea vor fi clasificate ca incidente de securitate (vezi 5.25),

(d)**analiza și raportarea**: mecanisme pentru ca personalul să raporteze evenimente observate sau suspectate de securitate a datelor prin canale adecvate, în timp util (cap. 6.8);

(3)**gestionarea** incidentelor de securitate a informațiilor până la încheiere:

(a)inclusiv răspunsul (vezi 5.26), în funcție de tipul și categoria incidentului

(b)posibila activare a managementului crizei și

(c)activarea planurilor de continuitate,

(d)recuperarea controlată de la un incident și

(e)comunicarea către părțile interesate externe;

(4)**coordonarea cu părțile interesate** interne și externe, cum ar fi autoritățile, grupurile și forumurile de interese externe, furnizorii și clienții (conf. cap. 5.5 și 5.6);

(5)**înregistrarea activităților de gestionare** a incidentelor;

(6)**manipularea probelor** (vezi 5.28);

(7)**analiza cauzei** principale sau proceduri post-incident;

(8)**stabilirea lecțiilor învățate**:

(a)îmbunătățiri ale procedurilor de gestionare a incidentelor sau ale controalelor de securitate a informațiilor în general care sunt necesare.

Proceduri de raportare

TREBUIE SĂ INCLUDĂ:

(1)**acțiuni care trebuie întreprinse** în cazul unui eveniment de securitate a datelor:

(a)notarea imediată a tuturor detaliilor pertinente (apariția defecțiunilor și mesajele de pe ecran),

(b)raportarea imediată la punctul de contact și

(c)luarea doar a acțiunilor coordonate;

(2)utilizarea **formularelor de incident**:

(a)sprijină personalul să efectueze toate acțiunile necesare la raportarea incidentelor de securitate;

(3)procese adecvate de **feedback**:

(a)persoanele care raportează evenimente de securitate sunt notificate, în măsura posibilului, cu privire la rezultate după soluționarea și închiderea problemei;

(4)realizarea **rapoartelor de incidente**:

(a)conform cerințelor de notificare a încălcării către autoritățile de reglementare;

(b)coordonarea răspunsului și partajarea datelor despre incidente cu organizații externe, după caz.

Îndrumări detaliate privind gestionarea incidentelor de securitate a informațiilor sunt furnizate în seria ISO/IEC 27035.

Evaluare și decizie a evenimentelor de securitate a datelor

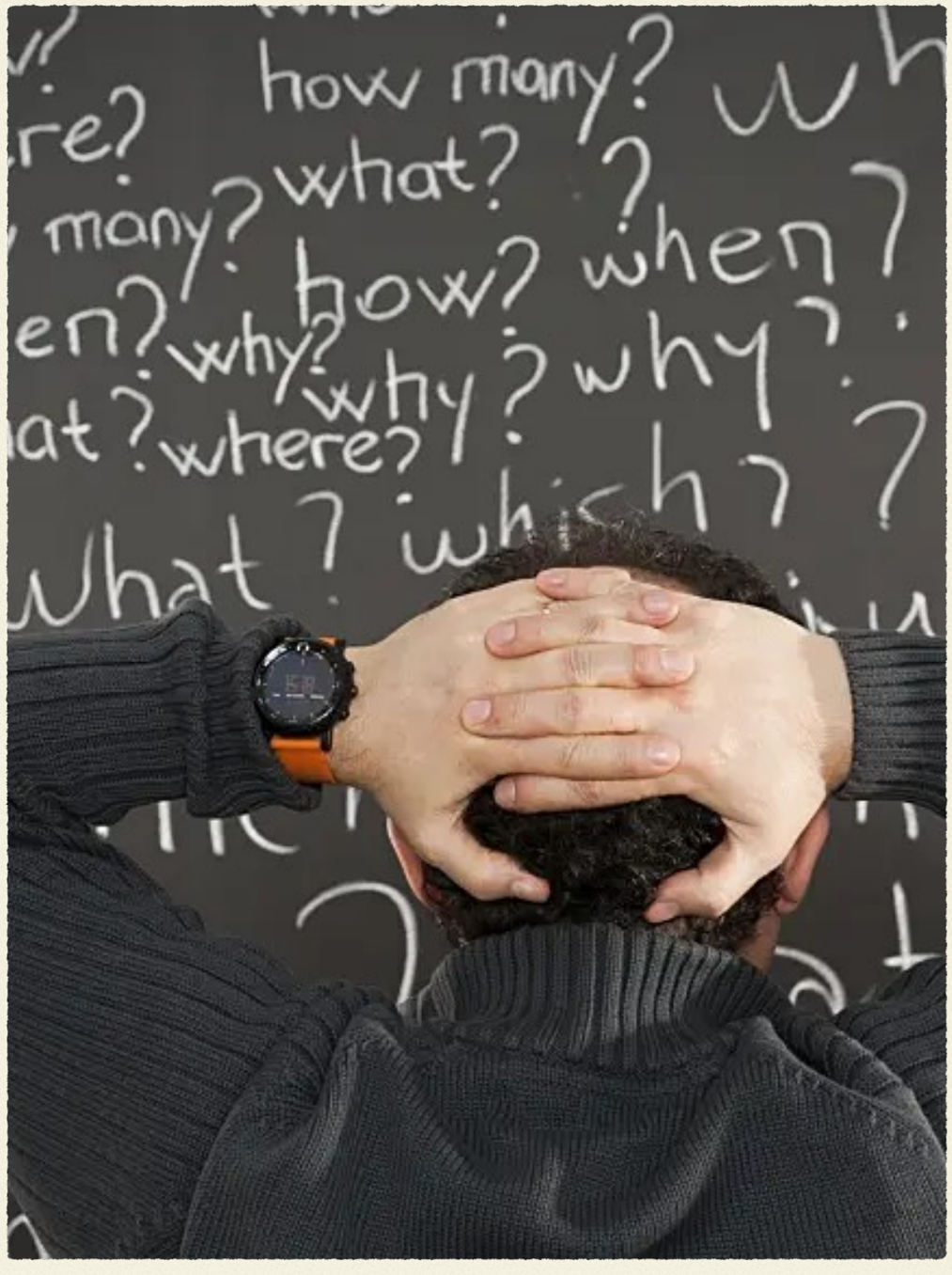
Conform standardului 27002 (5.25), organizația trebuie **să evalueze** evenimentele de securitate și **să decidă** dacă acestea vor fi clasificate ca **incidente de securitate a datelor și informațiilor**:

(1)scopul este **prioritizarea** evenimentelor de securitate a datelor;

(2)trebuie convenită o **schemă de clasificare** și prioritizare a evenimentelor stabilite drept incidente de securitate, evaluată de punctul de contact;

(3)**decizia** cu privire la evaluare o ia personalul responsabil cu coordonarea și răspunsul la incident;

(4)**rezultatele** evaluării și ale deciziei trebuie înregistrate în detaliu pentru verificări și referințe ulterioare.



Răspuns la incidentele de securitate

Procedurile de răspuns la incidentele de securitate (5.26) a datelor și informației trebuie să includă:

(1)**stabilirea sistemelor afectate** de incident și a faptului dacă urmările acestuia se pot răspândi;
(2)**colectarea probelor** (vezi 5.28) cât mai curând posibil după producerea evenimentului:
    (a)identificarea, colectarea, achiziția sau păstrarea dovezilor legate de evenimentul de securitate;
    (b)respectarea procedurilor interne de colectare pentru acțiuni disciplinare sau legale;
    (c)păstrarea dovezilor în funcție de mediile de stocare, dispozitive și starea acestora (pornit/oprit)
    (d)colectarea probelor trebuie realizată astfel încât să fie admisibilă în instanțele naționale sau foruri disciplinare;
    (e)dovezile nu trebuie să fie modificate, să fie complete, identice cu originalele;
(3)activități de **gestionare a crizelor** și eventual invocarea **planurilor de continuitate a activității** (a se vedea 5.29 și 5.30);
(4)asigurarea faptului că toate activitățile de răspuns implicate sunt **înregistrate** corespunzător pentru analize ulterioare;

Răspuns la incidentele de securitate

Procedurile de răspuns la incidentele de securitate (5.26) a datelor și informației trebuie să includă:

(5)**comunicarea** existenței incidentului de securitate a informațiilor sau a oricăror detalii relevante ale acestuia tuturor părților interesate interne și externe relevante, conform principiului necesității de a cunoaște;

(6)**coordonarea cu părțile** interne și externe, cum ar fi autoritățile, grupurile și forumurile de interese externe, furnizorii și clienții, pentru a îmbunătăți eficiența răspunsului și a ajuta la minimizarea consecințelor pentru alte organizații;

(7)odată ce incidentul a fost rezolvat cu succes, **închiderea și înregistrarea oficială** a acestuia;

(8)efectuarea de **analize criminalistice de securitate a informațiilor**, după cum este necesar (vezi 5.28);

(9)efectuarea **analizei post-incident** pentru a identifica cauza principală. Asigurați-vă că este documentat și comunicat conform procedurilor definite (vezi 5.27);

(10)identificarea și **gestionarea vulnerabilităților și punctelor slabe** în securitatea informațiilor, inclusiv cele legate de controalele care au cauzat, au contribuit la sau nu au reușit să prevină incidentul.

Învățare din incidentele de securitate

LECȚIILE ÎNVĂȚATE în urma incidentelor de securitate a datelor și informației (5.27) și cunoștințele dobândite trebuie utilizate pentru **îmbunătățirea controalelor de securitate** a informațiilor, pentru a reduce probabilitatea sau consecințele unor incidente viitoare.

Informațiile obținute în urma evaluării incidentelor de securitate a informațiilor trebuie utilizate pentru:

(a)**îmbunătățirea planului de management al incidentelor**, inclusiv scenariile și procedurile de incidente (a se vedea 5.24);

(b)**cuantificarea, colectarea și monitorizarea** tipurilor, volumelor și costurilor incidentelor de securitate;

(c)**identificarea incidentelor recurente sau grave** și cauzele acestora pentru:

i. actualizarea evaluării riscului de securitate a informațiilor a organizației și

ii. determinarea și implementarea controalele suplimentare necesare pentru a reduce probabilitatea sau consecințele unor incidente similare viitoare;

(d)**sporirea gradului de conștientizare și instruire** a utilizatorilor (a se vedea 6.3):

i. oferirea de exemple despre ceea ce se poate întâmpla,

ii. cum să răspundem la astfel de incidente și

iii. cum să le evitați în viitor [2].

Incidente de securitate a informațiilor clasificate

România

INCIDENTUL DE SECURITATE este definit ca fiind „orice acțiune sau inacțiune contrară reglementărilor de securitate a cărei consecință a determinat sau este de natură să determine compromiterea informațiilor clasificate” (art.3).

Același articol stabilește că „INFORMAȚIA CLASIFICATĂ COMPROMISĂ este informația clasificată care și-a pierdut integritatea, a fost rătăcită, pierdută sau accesată, total sau parțial, de persoane neautorizate”.

Standardele naționale de protecție a informațiilor clasificate, aprobate prin Hotărârea de Guvern nr.585 din 13 iunie 2002 pentru protecția informațiilor secrete de stat și de serviciu, Monitorul oficial, nr. 485 din 5 iulie 2002 [3]

Obligații și răspunderi pentru informațiile clasificate

Între obligațiile și răspunderile ce revin autorităților și instituțiilor publice, agenților economici și altor persoane juridice pentru protecția informațiilor secrete de stat (capitolul V din Standarde), se regăsește și **obligația conducătorului unității care gestionează informații secrete de stat**:

- de a sesiza instituțiile prevăzute la articolul 25 din Legea nr.182/2002, conform competențelor, în legătură cu incidentele de securitate și riscurile la adresa informațiilor secrete de stat:
  - sunt autorități desemnate de securitate, potrivit legii: Ministerul Apărării Naționale, Ministerul de Interne, Ministerul Justiției, Serviciul Român de Informații, Serviciul de Informații Externe, Serviciul de Protecție și Pază, Serviciul de Telecomunicații Speciale;
  - Parlamentul, Administrația Prezidențială, Guvernul și Consiliul Suprem de apărare a Țării, menționate la art.25, stabilesc măsuri proprii privind protecția informațiilor secrete de stat, cu asistența de specialitate a SRI;
- să dispună efectuarea de cercetări și, după caz, să sesizeze organele de urmărire penală în situația compromiterii informațiilor clasificate (art.86, lit s) și t).

Dispoziții normative privind incidentele de securitate

Atribuții privind incidentele de securitate a informațiilor clasificate:

1. PLANUL DE PAZĂ ȘI APĂRARE ce este anexat PROGRAMULUI DE PREVENIRE A SCURGERII DE INFORMAȚII CLASIFICATE va cuprinde procedura de raportare, cercetare și evidență a incidentelor de securitate;
2. AGENȚIA DE SECURITATE PENTRU INFORMATICĂ ȘI COMUNICAȚII, care este subordonată instituției desemnate la nivel național pentru protecția informațiilor electronice clasificate, din cadrul structurilor organizatorice cu atribuții specifice în domeniul INFOSEC, are ca atribuții:
    1. semnalarea către agenția de acreditare de securitate incidentele de securitate în domeniu sistemelor de comunicație și informatice
3. AGENȚIA DE PROTECȚIE CRIPTOGRAFICĂ, care se organizează la nivel național și este subordonată instituției desemnate la nivel național pentru protecția informațiilor clasificate, are ca atribuții și:
    1. raportarea către instituția desemnată pentru protecția informațiilor clasificate incidentele de securitate cu care s-a confruntat.

Cercetarea de securitate

Anexa nr.10/E din HG nr.585/2002 stabilește **reperele** cercetării de securitate în cazurile de încălcare a reglementărilor privind protecția informațiilor clasificate:

- cazurile de încălcare a reglementărilor de securitate vor fi comunicate imediat conducătorului instituției/agentului economic și instituțiilor abilitate;
- orice încălcare a reglementărilor de securitate va fi cercetată de persoane special desemnate, cu experiență în activitatea de securitate pentru a stabili:
  - dacă și în ce mod au fost compromise informații clasificate;
  - dacă persoanele neautorizate care au avut, sau ar fi putut avea acces la informații clasificate, prezintă suficientă încredere și loialitate, astfel încât rezultatul compromiterii să nu creeze prejudicii;
  - măsurile de remediere, corective sau disciplinare (inclusiv juridice), care sunt recomandate;
  - în situația în care persoanele care au luat cunoștință de conținutul informațiilor clasificate prezintă încredere:
    - vor fi instruite în mod corespunzător pentru a preveni diseminarea,
    - în caz contrar se va proceda la evaluarea prejudiciului rezultat și vor fi întreprinse măsurile necesare diminuării acestuia.

Evidența încălcărilor reglementărilor de securitate

(a)se organizează de către AUTORITĂȚILE ȘI INSTITUȚIILE PUBLICE, AGENȚII ECONOMICI CU CAPITAL INTEGRAL SAU PARȚIAL DE STAT ȘI ALTE PERSOANE JURIDICE DE DREPT PUBLIC SAU PRIVAT, deținătoare de informații clasificate și cuprinde:

i. evidența **cazurilor de încălcare** a reglementărilor de securitate,
ii.situația **rapoartelor de investigații** și
iii.evidența **măsurilor corective întreprinse**, în consecință.

(b)aceste evidențe vor fi **păstrate timp de trei ani** de către structura/funcționarul de securitate și vor fi puse **la dispoziție în timpul controalelor** efectuate de reprezentanții autorizați ai instituțiilor abilitate.

Scoaterea din evidență a documentelor clasificate pierdute sau distruse:
Documentul iremediabil pierdut (și nu rătăcit) va fi scos din evidența compartimentului care l-a gestionat, numai ***după finalizarea cercetărilor***, cu avizul instituțiilor abilitate, când există indicii certe, confirmate în scris de instituțiile abilitate cu atribuții de control și investigare a compromiterii informațiilor clasificate.

Comunicarea compromiterilor informațiilor clasificate

INFORMAȚIILE CLASIFICATE SUNT COMPROMISE CÂND:

- ✤conținutul acestora (total sau parțial) este cunoscut de persoane neautorizate (care nu au autorizare valabilă de acces la acestea) ori
- ✤când au fost supuse riscului acestei cunoașteri neautorizate (informațiile clasificate pierdute, chiar și temporar, în afara unei zone de securitate sunt considerate a fi compromise).

Comunicarea compromiterilor:

- ➡**instituțiile abilitate** vor fi încunoștințate prin cel mai operativ sistem de comunicare asupra circumstanțelor compromiterii unor astfel de informații;
- ➡**scopul** principal al comunicării compromiterii este de a da posibilitatea:
  - ✓recuperării informațiilor,
  - ✓evaluării prejudiciilor și
  - ✓întreprinderii acțiunilor necesare sau aplicabile pentru minimalizarea consecințelor.

Informarea preliminară a incidentului de securitate

Trebuie să conțină:

(a)o **descriere a informațiilor** respective (clasificare și marcare, numărul de înregistrare, numărul de exemplare, conținutul, data, emitentul);

(b)o scurtă **prezentare a împrejurărilor** în care a avut loc compromiterea, inclusiv data constatării, perioada în care informațiile au fost expuse compromiterii și, dacă se cunoaște, persoanele neautorizate care au avut sau ar fi putut avea acces la acestea;

(c)precizări cu privire la **eventuala informare a emitentului**;

(d)la solicitarea instituțiilor abilitate, informările preliminare vor fi **completate** pe măsura derulării cercetărilor.

Sancțiuni în cazul compromiterii informațiilor clasificate

Acestea pot fi: disciplinare, contravenționale și penale.

(1)**Disciplinare** (abateri disciplinare), stabilite conform statutelor, regulamentelor de organizare sau altor acte normative ale instituțiilor sau organizațiilor deținătoare:

(a)avertismentul,

(b)reducerea cu 5-15% a salariului și/sau indemnizației de conducere pentru 1-3 luni,

(c)retrogradarea în grad sau treapta profesională,

(d)revocarea din funcția de conducere,

(e)mutarea disciplinară și

(f)excluderea din profesie.

(2)**Contravenționale**, prevăzute de art.338 din HG nr. 585/2002:

a)amenda, în diverse cuantumuri, în funcție de faptele săvârșite,

b)avertisment sau amendă, cu valori mai mari, în funcție de gravitatea abaterii

c)confiscarea bunurilor destinate, folosite sau rezultate din contravenții

(3)**Penale**, prevăzute în Codul penal în mai multe texte:

(a)„divulgarea secretului profesional" (art. 196);

(b)„sustragerea sau distrugerea de înscrisuri" (art. 242 – din capitolul „Infracțiuni contra autorității");

(c)„neglijența în serviciu" (art.249);

(d)„neglijența în păstrarea secretului de stat" (art.252);

(e)„reținerea sau distrugeri de înscrisuri" (art.272 - din capitolul „Infracțiuni care împiedică înfăptuirea justiției");

(f)„călcarea de consemn" (art. 333 – în cazul infracțiunilor comise de militari) și

(g)mai multe din infracțiunile contra siguranței statului (art. 155 și urm.), dar, în special, „compromiterea unor interese de stat" (art. 168) și „divulgarea secretului care periclitează siguranța statului" (art. 169) [4].

Încălcări ale securității și compromiterea informațiilor clasificate Uniunea Europeană

Încălcările securității sau compromiterii informațiilor clasificate ale Uniunii Europene (IUEC):

(1) o încălcare a securității are loc în urma unei fapte sau omisiuni a unei persoane care contravine normelor de securitate stabilite în prezenta decizie;

(2) compromiterea IUEC are loc atunci când, în urma unei încălcări a securității, acestea au fost divulgate, integral sau parțial, unor persoane neautorizate;

(3) orice încălcare sau suspiciune de încălcare a securității este raportată imediat autorităților competente de securitate.

Decizia Consiliului UE nr.2013/488/UE (art.14)[5]

Norme anterioare privind compromiterea IUEC

Decizia Consiliului UE nr.2001/264/CE[6] (abrogată în 2011) stabilea anterior că:

(a)**persoanele neautorizate** sunt persoane care nu dispun de autorizație UE corespunzătoare sau care nu au nevoie să cunoască aceste informații, ori când există o suspiciune credibilă că un asemenea fapt a avut loc;

(b)informațiile clasificate ale UE **pot fi compromise prin** lipsă de atenție, prin neglijență sau prin indiscreție, precum și ca urmare a activităților serviciilor care au drept țintă UE sau statele membre ale acesteia și care sunt interesate de informațiile clasificate și de activitățile UE, sau de către organizații subversive;

(c)este important ca toate persoanele cărora li se cere să lucreze cu informații clasificate ale UE **să fie informate pe deplin cu privire la**:

i. procedurile de securitate,

ii.la pericolele prezentate de anumite conversații indiscrete si

iii.la relațiile pe care trebuie să le aibă cu presa.

(d)aceste persoane trebuie să fie conștiente de **importanța raportării fără întârziere** a oricărei încălcări a securității pe care ar putea-o observa, autorității de securitate a statului membru respectiv, a instituției sau agenției în cadrul cărora lucrează.

Managementul informațiilor clasificate, în scop preventiv

(a)are drept scop **aplicarea măsurilor administrative** pentru a controla IUEC pe durata ciclului lor de viață, contribuind la descurajarea și detectarea compromiterii sau pierderii deliberate sau accidentale a informațiilor de acest tip (art.9);

- ❖măsurile se referă la: crearea, înregistrarea, copierea, traducerea, reducerea nivelului de clasificare, declasificarea, transportul și distrugerea IUEC;

(b)Secretarul General este autoritatea de securitate a SGC, dispune **efectuarea de investigații** cu privire la orice compromitere sau pierdere, reală sau prezumată, de informații clasificate deținute sau elaborate de Consiliu și solicită autorităților de securitate competente să contribuie la astfel de investigații;

(c)statele membre trebuie să desemneze o Autoritate Națională de Securitate (ANS) care este responsabilă cu măsurile de securitate pentru protecția IUEC, astfel încât:

- ❖să fie instituite **programe de securitate** în funcție de necesități pentru a reduce la minimum riscul de pierdere sau de compromitere a IUEC.

Investigarea de securitate privind informațiile clasificate

SE REALIZEAZĂ ATUNCI CÂND se cunoaște sau există motive întemeiate să se presupună că IUEC au fost compromise sau pierdute:

(1)ANS sau altă autoritate competentă ia toate **măsurile** corespunzătoare în **conformitate cu actele cu putere de lege** și reglementările relevante pentru:

(a)a informa emitentul;

(b)a asigura investigarea cazului de membri ai personalului care nu sunt implicați în mod direct în încălcare, pentru a stabili faptele;

(c)a evalua eventualele prejudicii aduse intereselor Uniunii sau ale statelor membre;

(d)a lua măsurile adecvate pentru a împiedica repetarea situației; și

(e)a notifica autorităților competente acțiunea întreprinsă.

(2)orice **persoană responsabilă** de încălcarea normelor de securitate prevăzute în prezenta decizie poate fi pasibilă de **acțiuni disciplinare**, în conformitate cu normele și reglementările aplicabile;

(3)orice persoană responsabilă pentru compromiterea sau pierderea IUEC este **pasibilă de acțiuni disciplinare și/sau în justiție**, în conformitate cu actele cu putere de lege, normele și reglementările aplicabile.

Investigarea de securitate privind informațiile clasificate

Activități derulate de îndată, conform Deciziei 2001/264 (abrogată în 2011):

(1)stabilirea situației de fapt;

(2)evaluarea și minimizarea daunelor produse;

(3)prevenirea posibilei repetări a acelor fapte;

(4)anunțarea autorităților corespunzătoare asupra efectelor încălcării securității;

(5)se pun la dispoziție o descriere a informațiilor în cauză (clasificarea acestora, referința și numărul copiei, data, deținătorul, subiectul și domeniul documentului;

(6)descrierea pe scurt a circumstanțelor în care s-a produs încălcarea, inclusiv data și perioada de timp în care informațiile respective au fost expuse compromiterii.

Note bibliografice

1. Calder, Alan, Watkins, Steve - IT Governance - An international guide to data security and ISO 27001 / ISO 27002, 7th edition, 2020, pg.310

2. ISO/IEC 27002/2022 (E) - Information security, cybersecurity and privacy protection — Information security controls

3. https://legislatie.just.ro/Public/DetaliiDocument/37319

4. Narcis-Violin Stoica, Dan Condrea - Informații clasificate, suport de curs, Amara, 2009

5. Decizia Consiliului Uniunii Europene din 23 septembrie 2013 privind normele de securitate pentru protecția informațiilor UE clasificate (2013/488/UE), disponibilă la: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:02013D0488-20210701

6. Decizia Consiliului din 19 martie 2001 de adoptare a regulamentului de securitate al Consiliului (2001/264/CE), disponibilă la: https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32001D0264