Orientări 01/2021

referitoare la exemple de notificare privind încălcarea securității datelor cu caracter personal

Adoptate la 14 decembrie 2021

Versiunea 2.0

Istoricul versiunilor

Versiunea 2.0	14 12 2021	Adoptarea orientărilor în urma consultării publice
Versiunea 1.0	14 01 2021	Adoptarea orientărilor pentru consultarea publică

Cuprins

COMITETUL EUROPEAN PENTRU PROTECȚIA DATELOR

având în vedere articolul 70 alineatul (1) litera (e) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (denumit în continuare „RGPD”),

având în vedere Acordul privind SEE, în special anexa XI și Protocolul 37 la acesta, astfel cum a fost modificat prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018[1],

având în vedere articolele 12 și 22 din Regulamentul său de procedură,

având în vedere Comunicarea Comisiei către Parlamentul European și Consiliu intitulată „Protecția datelor ca pilon al capacitării cetățenilor și al abordării UE privind tranziția digitală – doi ani de aplicare a Regulamentului general privind protecția datelor”[2],

A ADOPTAT URMĂTOARELE ORIENTĂRI

1 INTRODUCERE

1. RGPD prevede, în anumite cazuri, cerința ca o încălcare a securității datelor cu caracter personal să fie notificată autorității naționale de supraveghere competente (denumită în continuare „AS”) și să fie comunicată persoanelor ale căror date cu caracter personal au fost afectate de încălcare (articolele 33 și 34).

2. Grupul de lucru „articolul 29” a elaborat deja, în octombrie 2017, orientări *generale* privind notificarea încălcării securității datelor, analizând secțiunile relevante din RGPD (Orientări privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului 2016/679, WP 250) (denumite în continuare „Orientările WP 250”)[3]. Cu toate acestea, având în vedere natura și data emiterii lor, aceste orientări nu au abordat suficient de detaliat toate aspectele practice. Prin urmare, a apărut necesitatea unor orientări *axate pe soluții practice, bazate pe cazuri*, care să utilizeze experiența dobândită de AS de la intrarea în vigoare a RGPD.

[1] Trimiterile la „statele membre” din prezentul document trebuie înțelese ca trimiteri la „statele membre ale SEE”.

[2] COM(2020) 264 final, 24 iunie 2020.

[3] G29 WP250 rev.1, 6 februarie 2018, Orientări privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului 2016/679 – aprobate de CEPD, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

3. Prezentul document are rolul de a completa Orientările WP 250 și reflectă experiențele comune ale AS din SEE de la intrarea în vigoare a RGPD. Scopul său este de a-i ajuta pe operatorii de date să decidă cum să gestioneze încălcările securității datelor și ce factori trebuie luați în considerare în timpul evaluării riscurilor.

4. Ca parte a oricărei încercări de a aborda o încălcare, operatorul și persoana împuternicită de operator ar trebui, în primul rând, să fie în măsură să recunoască o încălcare. RGPD definește „încălcarea securității datelor cu caracter personal" la articolul 4 punctul 12 drept „o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea".

5. În Avizul său 03/2014 privind notificarea încălcărilor[4] și în Orientările sale WP 250, GL29 a explicat că încălcările pot fi clasificate în funcție de următoarele trei principii bine cunoscute privind securitatea informațiilor:

   - „Încălcarea confidențialității" – în cazul în care are loc o divulgare neautorizată sau accidentală sau un acces neautorizat sau accidental la datele cu caracter personal.
   - „Încălcarea integrității" – în cazul în care are loc o modificare neautorizată sau accidentală a datelor cu caracter personal.
   - „Încălcarea disponibilității" – în cazul în care are loc o pierdere accidentală sau neautorizată a accesului sau distrugerea datelor cu caracter personal[5].

6. O încălcare poate avea o serie de efecte negative semnificative asupra persoanelor, ceea ce poate conduce la prejudicii fizice, materiale sau morale. RGPD explică faptul că acestea pot include pierderea controlului asupra datelor lor cu caracter personal, limitarea drepturilor persoanelor, discriminare, furt sau fraudă de identitate, pierdere financiară, inversarea neautorizată a pseudonimizării, prejudicii la adresa reputației și pierderea confidențialității datelor cu caracter personal protejate prin secret profesional. De asemenea, acestea pot include orice alt dezavantaj semnificativ de natură economică sau socială adus persoanelor respective. Una dintre cele mai importante obligații ale operatorului de date este de a evalua aceste riscuri pentru drepturile și libertățile persoanelor vizate și de a pune în aplicare măsuri tehnice și organizatorice adecvate pentru a le aborda.

7. În consecință, RGPD prevede obligația operatorului de a:

   - păstra documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse[6];

---

[4] G29 WP213, 25 martie 2014, Avizul 03/2014 privind notificarea încălcărilor securității datelor cu caracter personal, p. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4.

[5] A se vedea Orientările WP 250, p. 7. – Trebuie să se țină seama de faptul că o încălcare a securității datelor poate viza fie o categorie, fie mai multe categorii simultan sau combinate.

[6] RGPD, articolul 33 alineatul (5).

- notifica încălcarea securității datelor cu caracter personal autorității de supraveghere, cu excepția cazului în care este puțin probabil să genereze un risc pentru drepturile și libertățile persoanelor fizice[7];
- comunica persoanei vizate încălcarea securității datelor cu caracter personal în cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice[8].

8. Încălcările securității datelor reprezintă în sine o problemă, dar pot fi, de asemenea, simptome ale unui regim de securitate a datelor vulnerabil, posibil depășit, putând indica, de asemenea, deficiențe ale sistemului care trebuie remediate. În general, este întotdeauna mai bine să se prevină încălcările securității datelor prin pregătire prealabilă, deoarece mai multe consecințe ale acestora sunt, prin natura lor, ireversibile. Înainte ca un operator să poată evalua *pe deplin* riscul care decurge dintr-o încălcare cauzată de o anumită formă de atac, ar trebui identificată cauza principală a problemei, pentru a se stabili dacă există în continuare vreunele dintre vulnerabilitățile care au generat incidentul și, prin urmare, dacă acestea sunt încă exploatabile. În multe cazuri, operatorul este în măsură să identifice probabilitatea ca incidentul să genereze un risc și, prin urmare, trebuie notificat. În alte cazuri, notificarea nu trebuie amânată până la evaluarea completă a riscului și a impactului încălcării, deoarece evaluarea completă a riscurilor poate avea loc în paralel cu notificarea, iar informațiile astfel obținute pot fi furnizate autorității de supraveghere în mai multe etape, fără întârzieri suplimentare nejustificate[9].

9. Încălcarea ar trebui notificată atunci când operatorul consideră că este probabil ca încălcarea să genereze un risc pentru drepturile și libertățile persoanei vizate. Operatorii ar trebui să efectueze această evaluare în momentul în care iau cunoștință de încălcare. Operatorul nu ar trebui să aștepte o expertiză criminalistică detaliată și măsuri de atenuare (timpurii) înainte de a evalua dacă încălcarea securității datelor este susceptibilă să genereze sau nu un risc și, prin urmare, ar trebui notificată.

10. În cazul în care un operator autoevaluează riscul ca fiind puțin probabil, dar se dovedește că riscul se materializează, AS competentă își poate utiliza competențele corective și poate decide să aplice sancțiuni.

11. Fiecare operator și fiecare persoană împuternicită de operator ar trebui să dispună de planuri și proceduri pentru gestionarea eventualelor încălcări ale securității datelor. Organizațiile ar trebui să dispună de linii de raportare clare și de persoane responsabile de anumite aspecte ale procesului de recuperare.

12. Formarea și sensibilizarea cu privire la aspectele legate de protecția datelor pentru personalul operatorului și al persoanei împuternicite de operator, cu accent pe gestionarea încălcării securității datelor cu caracter personal (identificarea unui incident legat de încălcarea securității datelor cu caracter personal și acțiuni suplimentare care trebuie întreprinse etc.), sunt, de asemenea, esențiale pentru operatori și pentru persoanele împuternicite de operatori. Această formare ar trebui repetată periodic, în funcție de tipul activității de prelucrare și de dimensiunea operatorului, abordând cele mai recente tendințe și alerte generate de atacurile cibernetice sau de alte incidente de securitate.

13. Principiul responsabilității și conceptul de protecție a datelor din faza de proiectare ar putea include o analiză care să fie integrată în propriul „Manual privind gestionarea cazurilor de încălcare a securității datelor cu caracter personal” al unui operator de date și al unei persoane împuternicite de operator, care

[7] RGPD, articolul 33 alineatul (1).

[8] RGPD, articolul 34 alineatul (1).

[9] RGPD, articolul 33 alineatul (4).

urmărește să stabilească faptele pentru fiecare aspect al prelucrării în fiecare etapă majoră a operațiunii. Un astfel de manual elaborat în prealabil ar oferi o sursă de informații mult mai rapidă pentru a permite operatorilor de date și persoanelor împuternicite de operatori să atenueze riscurile și să își îndeplinească obligațiile fără întârzieri nejustificate. Acest lucru ar garanta că, în cazul în care s-ar produce o încălcare a securității datelor cu caracter personal, persoanele din organizație ar ști ce trebuie să facă, iar incidentul ar fi mai mult ca sigur gestionat mai rapid decât dacă nu ar exista măsuri sau un plan de atenuare.

14. Deși cazurile prezentate mai jos sunt fictive, ele se bazează pe cazuri tipice din experiența colectivă a AS-urilor în ceea ce privește notificările privind încălcarea securității datelor. Analizele oferite se referă în mod explicit la cazurile examinate, dar cu scopul de a oferi asistență operatorilor de date în evaluarea propriilor încălcări ale securității datelor. Orice modificare a circumstanțelor cazurilor descrise mai jos poate duce la niveluri de risc diferite sau mai semnificative, necesitând astfel măsuri diferite sau suplimentare. Aceste orientări structurează cazurile în funcție de anumite categorii de încălcări (de exemplu, atacuri de tip ransomware). Anumite măsuri de atenuare sunt necesare în fiecare caz atunci când se abordează o anumită categorie de încălcări. Aceste măsuri nu sunt neapărat repetate în analiza fiecărui caz care aparține aceleiași categorii de încălcări. Pentru cazurile care aparțin aceleiași categorii, sunt indicate numai diferențele. Prin urmare, cititorul ar trebui să parcurgă toate cazurile relevante pentru categoria relevantă a unei încălcări pentru a identifica și a distinge toate măsurile corecte care trebuie luate.

15. Documentarea internă a unei încălcări este o obligație independentă de riscurile aferente încălcării și trebuie efectuată în fiecare caz în parte. Cazurile prezentate mai jos încearcă să clarifice dacă o încălcare trebuie sau nu trebuie notificată autorității de supraveghere și comunicată persoanelor vizate afectate.

2 RANSOMWARE

16. O cauză frecventă a unei notificări a încălcării securității datelor este un atac de tip ransomware la adresa operatorului de date. În aceste cazuri, un cod dăunător criptează datele cu caracter personal și, ulterior, atacatorul solicită operatorului să plătească o răscumpărare în schimbul codului de decriptare. Acest tip de atac poate fi clasificat, de obicei, drept o încălcare a disponibilității, dar, adesea, ar putea apărea și o încălcare a confidențialității.

2.1 CAZUL nr. 01: Atac ransomware cu copie de rezervă adecvată și fără exfiltrare

Sistemele informatice ale unei mici întreprinderi din sectorul producției au fost expuse unui atac de tip ransomware, iar datele stocate în aceste sisteme au fost criptate. Operatorul de date a utilizat criptarea datelor stocate pe hard disk („encryption at rest”), astfel încât toate datele accesate de software-ul ransomware au fost stocate în formă criptată utilizând un algoritm de criptare de ultimă generație. Cheia de decriptare nu a fost compromisă în timpul atacului, și anume atacatorul nu a putut să o acceseze și nici să o utilizeze indirect. În consecință, atacatorul a avut acces numai la date cu caracter personal criptate. Mai precis, nu au fost afectate nici sistemul de e-mail al întreprinderii, nici sistemele clienților utilizate pentru a avea acces la acesta. Întreprinderea utilizează expertiza unei societăți externe specializate în securitate cibernetică pentru a investiga incidentul. Sunt disponibile jurnale care urmăresc toate fluxurile de date care părăsesc întreprinderea (inclusiv e-mailul de ieșire). După analizarea jurnalelor și a datelor colectate de sistemele de detectare pe care întreprinderea le-a instalat, o investigație internă sprijinită de societatea externă specializată în securitate cibernetică a stabilit *cu certitudine* că autorul doar a criptat datele, fără a le exfiltra. Jurnalele nu arată niciun flux de date de ieșire în intervalul de timp în care a avut loc atacul. Datele cu caracter personal afectate de încălcare se referă la clienții și angajații întreprinderii, câteva zeci de persoane în total. O copie de rezervă a fost disponibilă cu ușurință, iar datele au fost recuperate la câteva ore după ce a avut loc atacul. Încălcarea nu a avut consecințe asupra activității de zi cu zi a operatorului. Nu a existat nicio întârziere în ceea ce privește plățile către angajați sau gestionarea cererilor clienților.

17. În acest caz, următoarele elemente au fost obținute din definiția unei „încălcări a securității datelor cu caracter personal”: o încălcare a securității a condus la modificarea ilegală a datelor cu caracter personal stocate și la accesul neautorizat la acestea.

2.1.1 CAZUL nr. 01 – Măsuri prealabile și evaluarea riscului

18. La fel ca în cazul tuturor riscurilor prezentate de actorii externi, probabilitatea ca un atac de tip ransomware să aibă succes poate fi redusă drastic prin înăsprirea securității mediului de control al datelor. Majoritatea acestor încălcări pot fi prevenite prin asigurarea luării de măsuri adecvate de securitate organizațională, fizică și tehnologică. Exemple de astfel de măsuri sunt gestionarea adecvată a corecțiilor software și utilizarea unui sistem adecvat de detectare a programelor malware. Existența unei copii de rezervă adecvate și separate va contribui la atenuarea consecințelor unui atac reușit, în cazul în care acesta se produce. În plus, un program de educare, formare și sensibilizare în materie de securitate (SETA) pentru angajați va contribui la prevenirea și recunoașterea acestui tip de atac. (O listă de măsuri recomandabile este disponibilă în secțiunea 2.5). Printre aceste măsuri, una dintre cele mai importante este o gestionare adecvată a corecțiilor software care asigură actualizarea sistemelor și remedierea tuturor vulnerabilităților cunoscute ale sistemelor implementate, întrucât majoritatea atacurilor ransomware exploatează vulnerabilități bine cunoscute.

19. La evaluarea riscurilor, operatorul ar trebui să investigheze încălcarea și să identifice tipul de cod dăunător pentru a înțelege posibilele consecințe ale atacului. Printre aceste riscuri care trebuie luate în considerare se numără riscul ca datele să fi fost exfiltrate fără a lăsa o urmă în jurnalele sistemelor.

20. În acest exemplu, atacatorul a avut acces la date cu caracter personal, iar confidențialitatea textului cifrat conținând date cu caracter personal în formă criptată a fost compromisă. Cu toate acestea, datele care ar fi putut fi exfiltrate nu pot fi citite sau utilizate de autor, cel puțin pentru moment. Tehnica de criptare utilizată de operatorul de date este conformă cu stadiul actual al tehnologiei. Cheia de decriptare nu a fost compromisă și probabil nu a putut fi determinată prin alte mijloace. În consecință, riscurile de încălcare a confidențialității pentru drepturile și libertățile persoanelor fizice sunt reduse la minimum, împiedicând progresul criptanalitic care face ca datele criptate să fie inteligibile în viitor.

21. Operatorul de date ar trebui să ia în considerare riscul pentru persoanele fizice ca urmare a încălcării[10]. În acest caz, se pare că riscurile pentru drepturile și libertățile persoanelor vizate rezultă din lipsa disponibilității datelor cu caracter personal, iar confidențialitatea datelor cu caracter personal nu este compromisă[11]. În acest exemplu, efectele negative ale încălcării au fost atenuate destul de curând după producerea încălcării. Existența unui regim de rezervă adecvat[12] face ca efectele încălcării să fie mai puțin grave și, în acest caz, operatorul a fost în măsură să îl utilizeze în mod eficace.

22. În ceea ce privește gravitatea consecințelor pentru persoanele vizate, au putut fi identificate doar consecințe minore, deoarece datele afectate au fost recuperate în câteva ore, încălcarea nu a avut consecințe asupra funcționării zilnice a operatorului și nu a avut niciun efect semnificativ asupra persoanelor vizate (de exemplu, plățile către angajați sau tratarea cererilor clienților).

2.1.2 CAZUL nr. 01 – Atenuare și obligații

23. În lipsa unei copii de rezervă, sunt puține măsuri pe care operatorul le poate lua pentru a remedia pierderea datelor cu caracter personal, iar datele trebuie colectate din nou. Totuși, în acest caz particular, impactul atacului ar putea fi limitat în mod eficient prin resetarea tuturor sistemelor compromise la o stare „curată" cunoscută ca nefiind infectată cu coduri dăunătoare, prin remedierea vulnerabilităților și prin recuperarea datelor afectate la scurt timp după atac. În lipsa unei copii de rezervă, datele se pierd, iar gravitatea poate crește, deoarece și riscurile sau efectele asupra persoanelor se pot agrava.

24. Promptitudinea unei recuperări eficace a datelor din copia de rezervă ușor accesibilă este o variabilă-cheie în analizarea încălcării. Specificarea unui interval de timp adecvat pentru recuperarea datelor compromise depinde de circumstanțele unice ale încălcării în cauză. RGPD prevede că o încălcare a securității datelor cu caracter personal trebuie notificată fără întârzieri nejustificate și, dacă este posibil, în cel mult 72 de ore. Prin urmare, s-ar putea stabili că depășirea termenului de 72 de ore nu este recomandabilă în niciun caz, dar atunci când este vorba de cazuri cu un nivel de risc ridicat, chiar și respectarea acestui termen poate fi considerată nesatisfăcătoare.

25. În acest caz, în urma unei evaluări detaliate a impactului și a unui proces de răspuns la incidente, operatorul a stabilit că este puțin probabil ca încălcarea să genereze un risc pentru drepturile și libertățile persoanelor

---

[10] Pentru orientări privind operațiunile de prelucrare „susceptibile să genereze un risc ridicat", a se vedea documentul „Orientări privind evaluarea impactului asupra protecției datelor (DPIA) și modul în care se determină dacă prelucrarea este «susceptibilă să genereze un risc ridicat» în sensul Regulamentului 2016/679" al grupului de lucru A29, WP248 rev. 01, – aprobate de CEPD, PB, https://ec.europa.eu/newsroom/article29/items/611236, p. 9.

[11] Din punct de vedere tehnic, criptarea datelor va implica „accesul" la datele originale, iar în cazul ransomware, ștergerea originalului – datele trebuie să fie accesate prin codul ransomware pentru a fi criptate și pentru a elimina datele originale. Atacatorul poate face o copie a datelor originale înainte de ștergere, dar datele cu caracter personal nu vor fi întotdeauna extrase. Pe măsură ce investigația unui operator de date progresează, pot apărea noi informații care să modifice această evaluare. Accesul care duce la distrugerea ilegală, pierderea, modificarea, divulgarea neautorizată a datelor cu caracter personal sau la un risc la adresa securității unei persoane vizate, chiar și fără interpretarea datelor, poate fi la fel de grav ca accesul la datele cu caracter personal.

[12] Procedurile de rezervă ar trebui să fie structurate, coerente și repetabile. Exemple de proceduri de rezervă sunt metoda 3-2-1 și metoda „bunic-tată-fiu". Orice metodă ar trebui să fie întotdeauna testată din punctul de vedere al eficacității în ceea ce privește acoperirea și atunci când datele trebuie restabilite. Testarea ar trebui, de asemenea, repetată la anumite intervale de timp și, în special, atunci când apar modificări ale operațiunii de prelucrare sau ale circumstanțelor acesteia, pentru a se asigura integritatea sistemului.

fizice și, prin urmare, nu este necesară comunicarea către persoanele vizate, iar încălcarea nu necesită o notificare către AS. Cu toate acestea, la fel ca în cazul tuturor încălcărilor securității datelor, aceasta ar trebui să fie documentată în conformitate cu articolul 33 alineatul (5). De asemenea, este posibil ca organizația să trebuiască (sau ulterior să i se solicite de către AS)să își actualizeze și să își remedieze măsurile și procedurile organizatorice și tehnice de gestionare a securității datelor cu caracter personal și de atenuare a riscurilor. În cadrul acestei actualizări și remedieri, organizația ar trebui să investigheze în detaliu încălcarea și să identifice cauzele și metodele utilizate de autor pentru a preveni eventuale evenimente similare în viitor.

Acțiuni necesare în funcție de riscurile identificate		
Documentarea internă	Notificare către AS	Comunicare către persoanele vizate
✓	X	X

2.2 CAZUL nr. 02: Ransomware fără copie de rezervă adecvată

Unul dintre calculatoarele utilizate de o întreprindere agricolă a fost expus unui atac de tip ransomware, iar datele din calculatorul respectiv au fost criptate de atacator. Întreprinderea utilizează expertiza unei societăți externe specializate în securitate cibernetică pentru a-și monitoriza rețeaua. Sunt disponibile jurnale care urmăresc toate fluxurile de date care părăsesc întreprinderea (inclusiv e-mailul de ieșire). După analizarea jurnalelor și a datelor colectate de celelalte sisteme de detectare, investigația internă sprijinită de societatea specializată în securitate cibernetică a stabilit că autorul doar a criptat datele, fără a le exfiltra. Jurnalele nu arată niciun flux de date de ieșire în intervalul de timp în care a avut loc atacul. Datele cu caracter personal afectate de încălcare se referă la angajații și clienții societății, câteva zeci de persoane în total. Nu au fost afectate categorii speciale de date. Nu a fost disponibilă nicio copie de rezervă în format electronic. Majoritatea datelor au fost recuperate din copii de rezervă pe suport de hârtie. Recuperarea datelor a durat 5 zile lucrătoare și a condus la întârzieri minore în livrarea comenzilor către clienți.

2.2.1 CAZUL nr. 02 – Măsuri prealabile și evaluarea riscului

26. Operatorul de date ar fi trebuit să adopte aceleași măsuri prealabile precum cele menționate în partea 2.1 și în secțiunea 2.9. Principala diferență față de cazul anterior este lipsa unei copii de rezervă electronice și lipsa criptării datelor stocate pe hard disk. Acest lucru duce la diferențe critice în etapele următoare.

27. La evaluarea riscurilor, operatorul ar trebui să investigheze metoda de infiltrare și să identifice tipul de cod dăunător pentru a înțelege posibilele consecințe ale atacului. În acest exemplu, ransomware-ul a criptat datele cu caracter personal fără a le exfiltra. Drept urmare, se pare că riscurile pentru drepturile și libertățile persoanelor vizate rezultă din lipsa disponibilității datelor cu caracter personal, iar confidențialitatea datelor cu caracter personal nu este compromisă. O examinare aprofundată a jurnalelor firewall și a implicațiilor acestora este esențială pentru stabilirea riscului. Operatorul de date ar trebui să prezinte, la cerere, constatările de fapt ale acestor investigații.

28. Operatorul de date trebuie să țină seama de faptul că, în cazul unui atac mai sofisticat, programele malware au funcționalitatea de a edita fișiere jurnal și de a elimina urmele. Astfel – având în vedere că jurnalele nu sunt transmise sau reproduse către un server central de jurnale – chiar și după o investigație aprofundată care a stabilit că datele cu caracter personal nu au fost exfiltrate de atacator, operatorul de date nu poate afirma că lipsa unei înregistrări în jurnal dovedește absența unei exfiltrări și, prin urmare, probabilitatea unei încălcări a confidențialității nu poate fi înlăturată în totalitate.

29. Operatorul de date ar trebui să evalueze riscurile unei astfel de încălcări[13] în cazul în care datele au fost accesate de atacator. În cursul evaluării riscurilor, operatorul de date ar trebui, de asemenea, să ia în considerare natura, sensibilitatea, volumul și contextul datelor cu caracter personal afectate de încălcare. În acest caz, nu sunt afectate categorii speciale de date cu caracter personal, iar cantitatea de date încălcate și numărul persoanelor vizate afectate sunt scăzute.

30. Colectarea de informații exacte privind accesul neautorizat este esențială pentru determinarea nivelului de risc și prevenirea unui atac nou sau continuu. Dacă datele ar fi fost copiate din baza de date, ar fi fost în mod evident un factor de contribuție la creșterea riscurilor. Atunci când există incertitudine cu privire la particularitățile accesului nelegitim, ar trebui luat în considerare scenariul cel mai pesimist, iar riscul ar trebui evaluat în consecință.

31. Absența unei baze de date de rezervă poate fi considerată un factor de creștere a riscurilor, în funcție de gravitatea consecințelor pentru persoanele vizate care rezultă din lipsa disponibilității datelor.

2.2.2 CAZUL nr. 02 – Atenuare și obligații

32. În lipsa unei copii de rezervă, sunt puține măsuri pe care operatorul le poate lua pentru a remedia pierderea datelor cu caracter personal, iar datele trebuie colectate din nou, cu excepția cazului în care sunt disponibile alte surse (de exemplu, e-mailuri de confirmare a comenzilor). În lipsa unei copii de rezervă, datele pot fi pierdute, iar gravitatea va depinde de impactul asupra persoanelor.

33. Recuperarea datelor nu ar trebui să fie excesiv de problematică[14] dacă datele sunt încă disponibile pe suport de hârtie, dar, având în vedere lipsa unei baze de date electronice de rezervă, se consideră că este necesară o notificare către AS, deoarece recuperarea datelor a necesitat un anumit timp și ar putea cauza unele întârzieri în livrarea comenzilor către clienți, și este posibil ca un volum considerabil de metadate (de exemplu, jurnale, marcaje temporale) să nu poată fi recuperate.

34. Informarea persoanelor vizate cu privire la încălcare poate depinde, de asemenea, de perioada în care datele cu caracter personal nu sunt disponibile și de dificultățile pe care încălcarea le-ar putea cauza în activitatea operatorului (de exemplu, întârzieri în transferarea plăților către angajați). Întrucât aceste întârzieri ale plăților și livrărilor pot duce la pierderi financiare pentru persoanele ale căror date au fost compromise, s-ar putea susține, de asemenea, că încălcarea ar putea genera un risc ridicat. De asemenea, s-ar putea să nu fie posibil să se evite informarea persoanelor vizate în cazul în care contribuția lor este necesară pentru recuperarea datelor criptate.

35. Acest caz servește drept exemplu pentru un atac de tip ransomware cu risc la adresa drepturilor și libertăților persoanelor vizate, dar care nu atinge un grad ridicat de risc. Acest lucru ar trebui să fie documentat în conformitate cu articolul 33 alineatul (5) și notificat AS în conformitate cu articolul 33 alineatul (1). De asemenea, este posibil ca organizația să trebuiască (sau să i se solicite de către AS) să își actualizeze și să își remedieze măsurile și procedurile organizatorice și tehnice de gestionare a securității datelor cu caracter personal și de atenuare a riscurilor.

---

[13] Pentru orientări privind operațiunile de prelucrare „susceptibile să genereze un risc ridicat”, a se vedea nota de subsol 10 de mai sus.

[14] Acest lucru va depinde de complexitatea și structura datelor cu caracter personal. În scenariile cele mai complexe, restabilirea integrității datelor, coerența cu metadatele, asigurarea relațiilor corecte în cadrul structurilor de date și verificarea acurateței datelor pot necesita resurse și eforturi semnificative.

Acțiuni necesare în funcție de riscurile identificate		
Documentarea internă	Notificare către AS	Comunicare către persoanele vizate
✓	✓	X

2.3 CAZUL nr. 03: Ransomware cu copie de rezervă și fără exfiltrare într-un spital

Sistemul informatic al unui spital/centru medical a fost expus unui atac de tip ransomware, iar o parte semnificativă a datelor sale au fost criptate de atacator. Întreprinderea utilizează expertiza unei societăți externe specializate în securitate cibernetică pentru a-și monitoriza rețeaua. Sunt disponibile jurnale care urmăresc toate fluxurile de date care părăsesc întreprinderea (inclusiv e-mailul de ieșire). După analizarea jurnalelor și a datelor colectate de celelalte sisteme de detectare, investigația internă sprijinită de societatea specializată în securitate cibernetică a stabilit că autorul doar a criptat datele, fără a le exfiltra. Jurnalele nu arată niciun flux de date de ieșire în intervalul de timp în care a avut loc atacul. Datele cu caracter personal afectate de încălcare se referă la angajați și pacienți, care reprezintă mii de persoane. Au fost disponibile copii de rezervă în format electronic. Majoritatea datelor au fost recuperate, dar această operațiune a durat 2 zile lucrătoare și a condus la întârzieri majore în tratarea pacienților, o serie de intervenții chirurgicale fiind anulate/amânate, și la o scădere a nivelului serviciilor din cauza indisponibilității sistemelor.

2.3.1 CAZUL nr. 03 – Măsuri prealabile și evaluarea riscurilor

36. Operatorul de date ar fi trebuit să adopte aceleași măsuri prealabile precum cele menționate în partea 2.1 și în secțiunea 2.5. Diferența majoră față de cazul anterior este gravitatea ridicată a consecințelor pentru o parte substanțială a persoanelor vizate[15].

37. Cantitatea de date afectate de încălcare și numărul persoanelor vizate afectate sunt ridicate, deoarece spitalele prelucrează, de obicei, cantități mari de date. Indisponibilitatea datelor are un impact puternic asupra unei părți substanțiale a persoanelor vizate. În plus, există un risc rezidual de gravitate ridicată pentru confidențialitatea datelor pacienților.

38. Tipul de încălcare, natura, sensibilitatea și volumul datelor cu caracter personal afectate de încălcare sunt importante. Chiar dacă a existat o copie de rezervă a datelor și acestea au putut fi recuperate în câteva zile, există în continuare un risc ridicat din cauza gravității consecințelor pentru persoanele vizate care rezultă din lipsa disponibilității datelor în momentul atacului și în zilele următoare.

2.3.2 CAZUL nr. 03 – Atenuare și obligații

39. Se consideră că este necesară o notificare către AS, deoarece sunt implicate categorii speciale de date cu caracter personal, iar recuperarea datelor ar putea dura mult timp, ceea ce ar duce la întârzieri majore în

[15] Pentru orientări privind operațiunile de prelucrare „susceptibile să genereze un risc ridicat”, a se vedea nota de subsol 10 de mai sus.

îngrijirea pacienților. Informarea persoanelor vizate cu privire la încălcare este necesară din cauza impactului pentru pacienți, chiar și după recuperarea datelor criptate. Deși datele referitoare la toți pacienții tratați în spital în ultimii ani au fost criptate, au fost afectați numai pacienții care erau programați să fie tratați în spital în perioada în care sistemul informatic nu a fost disponibil. Operatorul ar trebui să comunice direct acestor pacienți încălcarea securității datelor. Comunicarea directă către ceilalți pacienți, în condițiile în care este posibil ca unii dintre aceștia să nu fi fost la spital de mai mult de douăzeci de ani, ar putea să nu fie necesară ca urmare a excepției de la articolul 34 alineatul (3) litera (c). În această situație, ar trebui să fie efectuată în schimb o comunicare publică[16] sau să se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace. În acest caz, spitalul ar trebui să facă public atacul de tip ransomware și efectele acestuia.

40. Acest caz servește drept exemplu pentru un atac de tip ransomware cu risc ridicat la adresa drepturilor și libertăților persoanelor vizate. Aceasta ar trebui să fie documentat în conformitate cu articolul 33 alineatul (5), notificat AS în conformitate cu articolul 33 alineatul (1) și comunicat persoanelor vizate în conformitate cu articolul 34 alineatul (1). De asemenea, organizația trebuie să își actualizeze și să își remedieze măsurile și procedurile organizatorice și tehnice de gestionare a securității datelor cu caracter personal și de atenuare a riscurilor.

Acțiuni necesare în funcție de riscurile identificate		
Documentarea internă	Notificare către AS	Comunicare către persoanele vizate
✓	✓	✓

2.4 CAZUL nr. 04: Ransomware fără copii de rezervă și cu exfiltrare

Serverul unei societăți de transport public a fost expus unui atac de tip ransomware, iar datele sale au fost criptate de atacator. Potrivit constatărilor investigației interne, nu numai că autorul a criptat datele, dar le-a și exfiltrat. Tipul de date afectate de încălcare a fost reprezentat de datele cu caracter personal ale clienților și angajaților, precum și ale câtorva mii de persoane care utilizau serviciile societății (de exemplu, cele care au achiziționat bilete online). În afară de datele de identitate de bază, încălcarea a afectat și numere ale cărților de identitate și date financiare, cum ar fi detalii ale cărților de credit. Exista o bază de date de rezervă, dar aceasta a fost, de asemenea, criptată de atacator.

2.4.1 CAZUL nr. 04 – Măsuri prealabile și evaluarea riscului

41. Operatorul de date ar fi trebuit să adopte aceleași măsuri prealabile precum cele menționate în partea 2.1 și în secțiunea 2.5. Deși a existat o copie de rezervă, aceasta a fost, de asemenea, afectată de atac. Numai

[16] Astfel cum se explică în considerentul 86 din RGPD, „[c]omunicările către persoanele vizate ar trebui efectuate în cel mai scurt timp posibil în mod rezonabil și în strânsă cooperare cu autoritatea de supraveghere, respectându-se orientările furnizate de aceasta sau de alte autorități competente, cum ar fi autoritățile de aplicare a legii. De exemplu, necesitatea de a atenua un risc imediat de producere a unui prejudiciu ar presupune comunicarea cu promptitudine către persoanele vizate, în timp ce necesitatea de a implementa măsuri corespunzătoare împotriva încălcării în continuare a securității datelor cu caracter personal sau împotriva unor încălcări similare ale securității datelor cu caracter personal ar putea justifica un termen mai îndelungat pentru comunicare”.

acest mecanism ridică semne de întrebare cu privire la calitatea măsurilor anterioare de securitate informatică ale operatorului și ar trebui să fie examinat în continuare în timpul investigației, deoarece, într-un regim de back-up bine conceput, trebuie stocate în siguranță mai multe copii de rezervă fără acces din sistemul principal; în caz contrar, acestea ar putea fi compromise în cadrul aceluiași atac. În plus, atacurile de tip ransomware pot rămâne nedescoperite timp de mai multe zile, criptând lent datele utilizate rar. Astfel, mai multe copii de rezervă pot deveni inutile; prin urmare, ar trebui, de asemenea, să se facă periodic back-up-uri și acestea să fie izolate. Acest lucru ar contribui la creșterea probabilității de recuperare, deși cu pierderi crescute de date.

42. Această încălcare se referă nu numai la disponibilitatea datelor, ci și la confidențialitate, întrucât este posibil ca atacatorul să fi modificat și/sau copiat date de pe server. Prin urmare, tipul de încălcare generează un risc ridicat[17].

43. Natura, sensibilitatea și volumul datelor cu caracter personal determină o creștere și mai mare a riscurilor, deoarece numărul persoanelor afectate este ridicat, la fel precum cantitatea totală de date cu caracter personal afectate. Pe lângă datele de identitate de bază, sunt implicate și documente de identitate și date financiare, cum ar fi detalii ale cărților de credit. O încălcare a securității pentru aceste tipuri de date prezintă un risc ridicat în sine și, dacă acestea sunt prelucrate împreună, ar putea fi utilizate, printre altele, pentru furtul sau frauda de identitate.

44. Din cauza logicii serverului sau a controalelor organizatorice defectuoase, fișierele de rezervă au fost afectate de atacul ransomware, împiedicând recuperarea datelor și sporind riscul.

45. Această încălcare a securității datelor prezintă un risc ridicat pentru drepturile și libertățile persoanelor fizice, deoarece ar putea conduce, probabil, atât la pierderi materiale (de exemplu, pierderi financiare deoarece detaliile cărții de credit au fost afectate), cât și la prejudicii nemateriale (de exemplu, furtul sau frauda de identitate, deoarece datele cărții de identitate au fost afectate).

2.4.2 CAZUL nr. 04 – Atenuare și obligații

46. Comunicarea către persoanele vizate este esențială, astfel încât acestea să poată lua măsurile necesare pentru a evita prejudiciile materiale (de exemplu, blocarea cărților lor de credit).

47. Pe lângă documentarea încălcării în conformitate cu articolul 33 alineatul (5), o notificare către AS este, de asemenea, obligatorie în acest caz [articolul 33 alineatul (1)], iar operatorul este, de asemenea, obligat să comunice încălcarea persoanelor vizate [articolul 34 alineatul (1)]. Comunicarea încălcării ar putea fi efectuată către fiecare persoană în parte, însă în cazul persoanelor ale căror date de contact nu sunt disponibile, operatorul ar trebui să comunice informațiile în mod public, cu condiția ca o astfel de comunicare să nu fie susceptibilă să genereze consecințe negative suplimentare pentru persoanele vizate, de exemplu prin intermediul unei notificări pe site-ul său. În acest din urmă caz, este necesară o comunicare precisă și clară, la vedere, pe pagina principală a operatorului, cu trimiteri exacte la dispozițiile relevante din RGPD. De asemenea, ar putea fi necesar ca organizația să își actualizeze și să își remedieze măsurile și procedurile organizatorice și tehnice de gestionare a securității datelor cu caracter personal și de atenuare a riscurilor.

Acțiuni necesare în funcție de riscurile identificate

[17] Pentru orientări privind operațiunile de prelucrare „susceptibile să genereze un risc ridicat”, a se vedea nota de subsol 10 de mai sus.

Documentarea internă	Notificare către AS	Comunicare către persoanele vizate
✓	✓	✓

2.5 Măsuri organizatorice și tehnice de prevenire/atenuare a impactului atacurilor ransomware

48. Faptul că un atac de tip ransomware ar fi putut avea loc este, de obicei, un semn al uneia sau al mai multor vulnerabilități ale sistemului operatorului. Acest lucru este valabil și în cazurile de atac de tip ransomware în care datele cu caracter personal au fost criptate, dar nu au fost exfiltrate. Indiferent de rezultatul și consecințele atacului, efectuarea unei evaluări atotcuprinzătoare a sistemului de securitate a datelor – cu un accent deosebit pe securitatea informatică – este extrem de importantă. Deficiențele și breșele de securitate identificate trebuie documentate și abordate fără întârziere.

49. Măsuri recomandate:

- (Lista următoarelor măsuri nu este în niciun caz exclusivă sau cuprinzătoare. Mai degrabă, obiectivul este de a oferi idei de prevenire și soluții posibile. Fiecare activitate de prelucrare diferă de celelalte; prin urmare operatorul ar trebui să ia decizia cu privire la măsurile cele mai adecvate în situația specifică.)
- actualizarea firmware-ului, a sistemului de operare și a aplicației software pe servere, pe dispozitivele client, pe componentele active ale rețelei și pe orice alte dispozitive instalate pe aceeași rețea LAN (inclusiv pe dispozitivele Wi-Fi); asigurarea unor măsuri adecvate de securitate informatică, asigurarea eficacității acestora și actualizarea periodică a acestora atunci când prelucrarea sau circumstanțele se schimbă sau evoluează. Aceasta include păstrarea unor evidențe detaliate ale corecțiilor aplicate cu mărcile temporale aferente;
- proiectarea și organizarea sistemelor și a infrastructurii de prelucrare pentru a segmenta sau a izola sistemele și rețelele de date cu scopul de a evita propagarea programelor malware în cadrul organizației și către sistemele externe;
- existența unei proceduri de back-up actualizate, sigure și testate; suporturile pentru copii de rezervă pe termen mediu și lung ar trebui să fie păstrate separat de alte mijlocare de stocare a datelor operaționale și să nu fie accesibile părților terțe, nici măcar în cazul unui atac reușit (cum ar fi copii de rezervă incrementale zilnice și copii de rezervă complete săptămânale);
- deținerea/obținerea unui software anti-malware adecvat, actualizat, eficace și integrat;
- existența unui firewall și a unui sistem adecvat, actualizat, eficace și integrat de detectare și prevenire a intruziunilor; direcționarea traficului în rețea prin intermediul sistemului firewall/de detectare a intruziunilor, chiar și în cazul birourilor la domiciliu sau al unei activități mobile (de exemplu, prin utilizarea de conexiuni VPN la mecanismele de securitate organizațională atunci când se accesează internetul);
- formarea angajaților cu privire la metodele de recunoaștere și prevenire a atacurilor informatice. Operatorul ar trebui să furnizeze mijloace pentru a se stabili dacă e-mailurile și mesajele obținute prin alte mijloace de comunicare sunt autentice și de încredere. Angajații ar trebui să fie instruiți să recunoască momentul în care un astfel de atac s-a concretizat, modul în care să deconecteze dispozitivul final de la rețea și obligația de a-l raporta imediat agentului de securitate;
- sublinierea necesității de a se identifica tipul de cod dăunător pentru a vedea consecințele atacului și pentru a putea găsi măsurile adecvate de atenuare a riscului; În cazul în care un atac de tip ransomware a avut succes și nu există nicio copie de rezervă disponibilă, se pot aplica instrumente disponibile, cum

ar fi cele ale proiectului „No more ransom” (nomoreransom.org) pentru a extrage date. Cu toate acestea, în cazul în care este disponibilă o copie de rezervă sigură, se recomandă reintroducerea datelor din aceasta;

- transmiterea sau reproducerea tuturor jurnalelor către un server central de jurnale (inclusiv, eventual, semnarea sau marcarea temporală criptografică a înregistrărilor din jurnal);
- criptarea puternică și autentificarea multifactorială, în special pentru accesul administrativ la sistemele informatice, gestionarea adecvată a cheilor și a parolei;
- efectuarea de teste periodice de vulnerabilitate și penetrare cibernetică;
- crearea unei echipe de intervenție în caz de incidente de securitate informatică (CSIRT) sau a unei echipe de răspuns la incidente de securitate cibernetică (CERT) în cadrul organizației sau aderarea la o CSIRT/CERT colectivă; elaborarea unui plan de intervenție în caz de incidente, a unui plan de recuperare în caz de dezastru și a unui plan de asigurare a continuității activității și asigurarea faptului că acestea sunt testate în detaliu;
- la evaluarea contramăsurilor, analiza riscului ar trebui revizuită, testată și actualizată.

3 ATACURI ÎNSOȚITE DE EXFILTRAREA DATELOR

50. Atacurile care exploatează vulnerabilitățile serviciilor oferite de operator părților terțe prin internet, de exemplu, prin intermediul unor atacuri de injecție (de exemplu, injecție SQL, atac de tip „path traversal”), compromiterea site-urilor și alte metode similare, pot semăna cu atacurile de tip ransomware în sensul că riscul provine din acțiunea unei terțe părți neautorizate, dar aceste atacuri vizează, de regulă, copierea, exfiltrarea și utilizarea abuzivă a datelor cu caracter personal în anumite scopuri rău-intenționate. Prin urmare, acestea reprezintă în principal încălcări ale confidențialității și, eventual, ale integrității datelor. În același timp, dacă operatorul cunoaște caracteristicile acestui tip de încălcări, există mai multe măsuri care pot reduce în mod substanțial riscul executării cu succes a unui atac.

3.1 CAZUL nr. 05: Exfiltrarea datelor din formularele de cerere de angajare de pe un site

O agenție de ocupare a forței de muncă a fost victima unui atac cibernetic, prin care pe site-ul său a fost introdus un cod dăunător. Acest cod dăunător a permis ca informațiile cu caracter personal transmise prin intermediul formularelor de cerere de angajare online și stocate pe serverul web să fie accesibile persoanelor neautorizate. Este posibil să fi fost afectate 213 astfel de formulare, iar după analizarea datelor afectate, s-a stabilit că nu au fost afectate categorii speciale de date în cadrul încălcării. Setul de instrumente de tip malware instalat avea funcționalități care au permis atacatorului să elimine orice istoric de exfiltrare și a permis, de asemenea, monitorizarea prelucrării pe server și captarea datelor cu caracter personal. Setul de instrumente a fost descoperit doar la o lună după instalare.

3.1.1 CAZUL nr. 05 – Măsuri prealabile și evaluarea riscului

51. Securitatea mediului operatorului de date este extrem de importantă, deoarece majoritatea acestor încălcări pot fi prevenite prin asigurarea faptului că toate sistemele sunt actualizate în mod constant, că datele sensibile sunt criptate și că aplicațiile sunt dezvoltate în conformitate cu standarde înalte de securitate, cum ar fi autentificarea puternică, măsuri împotriva atacurilor prin forță brută, a „evitării” sau a

„sanitizării”[18] intrărilor utilizatorilor etc. De asemenea, sunt necesare audituri periodice de securitate informatică, evaluări ale vulnerabilității și teste de penetrare cibernetică pentru a detecta în prealabil aceste tipuri de vulnerabilități și pentru a le remedia. În acest caz particular, este posibil ca instrumentele de monitorizare a integrității fișierelor în mediul de producție să fi contribuit la detectarea injectării codurilor. (O listă de măsuri recomandabile este disponibilă în secțiunea 3.7).

52. Operatorul ar trebui să înceapă întotdeauna să investigheze încălcarea prin identificarea tipului de atac și a metodelor folosite, pentru a evalua ce măsuri trebuie luate. Pentru ca acest lucru să se realizeze rapid și eficient, operatorul de date ar trebui să dispună de un plan de răspuns la incidente care să specifice măsurile rapide și necesare pentru a prelua controlul asupra incidentului. În acest caz particular, tipul de încălcare a fost un factor de creștere a riscului, deoarece nu numai că a fost restricționată confidențialitatea datelor, dar infiltratorul a avut, de asemenea, mijloacele de a face modificări în sistem, astfel încât integritatea datelor a devenit, de asemenea, discutabilă.

53. Natura, sensibilitatea și volumul datelor cu caracter personal afectate de încălcare ar trebui evaluate pentru a se stabili în ce măsură încălcarea a afectat persoanele vizate. Deși nu au fost afectate categorii speciale de date cu caracter personal, datele accesate conțin informații considerabile despre persoanele fizice din formularele online, iar aceste date ar putea fi utilizate abuziv în mai multe moduri (marketing nesolicitat, furt de identitate etc.), astfel încât gravitatea consecințelor ar trebui să crească riscul la adresa drepturilor și libertăților persoanelor vizate[19].

3.1.2 CAZUL nr. 05 – Atenuare și obligații

54. Dacă este posibil, după soluționarea problemei, baza de date ar trebui comparată cu cea stocată într-o copie de rezervă securizată. Experiența dobândită în urma încălcării ar trebui să fie utilizată la actualizarea infrastructurii informatice. Operatorul de date ar trebui să readucă toate sistemele informatice afectate la o stare „curată” cunoscută, să remedieze vulnerabilitatea și să pună în aplicare noi măsuri de securitate pentru a evita încălcări similare ale securității datelor în viitor, de exemplu verificări ale integrității dosarelor și audituri de securitate. În cazul în care datele cu caracter personal nu au fost doar exfiltrate, ci și șterse, operatorul trebuie să ia măsuri sistematice pentru a recupera datele cu caracter personal în starea în care se aflau înainte de încălcare. Ar putea fi necesar să se aplice copii de rezervă complete, modificări incrementale și apoi, eventual, să se efectueze din nou prelucrarea de la ultima copie de rezervă incrementală – iar pentru aceasta, operatorul trebuie să poată să fie în măsură să reproducă modificările efectuate de la ultima copie de rezervă. În acest sens, ar putea fi necesar ca sistemul operatorului să fie astfel conceput încât să păstreze fișierele de intrare zilnice în cazul în care acestea trebuie prelucrate din nou și sunt necesare o metodă solidă de stocare și o politică adecvată de păstrare.

55. Având în vedere cele de mai sus, întrucât încălcarea este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice, persoanele vizate ar trebui să fie cu siguranță informate cu privire la aceasta [articolul 34 alineatul (1)], ceea ce înseamnă, bineînțeles, că AS relevantă (relevante) ar trebui, de asemenea, să fie implicată (implicate) sub forma unei notificări a încălcării securității datelor.

[18] „Evadarea” sau „igienizarea” datelor de intrare ale utilizatorilor reprezintă o formă de validare a intrărilor, care asigură faptul că într-un sistem informatic se introduc numai date formatate în mod corespunzător.

[19] Pentru orientări privind operațiunile de prelucrare „susceptibile să genereze un risc ridicat”, a se vedea nota de subsol 10 de mai sus.

Documentarea încălcării este obligatorie în conformitate cu articolul 33 alineatul (5) din RGPD și facilitează evaluarea situației.

Acțiuni necesare în funcție de riscurile identificate		
Documentarea internă	Notificare către AS	Comunicare către persoanele vizate
✓	✓	✓

3.2 CAZUL nr. 06: Exfiltrarea parolei organizate ca hash de pe un site

O vulnerabilitate de tip injecție SQL a fost exploatată pentru a obține acces la o bază de date a serverului unui site de gătit. Utilizatorilor li s-a permis doar să aleagă pseudonime arbitrare ca nume de utilizator. Utilizarea adreselor de e-mail în acest scop a fost descurajată. Parolele stocate în baza de date au fost organizate ca hash cu ajutorul unui algoritm puternic, iar funcția „salt" nu a fost compromisă. Date afectate: parole organizate ca hash aparținând unui număr de 1 200 de utilizatori. Din motive de siguranță, operatorul a informat persoanele vizate cu privire la încălcare prin e-mail și le-a solicitat să își schimbe parolele, în special dacă aceeași parolă a fost utilizată și pentru alte servicii.

3.2.1 CAZUL nr. 06 – Măsuri prealabile și evaluarea riscului

56. În acest caz particular, confidențialitatea datelor este compromisă, însă parolele din baza de date au fost organizate ca hash printr-o metodă actualizată, ceea ce ar reduce riscul în ceea ce privește natura, sensibilitatea și volumul datelor cu caracter personal. Acest caz nu prezintă riscuri pentru drepturile și libertățile persoanelor vizate.

57. În plus, nicio informație de contact (de exemplu, adrese de e-mail sau numere de telefon) aparținând persoanelor vizate nu a fost compromisă, ceea ce înseamnă că nu există niciun risc semnificativ pentru persoanele vizate de a fi vizate de tentative de fraudă (de exemplu, primirea de e-mailuri de phishing sau mesaje text și apeluri telefonice frauduloase). Nu au fost implicate categorii speciale de date cu caracter personal.

58. Unele nume de utilizatori ar putea fi considerate date cu caracter personal, dar politica site-ului nu permite conotații negative. Trebuie remarcat totuși că evaluarea riscurilor se poate modifica[20], dacă tipul de site și datele accesate ar putea dezvălui categorii speciale de date cu caracter personal (de exemplu, site-ul unui partid politic sau al unui sindicat). Utilizarea criptării de ultimă generație ar putea atenua efectele negative ale încălcării. Asigurarea permiterii unui număr limitat de încercări de conectare va împiedica succesul atacurilor de autentificare prin forță brută, reducând astfel în mare măsură riscurile impuse de atacatorii care cunosc deja numele de utilizator.

3.2.2 CAZUL nr. 06 – Atenuare și obligații

59. În unele cazuri, comunicarea către persoanele vizate ar putea fi considerată un factor atenuant, întrucât acestea pot, de asemenea, să ia măsurile necesare pentru a evita alte prejudicii cauzate de încălcare, de exemplu prin schimbarea parolei. În acest caz, notificarea nu a fost obligatorie, dar, în multe cazuri, poate fi considerată o bună practică.

[20] Pentru orientări privind operațiunile de prelucrare „susceptibile să genereze un risc ridicat", a se vedea nota de subsol 10 de mai sus.

60. Operatorul de date ar trebui să corecteze vulnerabilitatea și să pună în aplicare noi măsuri de securitate pentru a evita încălcări similare ale securității datelor în viitor, cum ar fi, de exemplu, auditurile sistematice de securitate ale site-ului.

61. Încălcarea ar trebui să fie documentată în conformitate cu articolul 33 alineatul (5), dar nu este necesară nicio notificare sau comunicare.

62. De asemenea, este recomandabil să se comunice persoanelor vizate o încălcare care implică parole, chiar și atunci când parolele au fost stocate utilizând o funcție „salted hash" cu un algoritm care respectă stadiul actual al tehnologiei. Este preferabil să se utilizeze metode de autentificare care să evite necesitatea prelucrării parolelor pe partea serverului. Persoanelor vizate ar trebui să li se ofere posibilitatea de a lua măsuri adecvate cu privire la propriile parole.

Acțiuni necesare în funcție de riscurile identificate		
Documentarea internă	Notificare către AS	Comunicare către persoanele vizate
✓	X	X

3.3 CAZUL nr. 07: Atac de tip „credential stuffing" (atac automat ce presupune preluarea controlului asupra unor conturi) ce vizează un site bancar

O bancă a fost victima unui atac cibernetic ce a vizat unul dintre site-urile sale de servicii bancare electronice. Atacul a avut ca scop enumerarea tuturor identificatorilor de utilizator de conectare posibili, utilizând o parolă slabă fixă. Parolele conțin 8 cifre. Din cauza vulnerabilității site-ului, în unele cazuri au fost divulgate atacatorului informații privind persoanele vizate (nume, prenume, sex, data și locul nașterii, codul fiscal, codurile de identificare a utilizatorului), chiar dacă parola utilizată nu mai era corectă sau contul bancar nu mai era activ. Au fost afectate aproximativ 100 000 de persoane vizate. Dintre acestea, atacatorul s-a conectat cu succes la aproximativ 2 000 de conturi care utilizau parola slabă încercată de atacator. Ulterior, operatorul a fost în măsură să identifice toate încercările nelegitime de conectare. Operatorul de date a putut confirma că, în conformitate cu verificările antifraudă, de la aceste conturi nu s-a efectuat nicio tranzacție în timpul atacului. Banca a avut cunoștință de încălcarea securității datelor deoarece centrul său de operațiuni de securitate a detectat un număr mare de cereri de conectare adresate site-ului. Ca răspuns, operatorul a dezactivat posibilitatea de a conectare la site prin deconectarea acestuia și prin resetarea forțată a parolelor conturilor compromise. Operatorul a comunicat încălcarea numai utilizatorilor care dețineau conturile compromise, și anume utilizatorilor ale căror parole au fost compromise sau ale căror date au fost divulgate.

3.3.1 CAZUL nr. 07 – Măsuri prealabile și evaluarea riscului

63. Este important să se menționeze că operatorii care prelucrează date cu un caracter foarte personal[21] au o responsabilitate mai mare în ceea ce privește asigurarea unei securități adecvate a datelor, de exemplu, trebuie să dețină un centru de securitate și alte măsuri de prevenire, detectare și răspuns la incidente. Nerespectarea acestor standarde mai ridicate va conduce, cu siguranță, la măsuri mai stricte în cursul investigației unei autorități de supraveghere.

[21] De exemplu, informațiile persoanelor vizate se refereau la metode de plată, cum ar fi numere de card, conturi bancare, plăți online, state de plată, extrase de cont, studii economice sau orice alte informații care ar putea dezvălui informații economice referitoare la persoanele vizate.

64. Încălcarea se referă la date financiare care depășesc informațiile privind identitatea și identificatorul utilizatorului, ceea ce face ca aceasta să fie deosebit de gravă. Numărul persoanelor afectate este ridicat.

65. Faptul că o încălcare ar putea avea loc într-un mediu atât de sensibil indică existența unor lacune semnificative în materie de securitate a datelor în sistemul operatorului și poate fi un indicator al momentului când este „necesară" revizuirea și actualizarea măsurilor afectate, în conformitate cu articolul 24 alineatul (1), articolul 25 alineatul (1) și articolul 32 alineatul (1) din RGPD. Datele afectate de încălcare permit identificarea unică a persoanelor vizate și conțin alte informații cu privire la acestea (inclusiv sexul, data și locul nașterii); în plus, acestea pot fi utilizate de atacator pentru a ghici parolele clienților sau pentru a desfășura o campanie de „spear phishing" orientată către clienții băncii.

66. Din aceste motive, s-a considerat că încălcarea securității datelor este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile tuturor persoanelor vizate în cauză[22]. Prin urmare, producerea unor prejudicii materiale (de exemplu, pierderi financiare) și nemateriale (de exemplu, furt sau fraudă de identitate) este un rezultat posibil.

3.3.2 CAZUL nr. 07 – Atenuare și obligații

67. Măsurile operatorului menționate în descrierea cazului sunt adecvate. În urma încălcării, acesta a corectat, de asemenea, vulnerabilitatea site-ului și a luat alte măsuri pentru a preveni viitoare încălcări similare ale securității datelor, cum ar fi adăugarea unei autentificări duble pe site-ul în cauză și trecerea la o autentificare strictă a clienților.

68. Documentarea încălcării în conformitate cu articolul 33 alineatul (5) din RGPD și notificarea autorității de supraveghere cu privire la aceasta nu sunt opționale în acest scenariu. În plus, operatorul ar trebui să notifice toate cele 100 000 de persoane vizate (inclusiv persoanele vizate ale căror conturi nu au fost compromise) în conformitate cu articolul 34 din RGPD.

Acțiuni necesare în funcție de riscurile identificate		
Documentarea internă	Notificare către AS	Comunicare către persoanele vizate
✓	✓	✓

3.4 Măsuri organizatorice și tehnice de prevenire/atenuare a impactului atacurilor hackerilor

69. La fel ca în cazul atacurilor de tip ransomware, indiferent de rezultatul și consecințele atacului, reevaluarea securității informatice este obligatorie pentru operatori în cazuri similare.

70. Măsuri recomandate[23]:

- (Lista următoarelor măsuri nu este în niciun caz exclusivă sau cuprinzătoare. Mai degrabă, obiectivul este de a oferi idei de prevenire și soluții posibile. Fiecare activitate de prelucrare diferă de celelalte; prin urmare operatorul ar trebui să ia decizia cu privire la măsurile cele mai adecvate în situația specifică.)
- criptarea de ultimă generație și gestionarea cheilor, în special atunci când sunt prelucrate parole, date sensibile sau financiare; hashingul și saltingul criptografic pentru informațiile secrete (parole) se preferă

[22] Pentru orientări privind operațiunile de prelucrare „susceptibile să genereze un risc ridicat", a se vedea nota de subsol 10 de mai sus.

[23] Pentru dezvoltarea aplicațiilor web securizate, a se vedea, de asemenea: https://www.owasp.org/index.php/Main_Page.

întotdeauna în locul criptării parolelor. Se recomandă utilizarea unor metode de autentificare care să evite necesitatea de a prelucra parole pe partea serverului;

- actualizarea sistemului (software și firmware); asigurarea faptului că sunt luate toate măsurile de securitate informatică, asigurarea eficacității acestora și actualizarea periodică a acestora atunci când prelucrarea sau circumstanțele se schimbă sau evoluează. Pentru a putea demonstra conformitatea cu articolul 5 alineatul (1) litera (f) în conformitate cu articolul 5 alineatul (2) din RGPD, operatorul ar trebui să păstreze o evidență a tuturor actualizărilor efectuate, inclusiv a momentului în care acestea au fost aplicate;
- utilizarea unor metode de autentificare puternică, cum ar fi autentificarea dublă și serverele de autentificare, completate de o politică actualizată privind parolele;
- Standardele de dezvoltare securizată includ filtrarea datelor introduse de utilizatori (utilizând, pe cât posibil, liste albe), evitarea introducerii unor date nedorite de către utilizatori și măsuri de prevenire a atacurilor prin forță brută (cum ar fi limitarea numărului maxim de repetări). „Firewall-urile pentru aplicații web" pot contribui la utilizarea eficace a acestei tehnici;
- existența unei politici solide de gestionare a privilegiilor utilizatorilor și a controlului accesului;
- utilizarea unui firewall adecvat, actualizat, eficace și integrat, a detectării intruziunilor și a altor sisteme de apărare a perimetrului;
- efectuarea de audituri sistematice de securitate informatică și evaluări ale vulnerabilității (teste de penetrare cibernetică);
- efectuarea de revizuiri și testări periodice pentru a se asigura că pot fi utilizate copii de rezervă pentru a recupera orice date a căror integritate sau disponibilitate a fost afectată.
- Nu trebuie să existe niciun ID de sesiune în URL ca text normal.

4 SURSA INTERNĂ DE RISC UMAN

71. Având în vedere frecvența sa ridicată, trebuie subliniat rolul erorii umane în cazurile de încălcare a securității datelor cu caracter personal. Întrucât aceste tipuri de încălcări pot fi atât intenționate, cât și neintenționate, este foarte dificil pentru operatorii de date să identifice vulnerabilitățile și să adopte măsuri pentru a le evita. Conferința Internațională a Comisarilor pentru Protecția Datelor și a Vieții Private a recunoscut importanța abordării acestor factori umani și a adoptat, în octombrie 2019, o rezoluție pentru a aborda rolul erorii umane în cazurile de încălcare a securității datelor cu caracter personal[24]. Această rezoluție subliniază că ar trebui luate măsuri de protecție adecvate pentru a preveni erorile umane și furnizează o listă neexhaustivă a acestor garanții și abordări.

4.1 CAZUL nr. 08: Exfiltrarea datelor comerciale de către un angajat

[24] http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf.

În perioada de preaviz, angajatul unei societăți copiază date comerciale din baza de date a societății. Angajatul este autorizat să acceseze datele numai pentru a-și îndeplini sarcinile de serviciu. Câteva luni mai târziu, după ce a părăsit locul de muncă, acesta utilizează datele astfel obținute (date de contact de bază) pentru o nouă prelucrare a datelor pentru care este operator, pentru a-i contacta pe clienții societății și a-i încuraja să participe la noua sa afacere.

4.1.1 CAZUL nr. 08 – Măsuri prealabile și evaluarea riscului

72. În acest caz particular, nu au fost luate măsuri prealabile pentru a-l împiedica pe angajat să copieze datele de contact ale clientelei societății, întrucât acesta avea nevoie de – și avea – acces legitim la aceste informații pentru a-și îndeplini sarcinile profesionale. Întrucât pentru îndeplinirea majorității sarcinilor de muncă legate de relația cu clienții este necesar un oarecare nivel de acces al angajaților la datele cu caracter personal, aceste încălcări ale securității datelor pot fi cel mai dificil de prevenit. Limitările domeniului de aplicare al accesului pot limita activitatea pe care angajatul respectiv o poate efectua. Cu toate acestea, politicile de acces bine gândite și controlul constant pot contribui la prevenirea unor astfel de încălcări.

73. Ca de obicei, în timpul evaluării riscurilor, trebuie luate în considerare tipul încălcării și natura, sensibilitatea și volumul datelor cu caracter personal afectate. Aceste tipuri de încălcări sunt, de regulă, încălcări ale confidențialității, întrucât baza de date rămâne de obicei intactă, conținutul său fiind „doar" copiat pentru a fi utilizat ulterior. Cantitatea de date afectate este, de obicei, scăzută sau medie. În acest caz particular, nu au fost afectate categorii speciale de date cu caracter personal; angajatul avea nevoie doar de datele de contact ale clienților pentru a-i permite să ia legătura cu aceștia după părăsirea societății. Prin urmare, datele în cauză nu sunt sensibile.

74. Deși singurul obiectiv al fostului angajat care a copiat în mod rău-intenționat datele poate fi limitat la obținerea datelor de contact ale clientelei societății în scopuri comerciale proprii, operatorul nu este în măsură să considere că riscul pentru persoanele vizate afectate este scăzut, deoarece operatorul nu are niciun fel de siguranță cu privire la intențiile angajatului. Astfel, deși consecințele încălcării ar putea fi limitate la expunerea la marketing propriu nesolicitat al fostului angajat, nu este exclus un abuz suplimentar și mai grav al datelor furate, în funcție de scopul prelucrării efectuate de fostul angajat[25].

4.1.2 CAZUL nr. 08 – Atenuare și obligații

75. Atenuarea efectelor negative ale încălcării în cazul de mai sus este dificilă. Aceasta ar putea necesita acțiuni imediate în justiție pentru a-l împiedica pe fostul angajat să folosească abuziv datele și să le difuzeze în continuare. În etapa următoare, obiectivul ar trebui să fie evitarea unor situații viitoare similare. Operatorul ar putea încerca să solicite fostului angajat să înceteze utilizarea datelor, dar succesul acestei acțiuni este, în cel mai bun caz, îndoielnic. Ar putea fi util să se ia măsuri tehnice adecvate, cum ar fi unele care fac imposibilă copierea sau descărcarea datelor pe dispozitive detașabile.

76. Nu există o soluție universală pentru aceste tipuri de cazuri, dar o abordare sistematică poate contribui la prevenirea lor. De exemplu, societatea poate lua în considerare – atunci când este posibil – retragerea anumitor forme de acces pentru angajații care și-au semnalat intenția de a-și da demisia sau implementarea unor registre de acces, astfel încât accesul nedorit să poată fi înregistrat și marcat. Contractul semnat cu angajații ar trebui să includă clauze care interzic astfel de acțiuni.

[25] Pentru orientări privind operațiunile de prelucrare „susceptibile să genereze un risc ridicat", a se vedea nota de subsol 10 de mai sus.

77. În concluzie, întrucât încălcarea respectivă nu va conduce la un risc ridicat pentru drepturile și libertățile persoanelor fizice, este suficientă o notificare către AS. Cu toate acestea, informarea persoanelor vizate ar putea fi benefică și pentru operatorul de date, deoarece ar fi mai bine ca persoanele vizate să afle din partea societății despre scurgerile de date decât de la fostul angajat care încearcă să le contacteze. Păstrarea documentației referitoare la încălcarea securității datelor, în conformitate cu articolul 33 alineatul (5) este o obligație legală.

Acțiuni necesare în funcție de riscurile identificate		
Documentarea internă	Notificare către AS	Comunicare către persoanele vizate
✓	✓	X

4.2 CAZUL nr. 09: Transmiterea accidentală a datelor către o parte terță de încredere

Un agent de asigurări a observat că – date fiind setările defectuoase ale unui fișier Excel primit prin e-mail – a putut avea acces la informații referitoare la puțin peste douăzeci de clienți care nu se încadrează în domeniul său de aplicare. El este obligat să respecte secretul profesional și a fost singurul destinatar al e-mailului. Acordul dintre operatorul de date și agentul de asigurări îi obligă pe agent să semnaleze operatorului de date, fără întârzieri nejustificate, o încălcare a securității datelor cu caracter personal. Prin urmare, agentul a semnalat imediat eroarea operatorului, care a corectat fișierul și l-a trimis din nou, solicitând agentului să șteargă mesajul anterior. În conformitate cu acordul menționat mai sus, agentul trebuie să confirme ștergerea într-o declarație scrisă, ceea ce a făcut. Informațiile obținute nu includ categorii speciale de date cu caracter personal, ci doar date de contact și date despre asigurarea propriu-zisă (tipul de asigurare, suma). După analizarea datelor cu caracter personal afectate de încălcare, operatorul de date nu a identificat nicio caracteristică specială de partea persoanelor fizice sau a operatorului de date care ar putea afecta nivelul de impact al încălcării.

4.2.1 CAZUL nr. 09 – Măsuri prealabile și evaluarea riscului

78. În acest caz, încălcarea nu rezultă dintr-o acțiune intenționată a unui angajat, ci dintr-o eroare umană neintenționată, provocată din cauza neatenției. Aceste tipuri de încălcări pot fi evitate sau reduse ca frecvență prin (a) punerea în aplicare a unor programe de formare, educare și sensibilizare în cadrul cărora angajații să înțeleagă mai bine importanța protecției datelor cu caracter personal, (b) diminuarea schimburilor de fișiere prin e-mail și, în schimb, de exemplu, utilizarea unor sisteme dedicate de prelucrare a datelor clienților, (c) verificarea dublă a fișierelor înainte de trimitere, (d) separarea procesului de creare de cel de trimitere a fișierelor.

79. Această încălcare a securității datelor se referă numai la confidențialitatea datelor, iar integritatea și accesibilitatea acestora rămân intacte. Încălcarea securității datelor a vizat puțin peste douăzeci de clienți și, prin urmare, cantitatea de date afectată poate fi considerată scăzută. În plus, datele cu caracter personal afectate nu conțin date sensibile. Faptul că persoana împuternicită de operator l-a contactat imediat pe operatorul de date după ce a luat cunoștință de încălcarea securității datelor poate fi considerat un factor de atenuare a riscurilor. (Posibilitatea transmiterii datelor către alți agenți de asigurări ar trebui, de asemenea, evaluată și, dacă se confirmă, ar trebui luate măsuri adecvate.) Din cauza măsurilor adecvate luate după încălcarea securității datelor, probabil că aceasta nu va avea niciun impact asupra drepturilor și libertăților persoanelor vizate.

80. Combinația dintre numărul mic de persoane afectate, detectarea imediată a încălcării și măsurile luate pentru a reduce la minimum efectele acesteia face ca acest caz particular să nu prezinte niciun risc.

4.2.2 CAZUL nr. 09 – Atenuare și obligații

81. În plus, au existat și alte circumstanțe de atenuare a riscurilor: agentul este obligat să respecte secretul profesional; el însuși a raportat problema operatorului și a șters fișierul la cerere. Sensibilizarea și, eventual, includerea unor etape suplimentare în verificarea documentelor care implică date cu caracter personal vor contribui probabil la evitarea unor cazuri similare în viitor.

82. Pe lângă păstrarea documentației referitoare la încălcare, în conformitate cu articolul 33 alineatul (5), nu este necesară nicio altă acțiune.

Acțiuni necesare în funcție de riscurile identificate		
Documentarea internă	Notificare către AS	Comunicare către persoanele vizate
✓	X	X

4.3 Măsuri organizatorice și tehnice de prevenire/atenuare a impactului surselor interne de risc uman

83. O combinație a măsurilor menționate mai jos – aplicate în funcție de caracteristicile unice ale cazului – ar trebui să contribuie la reducerea șanselor de reapariție a unei încălcări similare.

84. Măsuri recomandate:

- (Lista următoarelor măsuri nu este în niciun caz exclusivă sau cuprinzătoare. Mai degrabă, obiectivul este de a oferi idei de prevenire și soluții posibile. Fiecare activitate de prelucrare diferă de celelalte; prin urmare operatorul ar trebui să ia decizia cu privire la măsurile cele mai adecvate în situația specifică.)
- punerea în aplicare periodică a unor programe de formare, educare și sensibilizare a angajaților cu privire la obligațiile lor în materie de confidențialitate și securitate și la detectarea și raportarea amenințărilor la adresa securității datelor cu caracter personal[26]; elaborarea unui program de sensibilizare pentru a reaminti angajaților erorile cele mai obișnuite care conduc la încălcarea securității datelor cu caracter personal și modul de evitare a acestora;
- stabilirea unor practici, proceduri și sisteme solide și eficace în materie de protecție a datelor și a vieții private[27];
- evaluarea practicilor, a procedurilor și a sistemelor de protecție a vieții private pentru a asigura eficacitatea continuă[28];
- elaborarea unor politici adecvate de control al accesului și obligarea utilizatorilor să respecte normele;
- implementarea unor tehnici pentru a forța autentificarea utilizatorilor atunci când accesează date cu caracter personal sensibile;
- dezactivarea contului de serviciu al utilizatorului de îndată ce persoana respectivă părăsește societatea;
- verificarea fluxului de date neobișnuit între serverul de fișiere și stațiile de lucru ale angajaților;
- configurarea securității interfeței I/O în BIOS sau prin utilizarea unui software care controlează utilizarea interfețelor calculatorului (blocare sau deblocare, de exemplu USB/CD/DVD etc.);
- revizuirea politicii de acces pentru angajați (de exemplu, înregistrarea accesului la date sensibile și solicitarea ca utilizatorul să introducă un motiv profesional, astfel încât acesta să fie disponibil pentru audituri);
- dezactivarea serviciilor de cloud deschis;
- interzicerea și împiedicarea accesului la servicii de corespondență deschisă cunoscute;

---

[26] Secțiunea 2) subsecțiunea (i) din Rezoluția privind abordarea rolului erorii umane în cazurile de încălcare a securității datelor cu caracter personal.

[27] Secțiunea 2) subsecțiunea (ii) din Rezoluția privind abordarea rolului erorii umane în cazurile de încălcare a securității datelor cu caracter personal.

[28] Secțiunea 2) subsecțiunea (iii) din Rezoluția privind abordarea rolului erorii umane în cazurile de încălcare a securității datelor cu caracter personal.

- dezactivarea funcției de captură de ecran în OS;
- punerea în aplicare a unei politici a „biroului curat”;
- blocarea automată a tuturor calculatoarelor după o anumită perioadă de inactivitate;
- utilizarea unor mecanisme [de exemplu, token-uri (fără fir) pentru conectarea la/deschiderea conturilor blocate] pentru comutarea rapidă a utilizatorilor în medii partajate;
- utilizarea unor sisteme dedicate de gestionare a datelor cu caracter personal care aplică mecanisme adecvate de control al accesului și care previn erorile umane, cum ar fi trimiterea de comunicări către un destinatar greșit; utilizarea foilor de calcul și a altor documente administrative nu este un mijloc adecvat de gestionare a datelor clienților.

5 DISPOZITIVE ȘI DOCUMENTE PE SUPORT DE HÂRTIE PIERDUTE SAU FURATE

85. Un tip frecvent de astfel de caz este pierderea sau furtul de dispozitive portabile. În aceste cazuri, operatorul trebuie să ia în considerare circumstanțele operațiunii de prelucrare, cum ar fi tipul de date stocate pe dispozitiv, precum și activele de sprijin și măsurile luate înainte de încălcare pentru a asigura un nivel adecvat de securitate. Toate aceste elemente afectează impactul potențial al încălcării securității datelor. Evaluarea riscurilor ar putea fi dificilă, deoarece dispozitivul nu mai este disponibil.

86. Aceste tipuri de încălcări pot fi întotdeauna clasificate drept încălcări ale confidențialității. Cu toate acestea, dacă nu există o copie de rezervă pentru baza de date furată, atunci tipul de încălcare poate fi, de asemenea, o încălcare a disponibilității și a integrității.

87. Scenariile de mai jos demonstrează modul în care circumstanțele menționate anterior influențează probabilitatea și gravitatea încălcării securității datelor.

5.1 CAZUL nr. 10: Materiale furate care stochează date cu caracter personal criptate

- În timpul intrării prin efracție într-un centru de zi pentru copii, au fost furate două tablete. Pe tablete era instalată o aplicație care conținea date cu caracter personal despre copiii care frecventau centrul de zi. Au fost afectate numele, data nașterii, date cu caracter personal privind educația copiilor. Atât tabletele criptate, care erau închise la momentul intrării prin efracție, cât și aplicația erau protejate printr-o parolă puternică. Datele de rezervă au fost puse efectiv și imediat la dispoziția operatorului. După ce a luat cunoștință de intrarea prin efracție, centrul a emis de la distanță o comandă de ștergere a datelor din tablete la scurt timp după descoperirea situației.

5.1.1 CAZUL nr. 10 – Măsuri prealabile și evaluarea riscului

88. În acest caz particular, operatorul de date a luat măsuri adecvate pentru a preveni și a atenua impactul unei potențiale încălcări a securității datelor prin criptarea dispozitivului, introducerea unei protecții adecvate prin parolă și securizarea unei copii de rezervă a datelor stocate pe tablete. (O listă de măsuri recomandabile este disponibilă în secțiunea 5.7).

89. După ce ia cunoștință de o încălcare, operatorul de date ar trebui să evalueze sursa riscului, sistemele care sprijină prelucrarea datelor, tipul de date cu caracter personal implicate și impactul potențial al încălcării securității datelor asupra persoanelor vizate. Încălcarea securității datelor descrisă mai sus ar fi vizat confidențialitatea, disponibilitatea și integritatea datelor în cauză; cu toate acestea, datorită procedurilor

adecvate ale operatorului de date înainte și după încălcarea securității datelor, niciuna dintre acestea nu a avut loc.

5.1.2 CAZUL nr. 10 – Atenuare și obligații

90. Confidențialitatea datelor cu caracter personal de pe dispozitive nu a fost compromisă datorită protecției puternice prin parolă atât a tabletelor, cât a aplicațiilor. Tabletele au fost configurate astfel încât setarea unei parole înseamnă, de asemenea, criptarea datelor de pe dispozitiv. Acest lucru a fost consolidat și de acțiunea operatorului în încercarea de a șterge de la distanță toate datele de pe dispozitivele furate.

91. Datorită măsurilor luate, confidențialitatea datelor a rămas, de asemenea, intactă. În plus, copia de rezervă a asigurat disponibilitatea continuă a datelor cu caracter personal, prin urmare nu s-ar fi putut produce niciun impact negativ potențial.

92. Datorită acestor fapte, era puțin probabil ca încălcarea securității datelor descrisă mai sus să genereze un risc pentru drepturile și libertățile persoanelor vizate și, prin urmare, nu a fost necesară notificarea autorității de supraveghere sau a persoanelor vizate în cauză. Totuși, această încălcare a securității datelor trebuie, de asemenea, să fie documentată în conformitate cu articolul 33 alineatul (5).

Acțiuni necesare în funcție de riscurile identificate		
Documentarea internă	Notificare către AS	Comunicare către persoanele vizate
✓	X	X

5.2 CAZUL nr. 11: Materiale furate care stochează date cu caracter personal necriptate

Computerul portabil al unui angajat al unei societăți furnizoare de servicii a fost furat. Computerul portabil furat conținea numele, prenumele, sexul, adresele și data nașterii a peste 100 000 de clienți. Din cauza indisponibilității dispozitivului furat, nu a fost posibil să se identifice dacă au fost afectate și alte categorii de date cu caracter personal. Accesul la hard diskul computerului portabil nu era protejat prin parolă. Datele cu caracter personal au putut fi recuperate din copiile de rezervă zilnice disponibile.

5.2.1 CAZUL nr. 11 – Măsuri prealabile și evaluarea riscului

93. Operatorul de date nu a luat nicio măsură de siguranță prealabilă și, prin urmare, datele cu caracter personal stocate pe computerul portabil furat au fost ușor accesibile pentru autorul furtului sau pentru orice altă persoană care a intrat ulterior în posesia dispozitivului.

94. Această încălcare a securității datelor se referă la confidențialitatea datelor stocate pe dispozitivul furat.

95. Computerul portabil care conținea datele cu caracter personal era vulnerabil în acest caz, deoarece nu era protejat prin parolă sau criptare. Lipsa unor măsuri de securitate de bază sporește nivelul de risc pentru persoanele vizate afectate. În plus, identificarea persoanelor vizate în cauză este, de asemenea, problematică, ceea ce sporește, de asemenea, gravitatea încălcării. Numărul considerabil de persoane vizate crește riscul; cu toate acestea, nicio categorie specială de date cu caracter personal nu a fost vizată de încălcarea securității datelor.

96. În timpul evaluării riscurilor[29], operatorul ar trebui să ia în considerare posibilele consecințe și efecte negative ale încălcării confidențialității. Ca urmare a încălcării, persoanele vizate în cauză pot suferi fraude de identitate bazate pe datele disponibile pe dispozitivul furat, astfel încât riscul este considerat ridicat.

5.2.2 CAZUL nr. 11 – Atenuare și obligații

97. Criptarea dispozitivului și utilizarea unei parole puternice pentru protecția bazei de date stocate ar fi putut preveni ca încălcarea securității datelor să genereze un risc pentru drepturile și libertățile persoanelor vizate.

98. Având în vedere aceste circumstanțe, este necesară notificarea AS, la fel cum este și notificarea persoanelor vizate în cauză.

Acțiuni necesare în funcție de riscurile identificate		
Documentarea internă	Notificare către AS	Comunicare către persoanele vizate
✓	✓	✓

5.3 CAZUL nr. 12: Dosare pe suport de hârtie furate conținând date sensibile

Un jurnal pe suport de hârtie a fost furat de la un centru de dezintoxicare pentru dependența de droguri. Jurnalul conținea date de identitate de bază și date medicale ale pacienților admiși în centrul de dezintoxicare. Datele erau stocate doar pe suport de hârtie și nu era disponibilă nicio copie de rezervă pentru medicii care tratează pacienții. Jurnalul nu era depozitat într-un sertar încuiat sau într-o încăpere încuiată, operatorul de date nu dispunea nici de un regim de control al accesului, nici de vreo altă măsură de protecție pentru documentația pe suport de hârtie.

5.3.1 CAZUL nr. 12 – Măsuri prealabile și evaluarea riscului

99. Operatorul de date nu a luat în prealabil nicio măsură de siguranță și, prin urmare, datele cu caracter personal din acest jurnal au fost ușor accesibile persoanei care l-a găsit. În plus, natura datelor cu caracter personal din jurnal face ca lipsa datelor de rezervă să fie un factor de risc foarte grav.

100. Acest caz servește drept exemplu pentru o încălcare cu grad ridicat de risc a securității datelor. Din cauza nerespectării măsurilor de precauție adecvate în materie de siguranță, datele sensibile privind starea de sănătate în temeiul articolului 9 alineatul (1) din RGPD au fost pierdute. Întrucât, în acest caz, a fost vizată o categorie specială de date cu caracter personal, riscurile potențiale pentru persoanele vizate în cauză au fost sporite, fapt pe care operatorul care evaluează riscul ar trebui, de asemenea, să îl ia în considerare[30].

101. Această încălcare se referă la confidențialitatea, disponibilitatea și integritatea datelor cu caracter personal în cauză. Ca urmare a încălcării, secretul medical este încălcat, iar terții neautorizați pot avea acces la informațiile medicale private ale pacienților, ceea ce poate avea un impact grav asupra vieții personale a pacientului. Încălcarea disponibilității poate, de asemenea, să perturbe continuitatea tratamentului pacienților. Întrucât modificarea/ștergerea unor părți din conținutul jurnalului nu poate fi exclusă, integritatea datelor cu caracter personal este, de asemenea, compromisă.

[29] Pentru orientări privind operațiunile de prelucrare „susceptibile să genereze un risc ridicat”, a se vedea nota de subsol 10 de mai sus.

[30] Pentru orientări privind operațiunile de prelucrare „susceptibile să genereze un risc ridicat”, a se vedea nota de subsol 10 de mai sus.

5.3.2 CAZUL nr. 12 – Atenuare și obligații

102. În timpul evaluării măsurilor de protecție, ar trebui luat în considerare, de asemenea, tipul activului de sprijin. Întrucât jurnalul pacienților este un document fizic, protecția sa ar fi trebuit să fie organizată diferit de cea a unui dispozitiv electronic. Pseudonimizarea numelor pacienților, depozitarea jurnalului într-un spațiu protejat și într-un sertar încuiat sau într-o încăpere încuiată, precum și controlul adecvat al accesului cu autentificare în momentul accesării acestuia ar fi putut împiedica încălcarea securității datelor.

103. Încălcarea securității datelor descrisă mai sus poate avea un impact grav asupra persoanelor vizate în cauză; prin urmare, notificarea AS și informarea persoanelor vizate cu privire la încălcare sunt obligatorii.

Acțiuni necesare în funcție de riscurile identificate		
Documentarea internă	Notificare către AS	omunicare către persoanele vizate
✓	✓	✓

5.4 Măsuri organizatorice și tehnice de prevenire/atenuare a impactului pierderii sau furtului de dispozitive

104. O combinație a măsurilor menționate mai jos – aplicate în funcție de caracteristicile unice ale cazului – ar trebui să contribuie la reducerea șanselor de reapariție a unei încălcări similare.

105. Măsuri recomandate:

- (Lista următoarelor măsuri nu este în niciun caz exclusivă sau cuprinzătoare. Mai degrabă, obiectivul este de a oferi idei de prevenire și soluții posibile. Fiecare activitate de prelucrare diferă de celelalte; prin urmare operatorul ar trebui să ia decizia cu privire la măsurile cele mai adecvate în situația specifică.)
- criptarea dispozitivului (folosind soluții precum Bitlocker, Veracrypt sau DM-Crypt);
- utilizarea unui cod de acces/unei parole pe toate dispozitivele; criptarea tuturor dispozitivelor electronice mobile într-un mod care necesită introducerea unei parole complexe pentru decriptare;
- utilizarea autentificării multifactor;
- activarea funcționalităților dispozitivelor extrem de mobile care permit localizarea acestora în caz de pierdere sau amplasare în locul greșit;
- utilizarea software-ului/aplicației MDM (*Mobile Devices Management* – „gestionarea dispozitivelor mobile") și a funcției de localizare; utilizarea de filtre antireflexie; închiderea oricărui dispozitiv nesupravegheat;
- salvarea datelor cu caracter personal pe un server back-end central, și nu pe un dispozitiv mobil, dacă acest lucru este posibil și adecvat pentru prelucrarea datelor în cauză;
- realizarea unei copii de rezervă automate din fișierele de lucru, cu condiția ca datele cu caracter personal să fie stocate acolo, dacă stația de lucru este conectată la rețeaua LAN corporativă;
- utilizarea unui VPN securizat (de exemplu, care necesită o cheie separată de autentificare bazată pe doi factori pentru stabilirea unei conexiuni securizate) pentru a conecta dispozitivele mobile la serverele back-end;
- punerea la dispoziția angajaților a unor dispozitive fizice de blocare pentru a le permite să securizeze fizic dispozitivele mobile pe care le utilizează atunci când acestea rămân nesupravegheate;
- reglementarea adecvată a utilizării dispozitivelor în afara întreprinderii;
- reglementarea adecvată a utilizării dispozitivelor în interiorul întreprinderii;

- utilizarea software-ului/aplicației MDM (*Mobile Devices Management* – „gestionarea dispozitivelor mobile") și activarea funcției de ștergere la distanță;
- utilizarea gestionării centralizate a dispozitivelor, cu drepturi minime pentru utilizatorii finali de a instala software;
- instalarea de dispozitive de control al accesului fizic;
- evitarea stocării informațiilor sensibile pe dispozitive mobile sau pe unități de hard disk. În cazul în care este necesar să se acceseze sistemul intern al întreprinderii, ar trebui utilizate canale sigure, astfel cum s-a menționat anterior.

6 EXPEDIERI ERONATE

106. Sursa de risc este o eroare umană internă și în acest caz, dar încălcarea nu a fost generată de o acțiune rău-intenționată. Este rezultatul neatenției. Operatorul poate întreprinde puține acțiuni după ce a avut loc, astfel încât prevenirea este chiar mai importantă în aceste cazuri decât în alte tipuri de încălcări.

6.1 CAZUL nr. 13: Erori poștale

O societate din sectorul vânzării cu amănuntul a ambalat două comenzi de articole de încălțăminte. Din cauza unei erori umane, două facturi au fost amestecate, rezultatul fiind că atât produsele, cât și facturile aferente au fost trimise persoanei greșite. Aceasta înseamnă că fiecare dintre cei doi clienți a primit comanda celuilalt client, inclusiv facturile care conțineau date cu caracter personal. După ce a luat cunoștință de încălcare, operatorul de date a rechemat comenzile și le-a trimis destinatarilor adecvați.

6.1.1 CAZUL nr. 13 – Măsuri prealabile și evaluarea riscului

107. Facturile conțineau datele cu caracter personal necesare pentru realizarea livrării cu succes (nume, adresă, plus articolul achiziționat și prețul acestuia). Este important să se identifice în primul rând cum s-a putut produce eroarea umană și, în orice caz, cum ar fi putut fi prevenită. În cazul respectiv, riscul a fost scăzut, deoarece nu au fost implicate categorii speciale de date cu caracter personal sau alte date a căror utilizare abuzivă ar putea conduce la efecte negative semnificative, încălcarea nu este rezultatul unei erori sistemice din partea operatorului și sunt vizate doar două persoane. Nu a putut fi identificat niciun efect negativ asupra persoanelor.

6.1.2 CAZUL nr. 13 – Atenuare și obligații

108. Operatorul ar trebui să asigure returnarea gratuită a articolelor și a facturilor însoțitoare și, de asemenea, ar trebui să solicite destinatarilor neintenționați să distrugă/să șteargă toate eventualele copii ale facturilor care conțin datele cu caracter personal ale celeilalte persoane.

109. Chiar dacă încălcarea în sine nu prezintă un risc ridicat pentru drepturile și libertățile persoanelor afectate și, prin urmare, nu se impune comunicarea către persoanele vizate, astfel cum se prevede la articolul 34 din RGPD, comunicarea încălcării către acestea nu poate fi evitată, întrucât este necesară cooperarea acestora pentru a atenua riscul.

Acțiuni necesare în funcție de riscurile identificate		
Documentarea internă	Notificare către AS	Comunicare către persoanele vizate
✓	X	X

6.2 CAZUL nr. 14: Date cu caracter personal foarte confidențiale trimise prin poștă din greșeală

Departamentul pentru ocuparea forței de muncă al unui birou al administrației publice a trimis un e-mail – cu privire la viitoarele cursuri de formare – persoanelor înregistrate în sistemul său ca persoane aflate în căutarea unui loc de muncă. Din greșeală, la acest e-mail a fost anexat un document care conținea toate datele cu caracter personal ale acestor persoane aflate în căutarea unui loc de muncă (nume, adresă de e-mail, adresă poștală, număr de asigurare socială). Numărul persoanelor afectate este de peste 60 000. Ulterior, biroul i-a contactat pe toți destinatarii și le-a solicitat să șteargă mesajul anterior și să nu utilizeze informațiile conținute în acesta.

6.2.1 CAZUL nr. 14 – Măsuri prealabile și evaluarea riscului

110. Ar fi trebuit puse în aplicare norme mai stricte privind transmiterea unor astfel de mesaje. Trebuie avută în vedere introducerea unor mecanisme de control suplimentare.

111. Numărul persoanelor afectate este considerabil, iar faptul că a fost implicat numărul lor de asigurare socială, împreună cu alte date cu caracter personal mai elementare, crește și mai mult riscul, care poate fi clasificat drept ridicat[31]. Eventuala distribuire a datelor de către oricare dintre destinatari nu poate fi limitată de operator.

6.2.2 CAZUL nr. 14 – Atenuare și obligații

112. După cum s-a menționat anterior, mijloacele de atenuare eficace a riscurilor unei încălcări similare sunt limitate. Deși a solicitat ștergerea mesajului, operatorul nu îi poate obliga pe destinatari să facă acest lucru și, în consecință, nici nu poate fi sigur că aceștia respectă cererea.

113. Executarea tuturor celor trei acțiuni indicate mai jos ar trebui să fie evidentă într-un astfel de caz.

Acțiuni necesare în funcție de riscurile identificate		
Documentarea internă	Notificare către AS	Comunicare către persoanele vizate
✓	✓	✓

6.3 CAZUL nr. 15: Date cu caracter personal trimise prin poștă din greșeală

O listă a participanților la un curs în limbă engleză juridică care se desfășoară într-un hotel timp de 5 zile este trimisă din greșeală unui număr de 15 foști participanți la curs în loc să fie trimisă hotelului. Lista conține numele, adresele de e-mail și preferințele alimentare ale celor 15 participanți. Numai doi participanți și-au completat preferințele alimentare, declarând că sunt intoleranți la lactoză. Niciunul dintre participanți nu are o identitate protejată. Operatorul descoperă eroarea imediat după trimiterea listei și îi informează pe destinatari cu privire la eroare și le solicită să șteargă lista.

[31] Pentru orientări privind operațiunile de prelucrare „susceptibile să genereze un risc ridicat”, a se vedea nota de subsol 10 de mai sus.

6.3.1 CAZUL nr. 15 – Măsuri prealabile și evaluarea riscului

114. Ar fi trebuit puse în aplicare norme stricte pentru trimiterea mesajelor care conțin date cu caracter personal. Trebuie avută în vedere introducerea unor mecanisme de control suplimentare.

115. Riscurile care decurg din natura, sensibilitatea, volumul și contextul datelor cu caracter personal sunt scăzute. Datele cu caracter personal includ date sensibile privind preferințele alimentare pentru doi dintre participanți. Chiar dacă informațiile că cineva are intoleranță la lactoză sunt date privind sănătatea, riscul ca aceste date să fie utilizate în mod negativ ar trebui considerat relativ scăzut. Deși în cazul datelor cu caracter personal privind sănătatea se presupune, de obicei, că încălcarea este susceptibilă să genereze un risc ridicat pentru persoana vizată[32], în același timp, în acest caz particular, nu se poate identifica niciun risc ca încălcarea să conducă la prejudicii fizice, materiale sau morale pentru persoana vizată din cauza divulgării neautorizate a informațiilor privind intoleranța la lactoză. Spre deosebire de alte preferințe alimentare, intoleranța la lactoză nu poate fi legată, în mod normal, de nicio convingere religioasă sau filozofică. Cantitatea de date afectate de încălcare și numărul persoanelor vizate afectate sunt, de asemenea, foarte scăzute.

6.3.2 CAZUL nr. 15 – Atenuare și obligații

116. Pe scurt, se poate afirma că încălcarea nu a avut niciun efect semnificativ asupra persoanelor vizate. Faptul că operatorul i-a contactat imediat pe destinatari după ce a luat cunoștință de eroare poate fi considerat un factor atenuant.

117. În cazul în care se trimite un e-mail unui destinatar incorect/neautorizat, se recomandă ca operatorul de date să trimită ulterior un e-mail destinatarilor neintenționați, enumerând adresele de e-mail ale acestora în câmpul „bcc”, în care să își ceară scuze, solicitând ștergerea e-mailului ofensator și avertizându-i pe destinatari că nu au dreptul să utilizeze în continuare adresele de e-mail identificate.

118. Datorită acestor fapte, a fost puțin probabil ca încălcarea securității acestor date să genereze un risc pentru drepturile și libertățile persoanelor vizate și, prin urmare, nu a fost necesară notificarea autorității de supraveghere sau a persoanelor vizate în cauză. Totuși, această încălcare a securității datelor trebuie, de asemenea, să fie documentată în conformitate cu articolul 33 alineatul (5).

Acțiuni necesare în funcție de riscurile identificate		
Documentarea internă	Notificare către AS	Comunicare către persoanele vizate
✓	X	X

6.4 CAZUL nr. 16: Erori poștale

[32] A se vedea Orientările WP 250, p. 23.

Un grup din domeniul asigurărilor oferă asigurări auto. În acest scop, trimite periodic prin poștă polițe cu contribuțiile ajustate. Pe lângă numele și adresa deținătorului poliței de asigurare, scrisoarea conține numărul de înmatriculare al vehiculului fără cifre cenzurate, ratele de asigurare pentru anul de asigurare curent și pentru următorul an de asigurare, kilometrajul anual aproximativ și data nașterii deținătorului poliței de asigurare. Datele cu caracter personal privind sănătatea în conformitate cu articolul 9 din RGPD, datele privind plățile (detalii bancare), datele economice și financiare nu sunt incluse.

Scrisorile sunt introduse în plicuri cu ajutorul unor mașini automate. Din cauza unei erori mecanice, două scrisori adresate unor deținători diferiți de polițe de asigurare sunt introduse într-un singur plic și trimise unui deținător de poliță prin poștă. Deținătorul poliței de asigurare deschide plicul acasă și analizează scrisoarea corectă, precum și pe cea trimisă din greșeală, care aparținea altui deținător de poliță de asigurare.

6.4.1 CAZUL nr. 16 – Măsuri prealabile și evaluarea riscului

119. Scrisoarea trimisă din greșeală conține numele, adresa, data nașterii, numărul de înmatriculare al vehiculului necenzurat și clasificarea ratei de asigurare pentru anul curent și anul următor. Efectele asupra persoanei afectate trebuie considerate ca fiind medii, întrucât informațiile care nu sunt disponibile publicului, cum ar fi data nașterii sau numerele de înmatriculare ale vehiculelor necenzurate, precum și detaliile privind majorarea tarifelor de asigurare sunt comunicate unui beneficiar neautorizat. Probabilitatea utilizării abuzive a acestor date este evaluată ca fiind între scăzută și medie. Cu toate acestea, deși mulți destinatari vor arunca probabil la gunoi scrisoarea primită în mod eronat, în anumite cazuri individuale nu se poate exclude complet faptul că scrisoarea va fi publicată pe rețelele de socializare sau că deținătorul poliței de asigurare va fi contactat.

6.4.2 CAZUL nr. 16 – Atenuare și obligații

120. Operatorul ar trebui să solicite restituirea documentului original pe propria sa cheltuială. Destinatarul neintenționat ar trebui, de asemenea, să fie informat că nu poate utiliza în mod abuziv informațiile citite.

121. Probabil că nu va fi niciodată posibil să se prevină complet o eroare de expediere poștală în cadrul unei corespondențe în masă cu ajutorul unor mașini complet automatizate. Cu toate acestea, în cazul unei frecvențe crescute, este necesar să se verifice dacă mașinile de introducere a hârtiei în plicuri sunt instalate și întreținute suficient de corect sau dacă o altă problemă sistemică conduce la o astfel de încălcare.

Acțiuni necesare în funcție de riscurile identificate		
Documentarea internă	Notificare către AS	Comunicare către persoanele vizate
✓	✓	X

6.5 Măsuri organizatorice și tehnice de prevenire/atenuare a impactului expedierilor eronate

122. O combinație a măsurilor menționate mai jos – aplicate în funcție de caracteristicile unice ale cazului – ar trebui să contribuie la reducerea șanselor de reapariție a unei încălcări similare.

123. Măsuri recomandate:

(*Lista următoarelor măsuri nu este în niciun caz exclusivă sau cuprinzătoare. Mai degrabă, obiectivul este de a oferi idei de prevenire și soluții posibile. Fiecare activitate de prelucrare diferă de celelalte; prin urmare operatorul ar trebui să ia decizia cu privire la măsurile cele mai adecvate în situația specifică*.)

- stabilirea unor standarde exacte – fără a lăsa loc de interpretare – pentru trimiterea de scrisori/e-mailuri;

- formare adecvată a personalului cu privire la modul de expediere a scrisorilor/e-mailurilor.
- Atunci când se trimit e-mailuri mai multor destinatari, aceștia sunt enumerați în mod implicit în câmpul „bcc”.
- Este necesară o confirmare suplimentară atunci când se trimit e-mailuri mai multor destinatari și aceștia nu sunt enumerați în câmpul „bcc”.
- Aplicarea „principiului celor patru ochi”;
- înscrierea automată a adreselor, și nu manuală, cu date extrase dintr-o bază de date disponibilă și actualizată; sistemul automat de înscriere a adreselor ar trebui revizuit periodic pentru a verifica erorile ascunse și setările incorecte;
- aplicarea unei perioade de întârziere a transmiterii mesajului (de exemplu, mesajul poate fi șters/editat într-un anumit interval de timp după apăsarea butonului de expediere);
- dezactivarea completării automate a adreselor de e-mail la scriere;
- sesiuni de sensibilizare cu privire la cele mai frecvente greșeli care conduc la o încălcare a securității datelor cu caracter personal;
- sesiuni de formare și manuale privind modul de gestionare a incidentelor care conduc la o încălcare a securității datelor cu caracter personal și persoana care trebuie să fie informată (implicarea responsabilului cu protecția datelor).

-
-

7 ALTE CAZURI – INGINERIE SOCIALĂ

7.1 CAZUL nr. 17: Furtul de identitate

Centrul de contact al unei societăți de telecomunicații primește un apel telefonic de la o persoană care se prezintă drept client. Presupusul client solicită societății să schimbe adresa de e-mail la care ar trebui trimise informațiile de facturare pe viitor. Lucrătorul centrului de contact validează identitatea clientului solicitând anumite date cu caracter personal, astfel cum este definit în procedurile societății. Apelantul indică în mod corect numărul fiscal și adresa poștală a clientului (deoarece a avut acces la aceste elemente). După validare, operatorul efectuează modificarea solicitată și, din acel moment, informațiile de facturare se vor trimite la noua adresă de e-mail. Procedura nu prevede nicio notificare la fosta adresă de e-mail de contact. În luna următoare, clientul legitim contactează societatea, întrebând de ce nu primește factura la adresa sa de e-mail și neagă faptul că a solicitat prin apel telefonic schimbarea adresei de e-mail. Ulterior, societatea își dă seama că informațiile au fost trimise unui utilizator nelegitim și inversează modificarea.

-

7.1.1 CAZUL nr. 17 – Evaluarea riscului, atenuare și obligații

124. Acest caz servește drept exemplu privind importanța măsurilor prealabile. Din punctul de vedere al riscului, încălcarea prezintă un nivel ridicat de risc33, întrucât datele de facturare pot oferi informații cu privire la viața privată a persoanei vizate (de exemplu, obiceiuri, contacte) și ar putea genera prejudicii materiale (de exemplu, urmărirea în scopul hărțuirii, riscul la adresa integrității fizice). Datele cu caracter personal obținute în timpul acestui atac pot fi, de asemenea, utilizate pentru a facilita preluarea contului în cadrul acestei organizații sau pentru a exploata alte măsuri de autentificare în alte organizații. Având în vedere aceste riscuri, măsura de autentificare „adecvată” ar trebui să fie una de nivel ridicat, în funcție de datele cu caracter personal care pot fi prelucrate ca urmare a autentificării.

125. Prin urmare, operatorul trebuie să transmită atât o notificare către AS, cât și o comunicare către persoana vizată.

126. Procesul de validare prealabilă a clientului trebuie în mod clar să fie îmbunătățit având în vedere acest caz. Metodele utilizate pentru autentificare nu au fost suficiente. Partea rău-intenționată a fost în măsură să pretindă că este utilizatorul vizat prin utilizarea informațiilor disponibile public și a informațiilor la care avea acces în alt mod.

127. Nu se recomandă utilizarea acestui tip de autentificare statică bazată pe cunoștințe (în cazul în care răspunsul nu se modifică și în cazul în care informațiile nu sunt „secrete”, cum ar fi cazul unei parole).

128. În schimb, organizația ar trebui să utilizeze o formă de autentificare care să aibă ca rezultat un grad ridicat de încredere că utilizatorul autentificat este persoana vizată, și nu altă persoană. Introducerea unei metode de autentificare multifactoriale în afara benzii ar rezolva problema, de exemplu, pentru a verifica cererea de modificare, trimițând o cerere de confirmare către persoana de contact anterioară; sau prin adăugarea de întrebări suplimentare și solicitarea de informații vizibile doar pe facturile anterioare. Este responsabilitatea operatorului să decidă ce măsuri să introducă, deoarece cunoaște cel mai bine detaliile și cerințele specifice operațiunilor sale interne.

Acțiuni necesare în funcție de riscurile identificate		
Documentarea internă	Notificare către AS	Comunicare către persoanele vizate
✓	✓	✓

7.2 CAZUL nr. 18: Exfiltrarea e-mailurilor

[33] Pentru orientări privind operațiunile de prelucrare „susceptibile să genereze un risc ridicat”, a se vedea nota de subsol 10 de mai sus.

Un lanț de hipermarketuri a detectat, la 3 luni de la configurarea sa, că unele conturi de e-mail au fost modificate și au fost create reguli astfel încât fiecare e-mail care conține anumite expresii (de exemplu, „factură", „plată", „transfer bancar", „autentificare card de credit", „date cont bancar") să fie transferat într-un folder neutilizat și, de asemenea, să fie transmis la o adresă de e-mail externă. De asemenea, la acel moment, se efectuase deja un atac de inginerie socială, și anume atacatorul, pretinzând că este un furnizor, solicitase înlocuirea datelor contului bancar al furnizorului respectiv cu cele ale propriului său cont bancar. În cele din urmă, la acel moment, fuseseră trimise mai multe facturi false care includeau datele noului cont bancar. Sistemul de monitorizare al platformei de e-mail a transmis în cele din urmă o alertă cu privire la foldere. Societatea nu a fost în măsură să detecteze în primul rând cum a putut avea acces atacatorul la conturile de e-mail, dar a presupus că un e-mail infectat a fost de vină pentru acordarea accesului la grupul de utilizatori responsabili de plăți.

Ca urmare a transmiterii e-mailurilor pe bază de cuvinte-cheie, atacatorul a primit informații cu privire la 99 de angajați: numele și salariul pentru o anumită lună cu privire la 89 de persoane vizate; numele, starea civilă, numărul de copii, salariul, orele de lucru și restul informațiilor de pe statul de plată pentru 10 angajați ale căror contracte au încetat. Operatorul i-a notificat numai pe cei 10 angajați care făceau parte din acest din urmă grup.

7.2.1 CAZUL nr. 18 – Evaluarea riscului, atenuare și obligații

129. Chiar dacă atacatorul nu a urmărit probabil colectarea de date cu caracter personal, întrucât încălcarea ar putea duce atât la prejudicii materiale (de exemplu, pierderi financiare), cât și la prejudicii morale (de exemplu, furt sau fraudă de identitate) sau datele ar putea fi utilizate pentru a facilita alte atacuri (de exemplu, phishing), este probabil ca încălcarea securității datelor cu caracter personal să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice. Prin urmare, încălcarea ar trebui comunicată tuturor celor 99 de angajați, și nu numai celor 10 angajați ale căror informații salariale au fost divulgate.

130. După ce a luat cunoștință de încălcare, operatorul a forțat schimbarea parolei pentru conturile compromise, a blocat trimiterea de e-mailuri către contul de e-mail al atacatorului, l-a informat pe furnizorul de servicii cu privire la e-mailul utilizat de atacator în legătură cu acțiunile sale, a eliminat regulile stabilite de atacator și a perfecționat alertele sistemului de monitorizare pentru a emite o alertă de îndată ce se creează o regulă automată. În mod alternativ, operatorul ar putea elimina dreptul utilizatorilor de a stabili reguli de transmitere, solicitând echipei serviciului IT să facă acest lucru numai la cerere, sau ar putea introduce o politică prin care utilizatorii ar trebui să verifice și să raporteze cu privire la regulile stabilite pentru conturile lor o dată pe săptămână sau mai des, în domeniile în care se prelucrează date financiare.

131. Faptul că o încălcare ar putea avea loc și ar putea rămâne nedetectată atât de mult timp și faptul că, într-o perioadă mai lungă de timp, ingineria socială ar fi putut fi utilizată pentru modificarea unui număr mai mare de date au evidențiat probleme semnificative în sistemul de securitate informatică al operatorului. Aceste probleme trebuie soluționate fără întârziere, de exemplu subliniind importanța revizuirilor proceselor automatizate și a controalelor modificărilor, a detectării incidentelor și a măsurilor de răspuns. Operatorii care gestionează date sensibile, informații financiare etc. au o responsabilitate mai mare în ceea ce privește asigurarea unei securități adecvate a datelor.

Acțiuni necesare în funcție de riscurile identificate		
Documentarea internă	Notificare către AS	Comunicare către persoanele vizate
✓	✓	✓