Ghid 01/2021
Exemple privind notificarea încălcării securității datelor cu caracter personal
(*notificarea breșelor de securitate - n. trad.*)
Adoptat la 14 decembrie 2021
Versiunea 2.0

Traducere în limba română: Daniela Simionovici, Vicepreşedinte ASCPD

Istoricul versiunilor

Versiunea 2.0	14 12 2021	Adoptarea Ghidului după consultare publică
Versiunea 1.0	14 01 2021	Adoptarea Ghidului pentru consultare publică

CUPRINS

CONSILIUL EUROPEAN PENTRU PROTECȚIA DATELOR
Având în vedere articolul 70, alineatul (1), litera e) din Regulamentul 2016/679/UE al Parlamentului European și al Consiliul 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 (Regulamentul general privind protecția datelor),

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

Având în vedere articolul 12 și articolul 22 din Regulamentul său de procedură,

Având în vedere Comunicarea Comisiei către Parlamentul European și Consiliu intitulat *Protecția datelor ca pilon al împuternicirii cetățenilor și abordarea UE față de tranziția digitală - doi ani de aplicare a Regulamentului general privind protecția datelor*[2],

A ADOPTAT URMĂTOARELE ORIENTĂRI

1 INTRODUCERE

1. GDPR introduce, în anumite cazuri, cerința ca o încălcare a securității datelor cu caracter personal să fie notificată către autoritatea națională de supraveghere competentă (denumită în continuare „AS") și să comunice încălcarea securității datelor cu caracter personal către persoanele ale căror date cu caracter personal au fost afectate de încălcarea securității datelor cu caracter personal (articolele 33 și 34).
2. Grupul de lucru „Articol 29" a elaborat deja, în octombrie 2017, un ghid general privind notificarea încălcării datelor, analizând secțiunile relevante ale GDPR (*Orientări privind notificarea privind încălcarea securității datelor cu caracter personal în conformitate cu Regulamentul 2016/679, WP 250*) (denumit în continuare „Orientări WP250)[3]. Cu toate acestea, datorită naturii și momentului său, acest ghid nu a abordat toate problemele practice în mod suficient de detaliat. Prin urmare, a apărut nevoia de o abordare orientată spre practică, bazată pe cazuri, care utilizează experiențele dobândite de AS de când GDPR este aplicabil.
3. Acest document este destinat să completeze Ghidurile WP 250 și reflectă experiențele comune ale AS din SEE de când GDPR a devenit aplicabil. Scopul său este de a ajuta operatorii să decidă cum să gestioneze încălcările securității datelor cu caracter personal și ce factori să ia în considerare în timpul evaluării riscurilor.
4. Ca parte a oricărei încercări de a aborda o încălcare a securității datelor cu caracter personal, operatorul și persoana împuternicită de operator ar trebui să poată recunoaște una, mai întâi. GDPR definește o „încălcare a securității datelor cu caracter personal" la articolul 4 alineatul (12) ca „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 03/2014 privind notificarea încălcării securității datelor cu caracter personal[4] și în Orientările WP 250, WP29 a explicat că încălcările securității datelor cu caracter personal pot fi clasificate în funcție de următoarele trei principii bine-cunoscute de securitate a informațiilor:

[1] Trimiterile la „state membre" făcute în acest document ar trebui înțelese ca referințe la „SEE State membre".
[2] COM(2020) 264 final, 24 iunie 2020.
[3] G29 WP250 rev.1, 6 februarie 2018, Orientări privind notificarea încălcării securtății datelor cu caracter personal conform Regulamentului 2016/679 - aprobat de EDPB, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.0.
[4] G29 WP213, 25 martie 2014, Avizul 03/2014 privind notificarea privind încălcarea datelor cu caracter personal, p. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4.

- „Încălcarea confidențialității” - în cazul în care există o dezvăluire neautorizată sau accidentală a, sau acces la, date cu caracter personal.
- „Încălcarea integrității” - în cazul în care există o modificare neautorizată sau accidentală a datelor cu caracter personal.
- „Încălcarea disponibilității” - în cazul în care există o pierdere accidentală sau neautorizată a accesului la sau distrugerea datelor cu caracter personal [5].

6. O încălcare a securității datelor cu caracter personal poate avea o serie de efecte adverse semnificative asupra persoanelor, care pot avea ca rezultat daune fizice, materiale sau nemateriale. GDPR explică faptul că aceasta poate include pierderea controlului asupra datele personale, limitarea drepturilor, discriminarea, furtul de identitate sau frauda, pierderea financiară, anularea neautorizată a pseudonimizării, deteriorarea reputației și pierderea confidențialității datelor personale protejate de secretul profesional. Poate include, de asemenea, orice alt dezavantaj semnificativ, economic sau social, pentru acei indivizi. Una dintre cele mai importante obligații ale operatorului este evaluarea acestor riscuri pentru drepturile și libertățile persoanelor vizate și punerea în aplicare de măsuri tehnice și organizatorice adecvate pentru abordarea acestora.

7. În consecință, GDPR cere operatorului să:

- documenteze orice încălcare a securității datelor cu caracter personal datelor cu caracter personal, cuprinzând faptele referitoare la încălcarea securității datelor cu caracter personal, a efectelor acesteia și măsurile de remediere întreprinse[6];
- notifice autorității de supraveghere încălcarea securității datelor cu caracter personal, cu excepția cazului în care este puțin probabil ca încălcarea securității datelor cu caracter personal să rezulte într-un risc pentru drepturile și libertățile persoanelor fizice[7];
- comunice persoanei vizate încălcarea securității datelor cu caracter personal atunci când este posibilă ca încălcarea securității datelor cu caracter personal să rezulte într-un risc ridicat pentru drepturile și libertățile persoanelor fizice[8].

8. Breșele de securitate a datelor cu caracter personal sunt probleme în sine, dar pot fi și simptome ale vulnerabilității unui sistem de securitate a datelor învechit, iar acestea pot indica, de asemenea, deficiențe ale sistemului care trebuie abordate. Ca adevăr general, este întotdeauna mai bine să preveniți o breșa de securitate prin pregătire anticipată, atât timp cât mai multe consecințe ale acesteia sunt, prin natura lor, ireversibile. Înainte ca un operator să poată evalua *pe deplin* riscul care decurge dintr-o breșă cauzată de o formă de atac, ar trebui identificată cauza principală a problemei, pentru a stabili dacă vulnerabilitățile care au dat naștere incidentului încă există și, prin urmare, sunt încă exploatabile. În multe cazuri operatorul este capabil să identifice faptul că incidentul este susceptibil să genereze un risc și, prin urmare, urmează să fie notificat. În alte cazuri, notificarea nu trebuie amânată până când riscul și impactul breșei au fost pe deplin evaluate, deoarece evaluarea completă a riscului poate avea loc în paralel cu notificarea și informațiile astfel obținute pot fi furnizate AS fără întârzieri suplimentare nejustificate[9].

9. Breșa de securitate ar trebui să fie notificată atunci când operatorul este de părere că este probabil să aibă ca rezultat un risc pentru drepturile și libertățile persoanei vizate. Operatorii ar trebui să facă această evaluare în momentul în care au luat la cunoștință despre breșă. Operatorul nu trebuie să aștepte efectuarea unei examinări criminalistice detaliate și să facă pași (de început) de atenuare înainte de a evalua dacă breșa de securitate este probabil sau nu să genereze un risc și, prin urmare, ar trebui notificată.

10. Dacă un operator autoevaluează riscul ca fiind improbabil, dar se dovedește că riscul se materializează, AS competentă își poate folosi puterile corective și poate aplica sancțiuni.

---

[5] Vezi Ghidul WP 250, p. 7. - Trebuie avut în vedere faptul că o încălcare a datelor poate viza oricare dintre aceste categorii sau mai multe categorii simultan sau combinate.
[6] GDPR articolul 33 alineatul (5).
[7] GDPR articolul 33 alineatul (1).
[8] GDPR articolul 34 alineatul (1).
[9] GDPR articolul 33 alineatul (4).

11. Fiecare operator și persoană împuternicită de operator ar trebui să aibă planuri și proceduri în vigoare pentru gestionarea eventualelor breșe de securitate. Organizațiile ar trebui să aibă linii de raportare clare și persoane responsabile pentru anumite aspecte ale procesului de recuperare.
12. Instruirea și conștientizarea personalului operatorului și a persoanei împuternicite de operator cu privire la aspectele legate de protecția datelor, cu focalizare pe gestionarea breșelor de securitate a datelor cu caracter personal (identificarea unei breșe de securitate și acțiuni ulterioare care trebuie luate etc.) este, de asemenea, esențială pentru operatori și persoanele împuternicite de operatori. Aceste instruiri trebuie repetate în mod regulat, în funcție de tipul activității de prelucrare și de dimensiunea operatorului, abordând ultimele tendințe și alerte provenite din atacuri cibernetice sau alte incidente de securitate.
13. Principiul responsabilității și conceptul de protecție a datelor din momentul conceperii (*by design*) ar putea include o analiză care se poate introduce în „Manualul privind tratarea breșelor de securitate a datelor cu caracter personal" propriu al operatorului și al persoanei împuternicite de operator, care urmărește să stabilească fapte pentru fiecare fațetă a prelucrării în fiecare etapă majoră a operațiunii. Un astfel de manual pregătit în prealabil ar oferi o sursă de informații mult mai rapidă pentru a permite operatorilor și persoanelor împuternicite de operatori de a reduce riscurile și pentru a-și îndeplini obligațiile fără întârzieri nejustificate. Acesta ar asigura că, dacă ar avea loc o breșă de securitate a datelor cu caracter personal, personalul din organizație ar ști ce să facă și, mai mult ca sigur, incidentul ar fi tratat mai repede decât dacă nu ar exista măsuri sau un plan de atenuare în vigoare.
14. Deși cazurile prezentate mai jos sunt fictive, ele se bazează pe cazuri tipice din experiența colectivă a AS rezultată din notificările privind încălcarea securității datelor cu caracter personal. Analizele oferite se referă în mod explicit la cazurile examinate, dar cu scopul de a oferi asistență operatorilor în evaluarea propriilor breșe de securitate. Orice modificare a circumstanțelor cazurilor descrise mai jos poate avea ca rezultat diferite sau mai semnificative niveluri de risc, necesitând astfel măsuri diferite sau suplimentare. Aceste linii directoare structurează cazurile în conformitate cu anumite categorii de breșe (de exemplu, atacuri ransomware). Anumite măsuri de atenuare se aplică în fiecare caz atunci când se confruntă cu o anumită categorie de breșe. Aceste măsuri nu sunt neapărat repetate în fiecare caz analizat aparținând aceleiași categorii de breșe. Pentru cazurile aparținând aceleiași categorii de breșe sunt prezentate doar diferențele. Prin urmare, cititorul ar trebui să citească toate cazurile relevante pentru categoria relevantă de breșe de securitate pentru a identifica și a distinge toate măsurile corecte care trebuie luate.
15. Documentarea internă a unei breșe este o obligație independentă de riscurile aferente acesteia și trebuie efectuată în fiecare caz. Cazurile prezentate mai jos încearcă să pună în lumină dacă să se notifice sau nu breșa către AS și să o comunice persoanelor vizate.

2 RANSOMWARE

16. O cauză frecventă pentru o notificare de încălcare a securității datelor cu caracter personal este un atac ransomware suferit de operator. În aceste cazuri, un cod rău intenționat criptează datele personale, iar ulterior atacatorul cere operatorului o răscumpărare în schimbul codului de decriptare. Acest tip de atac poate fi de obicei clasificat ca o breșă de disponibilitate, dar, de multe ori, ar putea apărea și ca o încălcare a confidențialității.

2.1 CAZ Nr. 01: Ransomware cu backup adecvat și fără exfiltrare[10]

Sistemele informatice ale unei mici companii de producție au fost expuse unui atac ransomware și datele stocate în acele sisteme au fost criptate. Operatorul a folosit criptarea în repaus[11], deci toate datele accesate de ransomware au fost stocate în formă criptată folosind o criptare cu un algoritm de ultimă generație.

[10] Exfiltrarea datelor reprezintă copierea, transferul sau regăsirea neautorizată a datelor de pe un computer sau server. Exfiltrarea datelor este cunoscută și sub denumirea de extrudare de date, export de date sau furt de date . - *n. trad.*
[11] Datele în repaus sunt datele stocate pe hard disk-uri sau SSD-uri aflate în utilizarea curentă a operatorului- *n. trad.*

Cheia de decriptare nu a fost compromisă în atac, adică atacatorul nu a putut nici să o acceseze și nici să o folosească indirect. În consecință, atacatorul a avut acces doar la date personale criptate. În mod particular, nici sistemul de e-mail al companiei, nici sistemele client utilizate pentru a-l accesa nu au fost afectate.
Compania folosește expertiza unei companii externe de securitate cibernetică pentru a investiga incidentul. Jurnalele care urmăresc toate fluxurile de date care părăsesc compania (inclusiv e-mailul de ieșire) sunt disponibile. După analizarea jurnalelor și a datelor colectate de sistemele de detectare lansate / utilizate de companie, o investigație internă desfășurată de compania externă de securitate cibernetică a stabilit *cu certitudine* că făptuitorul a criptat doar datele, fără a le exfiltra. Jurnalele arată că nu a existat flux de date către exterior / în ieșire în intervalul de timp de desfășurare a atacului.
Datele personale afectate de breșă se referă la câteva zeci de persoane în total, clienți și angajați ai companiei.
Un backup a fost ușor disponibil, iar datele au fost restaurate la câteva ore după ce a avut loc atacul.
Breșa nu a rezultat în nicio consecință asupra funcționării de zi cu zi a operatorului. Nu a existat nicio întârziere la plata angajaților sau gestionarea cererilor clienților.

17. În acest caz, din definiția unei „încălcări a securității datelor cu caracter personal” s-au realizat următoarele elemente: o breșă de securitate a condus la modificarea ilegală și accesul neautorizat la datele personale stocate.

2.1.1 CAZ Nr. 01 - Măsuri prealabile și evaluarea riscurilor

18. Ca și în cazul tuturor riscurilor prezentate de actorii externi, probabilitatea ca un atac ransomware să aibă succes poate fi redus drastic prin înăsprirea securității mediului de control al datelor. Majoritatea acestor breșe pot fi prevenite prin asigurarea că au fost luate măsuri de securitate organizaționale, fizice și tehnologice adecvate. Exemple de astfel de măsuri sunt gestionarea adecvată a patch-urilor[12] și utilizarea unui sistem adecvat de detectare anti-malware. Având o copie de rezervă adecvată și separată va ajuta la atenuarea consecințelor unui atac de succes, în cazul în care acesta ar avea loc. Mai mult, un program de educare, formare și conștientizare a angajaților în domeniul securității (EFCS) va ajuta la prevenirea și recunoașterea acestui tip de atac. (O listă de măsuri recomandate pot fi găsite în secțiunea 2.5.) Printre acele măsuri, o gestionare adecvată a patch-urilor care asigură că sistemele sunt actualizate și toate vulnerabilitățile cunoscute ale sistemelor implementate sunt remediate este una dintre cele mai importante, deoarece majoritatea atacurilor ransomware exploatează vulnerabilități bine cunoscute.
19. Atunci când evaluează riscurile, operatorul ar trebui să investigheze breșa și să identifice tipul de cod rău intenționat pentru a înțelege posibilele consecințe ale atacului. Printre acele riscuri care trebuie luate în considerare se numără și riscul ca acele date să fi fost exfiltrate fără a lăsa urme în jurnalele sistemelor.
20. În acest exemplu, atacatorul a avut acces la datele personale și confidențialitatea textului cifrat care conținea datele personale în formă criptată au fost compromise. Cu toate acestea, orice date care ar fi putut fi exfiltrate nu pot fi citite sau folosite de către făptuitor, cel puțin pentru moment. Metoda de criptare folosită de operator se conformează cu stadiul cel mai înalt al tehnicii. Cheia de decriptare nu a fost compromisă și probabil că nu ar putea fi determinată prin alte mijloace. În consecință, riscul de confidențialitate pentru drepturile și libertățile persoanelor fizice sunt reduse la minimum, cu excepția progresului criptoanalitic care face ca datele criptate să poată fi inteligibile în viitor.

[12] Patch - este o mică bucată de software care este folosit pentru a corecta o problemă, numită de obicei un *bug* - *n. trad.*

21. Operatorul ar trebui să ia în considerare riscul pentru persoanele fizice din cauza breșei[13]. În acest caz, se pare că riscul pentru drepturile și libertățile persoanelor vizate rezultă din lipsa disponibilității datelor cu caracter personal, dar confidențialitatea datelor cu caracter personal nu este compromisă[14]. În acest exemplu, efectele adverse ale breșei au fost atenuate destul de curând după ce aceasta a avut loc. Având un regim de backup adecvat[15] face efectele breșei mai puțin severe și aici operatorul a putut să îl folosească în mod eficient.
22. În ceea ce privește gravitatea consecințelor pentru persoanele vizate, au putut fi identificate doar consecințe minore întrucât datele afectate au fost restaurate în câteva ore, breșa nu a avut consecințe asupra funcționării de zi cu zi a operatorului și nu a avut niciun efect semnificativ asupra persoanelor vizate (de exemplu, plățile angajaților sau gestionarea cererilor clienților).

2.1.2 CAZUL Nr. 01 – Atenuare și obligații

23. Fără o copie de rezervă, operatorul poate lua puține măsuri de remediere pentru pierderea datelor cu caracter personal, iar datele trebuie colectate din nou. În acest caz particular, însă, impactul atacului ar putea să fie limitat în mod eficient prin resetarea tuturor sistemelor compromise la o stare „curată" despre care se știe că nu este infectată cu codul rău intenționat, reparând vulnerabilitățile și restabilind datele afectate imediat după atac. Fără o copie de rezervă, datele se pierde și severitatea poate crește, deoarece, de asemenea, riscurile sau impactul asupra indivizilor pot crește.
24. Promptitudinea unei restabiliri eficiente a datelor dintr-un backup ușor accesibil este o variabilă cheie când se analizează breșa. Precizarea unui interval de timp adecvat pentru restaurarea datelor compromise depinde de circumstanțele unice ale breșei în cauză. GDPR prevede că o încălcare a securității datelor cu caracter personal va fi notificată fără întârzieri nejustificate și, acolo unde este posibil, nu mai târziu de 72 de ore. Prin urmare, s-ar putea determina că depășirea limitei de timp de 72 de ore este nerecomandabilă în orice caz, dar, atunci când avem de-a face cu cazuri cu nivel de risc ridicat, chiar și respectarea acestui termen limită poate fi considerată nesatisfăcătoare.
25. În acest caz, în urma unei evaluări detaliate a impactului și a unui proces de răspuns la incident, operatorul a stabilit că breșa este puțin probabil să aibă ca rezultat un risc pentru drepturile și libertățile persoanelor fizice, prin urmare, nu este necesară nicio comunicare către persoanele vizate și nici nu necesită o notificare a breșei către AS. Cu toate acestea, ca toate încălcările securității datelor cu caracter personal, acestea ar trebui documentate în conformitate cu articolul 33 alineatul (5). Organizația poate avea, de asemenea, nevoie (sau mai târziu să fie solicitată de către AS), să-și actualizeze și să revizuiască procedurile și măsurile tehnice și organizatorice de gestionare a securității datelor cu caracter personal și de atenuare a riscurilor. În cadrul acestui proces actualizare și remediere, organizația ar trebui să investigheze amănunțit breșa și să identifice cauzele și metodele folosite de făptuitor, pentru a preveni eventualele evenimente similare în viitor.

---

[13] Pentru îndrumări cu privire la operațiunile de prelucrare „probabil să aibă ca rezultat un risc ridicat", a se vedea „Orientări privind Evaluarea impactului asupra protecției datelor (EIPD)" ale Grupul de lucru A29 și stabilirea dacă prelucrarea este „probabil să aibă ca rezultat un risc ridicat", în sensul Regulamentului 2016/679", WP248 rev. 01, - avizat de EDPB, https://ec.europa.eu/newsroom/article29/items/611236, p. 9.
[14] Din punct de vedere tehnic, criptarea datelor va implica „accesul" la datele originale, iar în cazul ransomware-ului, ștergerea originalului – datele trebuie să fie accesate prin cod ransomware pentru a le cripta și pentru a elimina datele originale. Un atacator poate lua o copie a originalului înainte de ștergere, dar datele personale nu vor fi întotdeauna extrase. Pe măsură ce investigația operatorului progresează, noi informații pot ieși la lumină pentru a schimba această evaluare. Accesarea ilegală care are ca rezultat distrugerea, pierderea, modificarea, dezvăluirea neautorizată a datelor cu caracter personal sau un risc de securitate pentru un persoana vizată, chiar și fără interpretarea datelor poate fi la fel de severă ca accesul la date, cu interpretarea datelor personale.
[15] Procedurile de backup trebuie să fie structurate, consecvente și repetabile. Exemple de proceduri de backup sunt metoda 3-2-1 și metoda bunic-tată-fiu. Orice metodă trebuie întotdeauna testată pentru eficacitatea acoperirii și când datele urmează să fie restaurate. Testarea ar trebui, de asemenea, să fie repetată la intervale de timp și mai ales atunci când apar modificări în operațiunile de prelucrare sau în circumstanțele acestora, pentru a asigura integritatea sistemului.

Acțiuni necesare pe baza riscurilor identificate		
Documentație internă	Notificare către AS	Comunicare către persoanele vizate
√	X	X

2.2 CAZ Nr. 02: Ransomware fără backup adecvat

Unul dintre computerele folosite de o companie agricolă a fost expus unui atac ransomware și datele acestuia au fost criptate de către atacator.
Compania folosește expertiza unei companiei externe de securitate cibernetică să-și monitorizeze rețeaua. Jurnalele care urmăresc toate fluxurile de date care părăsesc compania (inclusiv e-mail de ieșire) sunt disponibile. După analizarea jurnalelor și a datelor colectate de celelalte sisteme de detectare, ancheta internă efectuată cu ajutorul companiei de securitate cibernetică a stabilit că făptuitorul a criptat doar datele, fără a le exfiltra. Jurnalele nu arată niciun flux de date către exterior, în intervalul de timp al atacului.
Datele personale afectate de breșă se referă la angajați și clienți ai companiei, câteva zeci de persoane în total. Nu au existat categorii speciale de date afectate.
Nu a fost disponibilă nicio copie de rezervă în format electronic. Majoritatea datelor au fost restaurate de pe copiile de rezervă pe suport de hârtie. Restaurarea datelor a durat 5 zile lucrătoare și a dus la întârzieri minore în livrarea comenzilor către clienți.

2.2.1 CAZ NR. 02 - Măsuri prealabile și evaluarea riscurilor

26. Operatorul ar fi trebuit să adopte aceleași măsuri prealabile ca cele menționate în partea 2.1. și în secțiunea 2.9. Diferența majoră față de cazul precedent este lipsa unui backup electronic și lipsa criptării la repaus. Acest lucru duce la diferențe critice în următorii pași.
27. La evaluarea riscurilor, operatorul ar trebui să investigheze metoda de infiltrare și să identifice tipul codului rău intenționat pentru a înțelege posibilele consecințe ale atacului. În acest exemplu, ransomware-ul a criptat datele personale fără a le exfiltra. Ca urmare, riscurile care apar la adresa drepturilor și libertățile persoanelor vizate rezultă din lipsa disponibilității datelor cu caracter personal, dar confidențialitatea datelor cu caracter personal nu este compromisă. O examinare amănunțită a jurnalelor de firewall și implicațiile sale sunt esențiale în determinarea riscului. Operatorul ar trebui să prezinte, la cerere, constatările de fapt ale acestor investigații.
28. Operatorul trebuie să aibă în vedere că, dacă atacul este mai sofisticat, malware-ul are funcționalitate pentru a edita fișierele jurnal și a elimina urma. Deci - dat fiind că jurnalele nu sunt transmise sau replicate către un server central de jurnal – chiar și după o investigație amănunțită care a stabilit că datele personale nu au fost exfiltrate de atacator, operatorul nu poate afirma că absența unei intrări în jurnal dovedește absența de exfiltrare, prin urmare, probabilitatea unei încălcări a confidențialității nu poate fi respinsă în totalitate.
29. Operatorul ar trebui să evalueze riscurile acestei breșe[16] dacă datele au fost accesate de către atacator. Pe parcursul evaluării riscurilor, operatorul ar trebui să ia în considerare și natura, sensibilitatea, volumul și contextul datelor cu caracter personal afectate de încălcare. În acest caz nu există categorii speciale de date personale afectate, iar cantitatea de date personale expuse și numărul persoanelor vizate afectate sunt scăzute.
30. Culegerea de informații exacte privind accesul neautorizat este cheia pentru determinarea nivelului de risc și prevenirea un atac nou sau continuat. Dacă datele ar fi fost copiate din baza de date, evident că ar fi fost un factor de creștere a riscului. Când sunteți nesigur cu privire la specificul accesului nelegitim, cel mai rău scenariu ar trebui luat în considerare și riscul ar trebui evaluat în consecință.
31. Absența unei baze de date de rezervă poate fi considerată un factor de creștere a riscului, în funcție de severitatea consecințelor pentru persoanele vizate rezultate din lipsa disponibilității datelor.

[16] Pentru îndrumări cu privire la operațiunile de prelucrare „probabil să aibă ca rezultat un risc ridicat”, a se vedea nota de subsol 10 de mai sus.

2.2.2 CAZUL Nr. 02 – Atenuare și obligații

32. Fără o copie de rezervă, operatorul poate lua puține măsuri de remediere pentru pierderea datelor cu caracter personal, iar datele trebuie colectate din nou, cu excepția cazului în care este disponibilă o altă sursă (de exemplu, e-mailuri de confirmare a comenzii). Fără o copie de rezervă, datele se pot pierde, iar gravitatea va depinde de impactul asupra indivizilor.

33. Restaurarea datelor nu ar trebui să se dovedească a fi excesiv de problematică[17] dacă datele sunt încă disponibile pe hârtie, dar, având în vedere lipsa unei baze de date electronice de rezervă, se consideră necesară o notificare către AS, întrucât restaurarea datelor a durat ceva timp și ar putea cauza unele întârzieri în livrarea comenzilor către clienți și o cantitate considerabilă de metadate (de exemplu, jurnalele, marcajele de timp) ar putea să nu poată fi recuperate.

34. Informarea persoanelor vizate cu privire la breșă poate depinde, de asemenea, de durata în care datele cu caracter personal sunt indisponibile și dificultățile pe care le-ar putea cauza, ca urmare, în funcționarea operatorului (de exemplu, întârzieri în transferul plăților către angajați). Deoarece aceste întârzieri în plăți și livrări pot duce la pierderi financiare pentru persoanele ale căror date au fost compromise, s-ar putea argumenta, de asemenea, că breșa ar putea avea ca rezultat un risc ridicat. De asemenea, s-ar putea să nu fie posibil să se evite informarea persoanelor vizate dacă contribuția lor este necesară la restabilirea datelor criptate.

35. Acest caz servește ca exemplu pentru un atac ransomware cu risc pentru drepturile și libertățile persoanelor vizate, dar neatingând un risc ridicat. Ar trebui să fie documentată în conformitate cu articolul 33 alineatul (5) și notificată către AS în conformitate cu articolul 33 alineatul (1). De asemenea, organizația poate avea nevoie (sau poate fi solicitată de AS) să-și actualizeze și să revizuiască procedurile și măsurile tehnice și organizatorice de gestionare a securității datelor cu caracter personal și de atenuare a riscurilor.

Acțiuni necesare pe baza riscurilor identificate		
Documentație internă	Notificare către AS	Comunicare către persoanele vizate
√	√	X

2.3 CAZ Nr. 03: Ransomware cu backup și fără exfiltrare într-un spital

Sistemul informatic al unui spital/centru de sănătate a fost expus unui atac ransomware și o proporție semnificativă din datele sale au fost criptate de către atacator.

Compania folosește expertiza unei companii externe de securitate cibernetică pentru a-și monitoriza rețeaua. Jurnalele, care urmăresc toate fluxurile de date care părăsesc compania (inclusiv e-mailul de ieșire), sunt disponibile. După ce a analizat jurnalele și datele colectate de celelalte sisteme de detectare, investigația internă, ajutată de compania de securitate cibernetică a stabilit că făptuitorul a criptat doar datele, fără a le exfiltra. Jurnalele arată ca nu a existat flux de date spre exterior în intervalul de timp al atacului.

Datele personale afectate de breșă se refereau la angajați și pacienți, care reprezentau mii de indivizi.

Au fost disponibile copii de rezervă în format electronic. Majoritatea datelor au fost restaurate, dar această operațiune a durat 2 zile lucrătoare și a dus la întârzieri majore în tratarea pacienților, la intervenții chirurgicale anulate/amânate și la o scădere a nivelului serviciilor din cauza indisponibilității sistemelor.

[17] Acest lucru va depinde de complexitatea și structura datelor cu caracter personal. În cele mai complexe scenarii, restabilirea integrității datelor, coerența cu metadatele, asigurarea relațiilor corecte în cadrul structurilor de date și verificarea acurateței datelor poate necesita resurse și efort semnificativ.

2.3.1 CAZ NR. 03 - Măsuri prealabile și evaluarea riscurilor

36. Operatorul ar fi trebuit să adopte aceleași măsuri prealabile ca cele menționate în partea 2.1. și în secțiunea 2.5. Diferența majoră față de cazul precedent este severitatea ridicată a consecințelor pentru o parte substanțială a persoanelor vizate[18].

37. Volumul de date personale și numărul persoanelor vizate afectate de breșă sunt mari, deoarece spitalele procesează, de obicei, cantități mari de date. Indisponibilitatea datelor are un impact mare asupra unei părți substanțiale a persoanele vizate. În plus, există un risc rezidual de severitate ridicată asupra confidențialității datelor pacienților.

38. Tipul încălcării, natura, sensibilitatea și volumul datelor cu caracter personal afectate de încălcare sunt importante. Chiar dacă a existat o copie de rezervă a datelor și a putut fi restaurată în câteva zile, există încă un risc mare din cauza gravității consecințelor pentru persoanele vizate, rezultat din lipsa disponibilității datelor la momentul atacului și în zilele următoare.

2.3.2 CAZUL Nr. 03 – Atenuare și obligații

39. Se consideră necesară o notificare către AS, întrucât sunt implicate categorii speciale de date cu caracter personal și restaurarea datelor ar putea dura mult timp, ceea ce duce la întârzieri majore în îngrijirea pacienților. Informarea persoanelor vizate despre breșă este necesară din cauza impactului pentru pacienți, chiar și după restaurarea datelor criptate. În timp ce datele referitoare la toți pacienții tratați în spital în ultimii ani au fost criptate, au fost afectați numai acei pacienți care au fost programați să fie tratați în spital în timpul cât sistemul informatic a fost indisponibil. Operatorul ar trebui să comunice breșa direct acelor pacienți. Comunicarea directă cu ceilalți pacienți, dintre care unii poate nu au fost în spital mai bine de douăzeci de ani, ar putea să nu mai fie necesară din cauza excepției prevăzute la articolul 34 alineatul (3) litera c). Într-un astfel de caz, în schimb, acolo se va face o comunicare publică[19] sau se va lua o măsură similară prin care persoanele vizate să fie informate într-un mod la fel de eficient. În acest caz, spitalul ar trebui să facă publice atacul ransomware și efectele acestuia.

40. Acest caz servește ca exemplu pentru un atac ransomware cu risc ridicat pentru drepturile și libertățile persoanelor vizate. Ar trebui să fie documentat în conformitate cu articolul 33 alineatul (5), notificat AS în conformitate cu art. 33 alin. (1) și comunicat persoanelor vizate în conformitate cu art. 34 alin. (1). Organizația trebuie, de asemenea, să-și actualizeze și să revizuiască procedurile și măsurile tehnice și organizatorice de gestionare a securității datelor cu caracter personal și de atenuare a riscurilor.

Acțiuni necesare pe baza riscurilor identificate		
Documentație internă	Notificare către AS	Comunicare către persoanele vizate
√	√	√

2.4 CAZ Nr. 04: Ransomware fără backup și cu exfiltrare

Serverul unei companii de transport public a fost expus unui atac ransomware și datele sale au fost criptate de către atacator. Conform constatărilor anchetei interne, făptuitorul nu doar a criptat datele, dar le-a și exfiltrat. Tipul de date afectate de breșă au fost datele personale ale clienților și angajaților, precum și datele personale ale celor câteva mii de persoane care folosesc serviciile companiei (de ex. cumpărând bilete online). Dincolo de datele de identitate de bază, au fost afectate de breșă și

[18] Pentru îndrumări cu privire la operațiunile de prelucrare „probabil să aibă ca rezultat un risc ridicat”, a se vedea nota de subsol 10 de mai sus.

[19] Considerentul 86 al GDPR explică că „Comunicările 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.”

numerele cărților de identitate și date financiare, cum ar fi detaliile cardului de credit. A existat o bază de date de rezervă, dar a fost criptată de atacator.

2.4.1 CAZ NR. 04 - Măsuri prealabile și evaluarea riscurilor

41. Operatorul ar fi trebuit să adopte aceleași măsuri prealabile ca cele menționate în partea 2.1. și în secțiunea 2.5. Deși a existat o baza de date de rezervă, acesta a fost, de asemenea, afectată de atac. Acest fapt ridică întrebări despre calitatea măsurilor anterioare de securitate IT ale operatorului și ar trebui analizate în continuare în timpul investigației, deoarece într-un regim de backup bine conceput, backup-urile multiple trebuie să fie stocate în siguranță fără acces din sistemul principal, altfel ar putea fi compromise în același atac. În plus, atacurile ransomware pot rămâne nedescoperite zile întregi, criptând încet datele rar utilizate. Acest lucru poate face backup-urile multiple inutile, așa că, și backup-urile ar trebui să fie efectuate periodic și să fie izolate. Acest lucru ar crește probabilitatea de recuperare, deși cu pierderi crescute de date.

42. Această breșă se referă nu numai la disponibilitatea datelor, ci și la confidențialitate, atât timp cât atacatorul ar fi putut modifica și/sau copia date de pe server. Prin urmare, tipul breșei are ca rezultat un risc ridicat[20].

43. Natura, sensibilitatea și volumul datelor cu caracter personal crește și mai mult riscurile, deoarece numărul de persoane afectate este mare, la fel ca și cantitatea totală de date cu caracter personal prelucrate. Dincolo de datele de identitate de bază, sunt implicate și documentele de identitate și datele financiare, cum ar fi detaliile cardului de credit. O breșă care afectează aceste tipuri de date prezintă un risc ridicat în sine și, dacă sunt prelucrate împreună, ar putea fi utilizate, printre altele, pentru furtul de identitate sau pentru fraudă.

44. Din cauza logicii defectuoase a serverului sau a controalelor organizaționale, fișierele de rezervă au fost afectate de ransomware, prevenind restabilirea datelor și crescând riscul.

45. Această breșă prezintă un risc ridicat pentru drepturile și libertățile persoanelor, deoarece ar putea duce probabil, atât la daune materiale (de exemplu, pierderi financiare, deoarece detaliile cardului de credit au fost afectate), cât și nemateriale (de ex. furtul de identitate sau frauda, deoarece detaliile 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 face demersurile necesare pentru a evita daunele materialele (de exemplu, blocarea cardurilor de credit).

47. Pe lângă documentarea breșei, în conformitate cu articolul 33 alineatul (5), o notificare către AS este, de asemenea, obligatorie în acest caz [articolul 33 alin. (1)], iar operatorul este, de asemenea, obligat să comunice breșa către persoanele vizate [articolul 34 alineatul (1)]. Aceasta din urmă ar putea fi întreprinsă în regim persoană cu persoană, dar, pentru persoanele fizice ale căror date de contact nu sunt disponibile, operatorul ar trebui să facă acest lucru în mod public, cu condiția ca o astfel de comunicare să nu fie susceptibilă să declanșeze consecințe negative suplimentare asupra persoanelor vizate, de ex. notificarea se poate face prin intermediul site-ul organizației. În acest din urmă caz este necesară o comunicare precisă și clară, la vedere, pe pagina de start a site-ului a operatorului, cu referințe exacte ale dispozițiilor GDPR relevante. Organizația ar putea, de asemenea, să-și actualizeze și să revizuiască procedurile și măsurile tehnice și organizatorice de gestionare a securității datelor cu caracter personal și de atenuare a riscurilor

Acțiuni necesare pe baza riscurilor identificate		
Documentație internă	Notificare către AS	Comunicare către persoanele vizate
√	√	√

[20] Pentru îndrumări cu privire la operațiunile de prelucrare „probabil să aibă ca rezultat un risc ridicat”, a se vedea nota de subsol 10 de mai sus.

2.5 Măsuri tehnice și organizatorice pentru prevenirea/atenuarea impactului atacurilor ransomware

48. Faptul că un atac ransomware a putut avea loc este, de obicei, un semn al uneia sau mai multor vulnerabilități în sistemul operatorului. Acest lucru se aplică și în cazurile de ransomware în care datele personale au fost criptate, dar nu au fost exfiltrate. Indiferent de rezultat și de consecințele atacului, oricât de mult s-ar insista pe importanța unei evaluări cuprinzătoare a sistemului de securitate a datelor - cu accent deosebit pe securitatea IT - nu este niciodată suficient. Punctele slabe și deficiențele de securitate identificate trebuie să fie documentate și adresate fără întârziere.

49. **Măsuri recomandate:**

(*Lista următoarelor măsuri nu este deloc exclusivă sau cuprinzătoare. Mai degrabă, scopul este de a oferi idei de prevenire și posibile soluții. Fiecare activitate de prelucrare este diferită, deci operatorul ar trebui să ia decizia asupra măsurilor care se potrivesc cel mai mult cu situația dată.*)

- Menținerea actualizată a firmware-ului[21], a sistemului de operare și a aplicației software pe servere, mașini client, componente active de rețea și orice alte mașini de pe aceeași rețea LAN (inclusiv dispozitive Wi-Fi). Asigurați-vă că sunt în vigoare măsuri de securitate IT adecvate, că sunt eficiente și sunt actualizate în mod regulat, atunci când prelucrarea sau circumstanțele se schimbă sau evoluează. Aceasta include păstrarea jurnalelor detaliate despre ce patch-uri sunt aplicate în fiecare moment.
- Proiectarea și organizarea sistemelor și infrastructurii de prelucrare pentru segmentarea sau izolarea sistemelor de date și rețelelor pentru a evita propagarea malware-ului în cadrul organizației și către sistemele externe.
- Existența unei proceduri de backup actualizate, sigure și testate. Dispozitivele de stocare pe termen mediu și lung a backup-ului ar trebui păstrate separat de mediile de stocare aflate în utilizare curentă și să nu fie la îndemâna terților, chiar și în cazul unui atac reușit (cum ar fi backup incremental, zilnic și backup complet, săptămânal).
- Deținerea/obținerea unui software anti-malware adecvat, actualizat, eficient și integrat.
- Deținerea și utilizarea unui sistem integrat de prevenire și de detectare a intruziunilor cu un firewall adecvat, actualizat, și eficient. Dirijarea traficului de rețea prin firewall/detecția intruziunilor, chiar și în cazul muncii de la domiciliu sau al telemuncii (de exemplu, prin utilizarea conexiunilor VPN la mecanismele de securitate organizaționale când se accesează internetul).
- Instruirea angajaților cu privire la metodele de recunoaștere și prevenire a atacurilor IT. Operatorul ar trebui să furnizeze mijloace pentru a 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 când s-a realizat un astfel de atac, cum să deconecteze punctul final din rețea și despre obligația lor de a raporta imediat atacul ofițerului de securitate.
- Sublinierea necesității identificării tipului de cod rău intenționat pentru a vedea consecințele atacului și să se poată găsi măsurile potrivite pentru a reduce riscul. În cazul în care un atac ransomware a reușit și nu există nicio copie de rezervă disponibilă, recuperarea datelor se poate face utilizând instrumente disponibile, cum ar fi cele de la „Fără răscumpărare” (nomoreransom.org). Cu toate acestea, în cazul în care este disponibilă o copie de rezervă sigură, este recomandabilă restaurarea datelor de pe aceasta.
- Redirecționarea sau replicarea tuturor jurnalelor către un server central de jurnal (incluzând eventual semnarea sau criptarea mărcilor temporale ale intrărilor de jurnal).
- Criptare puternică și autentificare cu mai mulți factori, în special pentru accesul administrativ la sistemele IT, gestionarea adecvată a cheilor și parolelor.

[21] (FIRM softWARE) - Instrucțiuni de software care se află într-un spațiu de stocare nevolatil, care își păstrează conținutul fără alimentare. Firmware-ul se găsește pe plăcile de bază ale computerelor pentru a păstra setările hardware și datele de pornire (vezi BIOS) și pe nenumărate dispozitive electronice pe care sunt instalate sisteme de operare și aplicații - *n. trad.*

- Testare de vulnerabilitate și penetrare în mod regulat.
- Înființați în cadrul organizației o echipă de răspuns la incidente de securitate informatică (CSIRT) sau o echipă de răspuns în caz de urgență computerizată (CERT), sau alăturați-vă unui CSIRT/CERT colectiv. Creați un plan de răspuns la incident, un plan de recuperare în caz de dezastru și un plan de continuitate a afacerii și asigurați-vă că acestea sunt testate temeinic.
- Atunci când se evaluează contramăsurile – analiza riscului trebuie revizuită, testată și actualizată.

3 ATACURI DE EXFILTRARE A DATELOR

50. Atacurile care exploatează vulnerabilitățile serviciilor oferite terților de către operator, prin internet, de ex. atacuri comise prin injectare de cod (de exemplu, injectare de cod SQL, traversare a căii[22]), compromiterea site-ului web și metode similare, pot semăna cu atacurile ransomware, prin aceea că riscul provine din acțiunea unei terțe părți neautorizate, dar aceste atacuri vizează de obicei copierea, exfiltrarea și abuzul de date cu caracter personal pentru un scop rău intenționat. Prin urmare, acestea sunt, în principal, breșe de confidențialitate și, posibil, de asemenea, de integritate a datelor. În același timp, dacă operatorul este conștient de caracteristicile acestui tip de breșe, există multe măsuri disponibile operatorilor care pot reduce substanțial riscul executării cu succes a unui atac.

3.1 CAZ Nr. 05: Exfiltrarea datelor privind cererile de angajare de pe un site web

O agenție de ocupare a forței de muncă a fost victima unui atac cibernetic, care a plasat un cod rău intenționat pe site-ul său.
Acest cod rău intenționat a făcut ca informațiile personale să fie transmise prin intermediul formularelor de cerere de angajare online și stocate pe serverul web accesibil persoanelor neautorizate. Este posibil să fi fost afectate 213 astfel de formulare, dar, în urma analizei datelor afectate, s-a stabilit că breșa nu a afectat categorii speciale de date.
Setul de instrumente malware instalat avea funcționalități care i-au permis atacatorului să elimine orice istoric de exfiltrare și, de asemenea, a permis monitorizarea prelucrărilor de pe server și capturarea de date personale. Setul de instrumente a fost descoperit doar la o lună de la instalare.

3.1.1 CAZ NR. 05 - Măsuri prealabile și evaluarea riscurilor

51. Securitatea mediului operatorului este extrem de importantă, deoarece majoritatea acestor încălcări poate fi prevenită prin asigurarea faptului că toate sistemele sunt actualizate în mod constant, că datele sensibile sunt criptate și că aplicațiile sunt dezvoltate conform standardelor înalte de securitate, cum ar fi autentificarea puternică, măsurile împotriva atacurilor tip „forță brută", „evadarea" sau „igienizarea"[23] intrărilor utilizatorilor etc. Audituri periodice de securitate IT, evaluări de vulnerabilitate și teste de penetrare sunt, de asemenea, necesare pentru a detecta anticipat acest tip de vulnerabilități și a le remedia. În acest caz particular, instrumentele de monitorizare a integrității fișierelor în mediul de producție ar putea să fi ajutat la detectarea injectării codului. (O listă cu măsurile recomandate se găsește în secțiunea 3.7).
52. Operatorul ar trebui să înceapă întotdeauna să investigheze breșa prin identificarea tipului de atac și a metodelor acestuia, pentru a evalua ce măsuri trebuie luate. Pentru a fi rapid și eficient, operatorul ar trebui să aibă un plan de răspuns la incident, care să specifice pașii rapizi și necesari pentru preluarea controlului asupra incidentului. În acest caz particular, tipul breșei a fost un factor de creștere a riscului, deoarece nu numai că a fost redusă

[22] Directory traversal (cunoscut și sub numele de file *path traversal*) este o vulnerabilitate de securitate web care permite unui atacator să citească fișiere arbitrare de pe serverul care rulează o aplicație. Acestea pot include codul aplicației și datele, acreditările pentru sistemele back-end și fișierele sensibile ale sistemului de operare. - *n. trad.*
[23] Evadarea sau igienizarea intrărilor utilizatorului este o formă de validare a intrărilor, care asigură că numai datele formatate corespunzător sunt introduse într-un sistem informatic.

confidențialitatea datelor, atacatorul a avut și mijloacele de a face modificări în sistem, deci integritatea datelor a devenit, de asemenea, discutabilă.

53. Natura, sensibilitatea și volumul datelor cu caracter personal afectate de încălcare ar trebui evaluate pentru a determina în ce măsură breșa a afectat persoanele vizate. Deși nu au existat categorii speciale de date cu caracter personal afectate, datele accesate din formularele online conțin informații considerabile despre persoane și, astfel de date, ar putea fi utilizate greșit în mai multe moduri (marketing nesolicitat direcționat, furt de identitate, etc.), astfel încât gravitatea consecințelor ar trebui să crească riscul pentru drepturile și libertățile persoanelor vizate[24].

3.1.2 CAZUL Nr. 05 – Atenuare și obligații

54. Dacă este posibil, după rezolvarea problemei, baza de date ar trebui comparată cu cea de backup stocată într-un spațiu securizat. Experiențele obținute în urma breșei ar trebui utilizate în actualizarea infrastructurii IT. Operatorul ar trebui să readucă toate sistemele IT infectate la o stare curată cunoscută, să remedieze vulnerabilitatea și să implementeze noi măsuri de securitate pentru a evita, în viitor, breșe similare, de ex. verificări de integritate a fișierelor și audituri de securitate. Dacă datele cu caracter personal nu au fost doar exfiltrate, ci și șterse, operatorul trebuie să ia măsuri sistematice de recuperare a datelor cu caracter personal în starea în care se aflau înainte de breșă. Poate fi necesar un backup complet, modificări incrementale și apoi, eventual, reluarea prelucrării de la ultimul backup incremental – care necesită ca operatorul să poată reproduce modificările făcute de la ultimul backup. Acest lucru putea însemna ca operatorul să aibă sistemul proiectat pentru a păstra fișierele zilnice de intrare în cazul în care este nevoie să fie prelucrate din nou și necesită o metodă robustă de stocare și o politică de stocare adecvată.

55. Având în vedere cele de mai sus, întrucât breșa este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor vizate, acestea ar trebui să fie cu siguranță informate cu privire la aceasta [articolul 34 alineatul (1)], ceea ce înseamnă, desigur, că AS(urile) relevante ar trebui să fie, de asemenea, implicate sub forma unei notificări privind încălcarea securității datelor personale. Documentarea încălcării este obligatorie, conform articolului 33 (5) GDPR și facilitează evaluarea situației.

Acțiuni necesare pe baza riscurilor identificate		
Documentație internă	Notificare către AS	Comunicare către persoanele vizate
√	√	√

3.2 CAZ Nr. 06: Exfiltrarea parolei hashed de pe un site web

O vulnerabilitate de tip „injectare cu cod SQL” a fost exploatată pentru a avea acces la o bază de date a serverului unui site de artă culinară. Utilizatorilor li se permitea să aleagă doar 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 „hashed”[25] (codate - *n. trad.*) cu un algoritm puternic și codul „salt”[26] nu a fost compromis.
Date afectate: parole hashed ale 1.200 utilizatorii.
Din motive de siguranță, operatorul a informat persoanele vizate despre breșa, prin e-mail și le-a cerut să-și schimbe parolele, mai ales dacă aceeași parolă a fost folosită și pentru alte servicii.

[24] Pentru îndrumări cu privire la operațiunile de prelucrare „probabil să aibă ca rezultat un risc ridicat”, a se vedea nota de subsol 10 de mai sus.
[25] Când o parolă a fost „hashed”, înseamnă că a fost transformată într-o reprezentare amestecată a ei însăși. Este preluată parola unui utilizator și – folosind o cheie cunoscută site-ului – valoarea hash este derivată din combinația atât a parolei, cât și a cheii, folosind un algoritm special - *n. trad*.
[26] Codul „salt” reprezintă un șir aleator de caractere adăugat suplimentar de un algoritm, unei parole, înainte ca aceasta să fie codată hash și salvată în baza de date - *n. trad*.

3.2.1 CAZ NR. 06 - Măsuri prealabile și evaluarea riscurilor

56. În acest caz particular, confidențialitatea datelor este compromisă, dar parolele din baza de date au fost codate cu o metodă actualizată, care ar scădea riscul având în vedere natura, sensibilitatea și volumul de date personale. Acest caz nu prezintă niciun risc pentru drepturile și libertățile persoanelor vizate.

57. În plus, nu au fost compromise date de contact (de exemplu, adrese de e-mail sau numere de telefon) ale persoanelor vizate, ceea ce înseamnă că nu există un risc semnificativ pentru persoanele vizate de a deveni ținta unor încercări de fraudă (de exemplu, primirea de e-mailuri de tip phishing sau mesaje text și apeluri telefonice frauduloase). Nu au fost implicate categorii speciale de date personale.

58. Unele nume de utilizator pot fi considerate date personale, dar subiectul site-ului web nu permite atribuirea de conotații negative. Deși trebuie menționat că evaluarea riscului se poate modifica[27], dacă tipul de site web și datele accesate ar putea dezvălui categorii speciale de date cu caracter personal (de exemplu, site-ul web al unei persoane politice, partid sau sindicat). Utilizarea criptării de ultimă generație ar putea atenua efectele adverse ale breșei. Asigurarea faptului că este permis un număr limitat de încercări de autentificare va preveni atacurile de succes de conectare în 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. Comunicarea către persoanele vizate ar putea fi considerată, în unele cazuri, un factor atenuant, deoarece persoanele vizate sunt, de asemenea, în măsură să facă demersurile necesare pentru a evita daune ulterioare rezultate din breșă, de exemplu prin schimbarea parolei. În acest caz, notificarea nu era obligatorie, dar, în multe cazuri, poate fi considerată o bună practică.

60. Operatorul ar trebui să elimine vulnerabilitatea și să implementeze noi măsuri de securitate pentru a evita breșe similare în viitor, cum ar fi, de exemplu, audituri sistematice de securitate a site-ului web.

61. Breșa ar trebui să fie documentată în conformitate cu articolul 33 alineatul (5), dar fără să fie **necesară** notificarea AS sau a persoanelor vizate.

62. De asemenea, este foarte recomandabil să se comunice persoanelor vizate o breșă care implică parole, chiar și atunci când parolele au fost stocate fiind codate cu un cod hash de ultimă generație care a fost îmbogățit, în prealabil, cu un cod „salt”. Este de preferat să se utilizeze metode de autentificare care să evite necesitatea procesării parolelor din partea serverului. Persoanele vizate ar trebui să aibă posibilitatea de a alege să ia măsurile adecvate cu privire la propriile parole.

Acțiuni necesare pe baza riscurilor identificate		
Documentație internă	Notificare către AS	Comunicare către persoanele vizate
√	X	X

3.3 CAZ Nr. 07: Atacul de tip „Credential stuffing” pe un site bancar

O bancă a suferit un atac cibernetic de tip „Credential stuffing”[28] împotriva unuia dintre site-urile sale online. Atacul a urmărit rularea / încercarea tuturor ID-urilor de utilizator posibile folosind o parolă banală fixă. Parolele constau din 8 cifre.

Datorită unei vulnerabilități a site-ului web, în unele cazuri informații referitoare la persoanele vizate (nume, prenume, sex, data și locul nașterii, cod fiscal, coduri de identificare a utilizatorului) au devenit disponibile atacatorului, chiar dacă parola folosită nu era corectă sau contul bancar nu mai era activ.

[27] Pentru îndrumări cu privire la operațiunile de prelucrare „probabil să aibă ca rezultat un risc ridicat”, a se vedea nota de subsol 10 de mai sus.

[28] Credential Stuffing - este o metodă de atac cibernetic în care atacatorii folosesc liste de credențiale compromise ale utilizatorilor pentru a pătrunde într-un sistem. Atacul folosește roboți pentru automatizare și scalare și se bazează pe presupunerea că mulți utilizatori reutilizează numele de utilizator și parolele în mai multe servicii - *n. trad.*

Acest lucru a afectat aproximativ 100.000 de persoane vizate. Dintre acestea, atacatorul s-a conectat cu succes pe aproximativ 2.000 de conturi care foloseau parola banală încercată de acesta.
După atac, operatorul a fost capabil să identifice toate încercările nelegitime de conectare. Operatorul a putut confirmă că, în urma verificărilor antifraudă, nu au fost efectuate tranzacții pe conturi în timpul atacului.
Banca era conștientă de breșă, deoarece centrul său de operațiuni de securitate a detectat un număr mare de solicitări de conectare direcționate către site-ul web. Ca răspuns, operatorul a dezactivat posibilitatea autentificare pe site, prin dezactivarea acestuia și a forțat resetarea parolei conturilor compromise.
Operatorul a comunicat breșă numai utilizatorilor cu conturi compromise, adică utilizatorilor ale căror parole au fost compromise sau ale căror date au fost dezvăluite.

3.3.1 CAZ NR. 07 - Măsuri prealabile și evaluarea riscurilor

63. Este important de menționat că operatorii care prelucrează date de natură foarte personală[29] au responsabilitate mult mai mare în ceea ce privește asigurarea securității adecvate a datelor, de ex. deținând / folosind un centru de operațiuni de securitate și altele măsuri de prevenire, detectare și răspuns la incidente. Nerespectarea acestor standarde mai înalte va duce, cu siguranță, la măsuri mai serioase în timpul anchetei unei AS.
64. Breșa se referă la date financiare, dincolo de informațiile privind identitatea și ID-ul utilizatorului, ceea ce o face deosebit de gravă. Numărul persoanelor afectate este mare.
65. Faptul că o încălcare ar putea avea loc într-un mediu atât de sensibil indică lacune semnificative de securitate a datelor în sistemul operatorului și poate fi un indicator al unui moment în care revizuirea și actualizarea măsurilor de securitate este „necesară", în conformitate cu articolele 24 alineatul (1), 25 alineatul (1) și 32 alineatul (1) din GDPR. Datele afectate permit identificarea unică a persoanelor vizate și conțin alte informații despre acestea (inclusiv sex, data și locul nașterii) și, în plus, pot fi folosite de atacator pentru a ghici parolele clienților sau pentru a rula o campanie de „spear phishing" îndreptată către clienții băncii.
66. Din aceste motive, s-a considerat că breșa ar putea avea ca rezultat un risc ridicat pentru drepturile și libertățile tuturor persoanelor vizate în cauză[30]. Prin urmare, apariția daunelor materiale (de exemplu, pierderi financiare) și nemateriale (de exemplu, furtul de identitate sau frauda) este un rezultat credibil.

3.3.2 CAZUL Nr. 07 - Atenuare și obligații

67. Măsurile operatorului menționate în descrierea cazului sunt adecvate. În urma breșei a corectat, de asemenea, vulnerabilitatea site-ului web și a făcut alți pași pentru a preveni viitoare breșe similare, cum ar fi adăugarea de autentificare cu doi factori pe site-ul respectiv și trecerea la un sistem mai puternic de autentificare a clienților.
68. Documentarea breșei conform articolului 33 alineatul (5) GDPR și notificarea AS despre 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 GDPR.

Acțiuni necesare pe baza riscurilor identificate		
Documentație internă	Notificare către AS	Comunicare către persoanele vizate
√	√	√

[29] Cum ar fi informațiile persoanelor vizate referitoare la metode de plată, numere de card, conturi bancare, plată online, state de plată, extrase bancare, studii economice sau orice alte informații care ar putea dezvălui informații economice referitoare la persoanele vizate.
[30] Pentru îndrumări cu privire la operațiunile de prelucrare „probabil să aibă ca rezultat un risc ridicat", a se vedea nota de subsol 10 de mai sus.

3.4 Măsuri tehnice și organizatorice pentru prevenirea/atenuarea impactului atacurilor hackerilor

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

70. **Măsuri recomandabile**[31]:

(*Lista următoarelor măsuri nu este deloc exclusivă sau cuprinzătoare. Mai degrabă, scopul este de a oferi idei de prevenire și posibile soluții. Fiecare activitate de prelucrare este diferită, deci operatorul ar trebui să ia decizia asupra măsurilor care se potrivesc cel mai mult cu situația dată.*)

- Criptare de ultimă generație și gestionare a cheilor, în special atunci când sunt procesate parole, date sensibile sau financiare. Utilizarea de hashing criptografic și cod „salt" pentru informații secrete (parole) este întotdeauna preferabilă față de criptarea parolelor. Este de preferat utilizarea metodelor de autentificare evitând necesitatea de procesare a parolelor pe server.
- Menținerea la zi a sistemului (software și firmware). Asigurarea că toate măsurile de securitate IT sunt în vigoare, asigurându-se că sunt eficiente și menținându-le actualizate în mod regulat în timpul procesării sau dacă circumstanțele se schimbă sau evoluează. Pentru a putea demonstra conformitatea cu articolul 5 alineatul (1) litera (f) și în conformitate cu articolul 5 alineatul (2) GDPR, operatorul trebuie să păstreze o evidență a tuturor actualizărilor efectuate, incluzând și momentul în care au fost aplicate.
- Utilizarea unor metode puternice de autentificare, cum ar fi autentificarea cu doi factori și autentificarea serverelor, completată de o politică actualizată privind parolele.
- Standardele de dezvoltare sigură includ filtrarea intrărilor utilizatorilor (folosind „lista albă" [32], în măsura în care este posibil), evitarea intrărilor utilizatorilor și a măsurilor de prevenire a forței brute (cum ar fi limitarea cantității maxime de reîncercări). „Web Application Firewalls" poate ajuta la utilizarea eficientă a acestei tehnici.
- Privilegii puternice ale utilizatorului și politici de gestionare a controlului accesului.
- Utilizarea unui firewall adecvat, actualizat, eficient și integrat, detecția intruziunilor și a altor sisteme de apărare a perimetrelor.
- Audituri sistematice de securitate IT și evaluări ale vulnerabilităților (testare de penetrare).
- Evaluări și teste regulate pentru a se asigura că backup-urile pot fi folosite pentru a restaura orice date a căror integritate sau disponibilitatea a fost afectată.
- Niciun ID de sesiune în URL în text simplu.

4 SURSA INTERNĂ DE RISC UMAN

71. Trebuie subliniat rolul erorii umane în breșele datelor cu caracter personal, datorită aspectului lor comun. Deoarece aceste tipuri de breșe pot fi atât intenționate, cât și neintenționate, este foarte greu pentru operatori să identifice vulnerabilitățile și să adopte măsuri pentru evitarea acestora. Conferința Internațională a Comisarilor pentru Protecția și Confidențialitatea Datelor a recunoscut importanța abordării acestor factori umani și a adoptat rezoluția pentru a aborda rolul erorii umane în încălcările datelor cu caracter personal în octombrie 2019[33]. Rezoluția subliniază că ar trebui luate măsuri de salvgardare adecvate pentru a preveni erorile umane și oferă o listă neexhaustivă a unor astfel de garanții și abordări.

4.1 CAZ Nr. 08: Exfiltrarea datelor de afaceri de către un angajat

În perioada de preaviz, angajatul unei companii copiază datele de afaceri ale companiei din baza de date a acesteia. Angajatul este autorizat să acceseze datele numai pentru îndeplinirea sarcinilor sale de serviciu.

[31] Pentru dezvoltarea securizată a aplicațiilor web, consultați și: https://www.owasp.org/index.php/Main_Page .

[32] O „listă albă" este un mecanism care permite în mod explicit unor entități identificate să acceseze un anumit privilegiu, serviciu, mobilitate sau recunoaștere, adică este o listă de acțiuni permise atunci când totul este refuzat implicit - *n. trad.*

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

Câteva luni mai târziu, după ce a renunțat la locul de muncă, el folosește datele astfel obținute (date de contact de bază) pentru o noua prelucrare a acestor date, pentru care este operator, pentru a contacta clienții societății pentru a-i atrage în noua lui afacere.

4.1.1 CAZ NR. 08 - Măsuri prealabile și evaluarea riscurilor

72. În acest caz particular, nu au fost luate măsuri prealabile pentru a împiedica angajatul să copieze informațiile de contact ale clientelei companiei, întrucât avea nevoie – și avea – acces legitim la aceste informații pentru îndeplinirea sarcinilor sale de serviciu. Deoarece îndeplinirea mai multor activități în relația cu clienții necesită un anumit fel de acces al angajatului la date personale, aceste încălcări ale datelor pot fi cel mai dificil de prevenit. Limitările sferei de acces se pot rezuma la munca pe care angajatul respectiv este capabil să o facă. Cu toate acestea, politici de acces bine gândite și control constant pot ajuta la prevenirea unor astfel de încălcări.

73. Ca de obicei, în timpul evaluării riscurilor, tipul breșei și natura, sensibilitatea și volumul datelor personale afectate trebuie luate în considerare. Aceste tipuri de breșe sunt, de obicei, încălcări ale confidențialității, deoarece baza de date este, de obicei, lăsată intactă, „doar" conținutul ei fiind copiat pentru utilizare ulterioară. Cantitatea de date afectată este de obicei scăzută sau medie. În acest caz particular nu există categorii speciale de datele personale care au fost afectate, angajatul avea nevoie doar de informațiile de contact ale clienților pentru a-i permite să ia legătura cu ei după părăsirea companiei. Prin urmare, datele în cauză nu sunt sensibile.

74. Deși singurul obiectiv al fostului angajat care a copiat cu răutate datele poate fi limitat la obținerea informațiilor de contact ale clientelei companiei în scopuri comerciale proprii, operatorul nu se află în poziția de a considera că riscul pentru persoanele vizate este scăzut, deoarece operatorul nu are niciun fel de reasigurare asupra intențiilor angajatului. Astfel, în timp ce consecințele încălcării ar putea fi limitate la expunerea la marketing nedorit a fostului angajat, abuzuri și mai grave ale datelor furate nu sunt excluse, în funcție de scopul prelucrării pus în aplicare de fostul angajat[34].

4.1.2 CAZUL Nr. 08 – Atenuare și obligații

75. Atenuarea efectelor negative ale breșei în cazul de mai sus este dificilă. S-ar putea să fie nevoie să implice acțiuni imediate în justiție pentru a împiedica fostul angajat să abuzeze și să difuzeze în continuare datele. Ca pas următor, scopul ar trebui să fie evitarea unor situații viitoare similare. Operatorul ar putea încerca să comande / solicite fostului angajat să nu mai folosească datele, dar succesul acestei acțiuni este, în cel mai bun caz, dubios. Măsuri tehnice adecvate, precum imposibilitatea copierii sau descărcării datelor pe dispozitive amovibile pot ajuta.

76. Nu există o soluție „unică pentru toate" pentru acest tip de cazuri, dar o abordare sistematică poate ajuta la prevenirea lor. De exemplu, compania poate lua în considerare – atunci când este posibil – retragerea anumitor forme de acces de la angajații care și-au semnalat intenția de a renunța (*la locul de muncă - n. trad.*) sau de a implementa jurnale de acces astfel încât accesul nedorit să poată fi înregistrat și marcat. Contractul semnat cu angajații ar trebui să includă clauze care să interzică aceste acțiuni.

77. În general, întrucât breșa nu va avea ca rezultat un risc ridicat pentru drepturile și libertățile persoanelor fizice, notificarea către AS va fi suficientă. Cu toate acestea, informarea persoanelor vizate ar putea fi, de asemenea, benefică pentru operator, deoarece ar putea fi mai bine să audă de la companie despre scurgerea de date, mai degrabă decât de la fostul angajat care încearcă să-i contacteze. Documentația privind breșa, în conformitate cu articolul 33 alineatul (5), este o obligație legală.

[34] Pentru îndrumări cu privire la operațiunile de prelucrare „probabil să aibă ca rezultat un risc ridicat", a se vedea nota de subsol 10 de mai sus.

Acțiuni necesare pe baza riscurilor identificate		
Documentație internă	Notificare către AS	Comunicare către persoanele vizate
√	√	X

4.2 CAZ Nr. 09: Transmiterea accidentală a datelor către o terță parte de încredere

Un agent de asigurări a observat că – posibil datorită setărilor defectuoase ale unui fișier Excel primit prin e-mail – a putut accesa informații legate de două duzini de clienți care nu aparțin domeniul său de activitate.
El este obligat să respecte secretul profesional și a fost singurul destinatar al e-mailului. Acordul dintre operator și agentul de asigurări obligă agentul să semnaleze breșa către operator, fără întârzieri nejustificate. Prin urmare, agentul a semnalat instantaneu greșeala operatorului, care a corectat dosarul și l-a trimis din nou, solicitând agentului ștergerea mesajului anterior. Conform acordului 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, numai date de contact și date despre asigurare în sine (tip de asigurare, cantitate).
După analizarea datelor cu caracter personal afectate de breșă, operatorul nu a identificat nicio caracteristică specială a persoanelor fizice sau a operatorului care ar putea afecta nivelul de impact al breșei.

4.2.1 CAZ Nr. 09 – Măsuri prealabile și evaluarea riscurilor

78. Breșa nu derivă, aici, dintr-o acțiune intenționată a unui angajat, ci dintr-o eroare umană, cauzată de neatenție. Aceste tipuri de breșe pot fi evitate sau reduse ca frecvență prin:
   a) aplicarea programelor de formare, educație și conștientizare în care angajații obțin o mai bună înțelegere a importanța protecției datelor cu caracter personal
   b) reducerea schimbului de fișiere prin e-mail, în schimb utilizarea dedicată sisteme de prelucrare a datelor clienților, de exemplu
   c) dubla verificare a fișierelor înainte de trimitere
   d) separarea crearea și trimiterea fișierelor.

79. Această breșă se referă doar la confidențialitatea datelor, prin urmare, integritatea și accesibilitatea acestora sunt lăsate intacte. Breșa a vizat doar două duzini de clienți, de unde și cantitatea de date afectate poate fi considerată ca fiind scăzută. În plus, datele personale afectate nu conțin niciun fel de date sensibilitate. Faptul că persoana împuternicită de operator a contactat imediat operatorul după ce a luat la cunoștință despre breșă poate fi considerată un factor de atenuare a riscului. (Posibilitatea ca datele să fi fost trimise altor agenți de asigurare ar trebui, de asemenea, evaluată și, dacă se confirmă, ar trebui luate măsuri adecvate.) Datorită măsurilor adecvate luate după breșă, probabil că nu va avea niciun impact asupra drepturilor și libertăților persoanelor vizate.

80. Combinația dintre numărul redus de persoane afectate, detectarea imediată a breșei și măsurile luate pentru ca efectele sale să fie reduse la minimum fac ca acest caz particular să nu aibă niciun risc.

4.2.2 CAZUL Nr. 09 – Atenuare și obligații

81. Mai mult, sunt în joc și alte circumstanțe de atenuare a riscului: agentul este obligat să respecte secretul profesional, el însuși a raportat problema operatorului și a șters fișierul la cerere. Creșterea gradului de conștientizare și, eventual, includerea unor pași suplimentari în verificarea documentelor care implică date cu caracter personal va ajuta, probabil, la evitarea cazurilor similare pe viitor.

82. Pe lângă documentarea încălcării în conformitate cu articolul 33 alineatul (5), nu este necesară nicio altă acțiune.

Acțiuni necesare pe baza riscurilor identificate		
Documentație internă	Notificare către AS	Comunicare către persoanele vizate
√	X	X

4.3 Măsuri tehnice și organizatorice pentru prevenirea/atenuarea impactului surselor interne de risc de natură umană

83. O combinație a măsurilor menționate mai jos – aplicate în funcție de caracteristicile unice ale cazului – ar trebui să contribuie la reducerea șanselor ca o încălcare similară să se repete.

84. **Măsuri recomandate**:

(*Lista următoarelor măsuri nu este deloc exclusivă sau cuprinzătoare. Mai degrabă, scopul este de a oferi idei de prevenire și posibile soluții. Fiecare activitate de prelucrare este diferită, deci operatorul ar trebui să ia decizia asupra măsurilor care se potrivesc cel mai mult cu situația dată.*)

- Implementarea periodică a programelor de instruire, educare și conștientizare a angajaților cu privire la obligațiile acestora privind confidențialitatea și securitatea datelor personale și de detectare și raportare a amenințărilor la adresa securității datelor cu caracter personal[35]. Dezvoltați un program de conștientizare pentru a reaminti angajaților cele mai comune erori care duc breșe ale datelor personale și cum să le evitați.
- Stabilirea unor practici, proceduri și sisteme solide și eficiente de confidențialitate și protecție a datelor[36].
- Evaluarea practicilor, procedurilor și sistemelor de confidențialitate pentru a asigura eficacitatea continuă[37].
- Elaborarea unor politici adecvate de control al accesului și forțarea utilizatorilor să respecte regulile.
- Implementarea tehnicilor pentru a forța autentificarea utilizatorului la accesarea datelor personale sensibile.
- Dezactivarea contului utilizatorului asociat companiei, de îndată ce persoana părăsește compania.
- 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 interfeței pentru computer (blocare sau deblocare, de exemplu, USB/CD/DVD etc.).
- Revizuirea politicii de acces a angajaților (de exemplu, înregistrarea accesului la date sensibile și solicitarea utilizatorului să introducă un motiv de afaceri, astfel încât acesta să fie disponibil pentru audituri).
- Dezactivarea serviciilor cloud deschise.
- Interzicerea și împiedicarea accesului la serviciile deschise de poștă cunoscute.
- Dezactivarea funcției „print screen” în sistemul de operare.
- Aplicarea unei politici de birou curat.
- Blocarea automată a tuturor computerelor după un anumit interval de timp de inactivitate.
- Folosiți mecanisme (de exemplu, token (fără fir) pentru a vă conecta/a deschide conturi blocate) pentru comutarea rapidă a utilizatorilor în medii de lucru partajate.
- Utilizarea sistemelor dedicate de gestionare a datelor cu caracter personal care aplică mecanisme adecvate de control al accesului și care previn greșelile umane, cum ar fi trimiterea de comunicări către destinatarul greșit. Utilizarea foilor de calcul și a altor documente de birou nu reprezintă un mijloc adecvat de a gestiona datele clienților.

[35] Secțiunea 2) subsecțiunea (i) din Rezoluție pentru a aborda rolul erorii umane în încălcarea datelor cu caracter personal.
[36] Secțiunea 2) subsecțiunea (ii) din Rezoluție pentru a aborda rolul erorii umane în încălcarea datelor cu caracter personal.
[37] Secțiunea 2) subsecțiunea (iii) din Rezoluție pentru a aborda rolul erorii umane în încălcarea datelor cu caracter personal.

5 DISPOZITIVE ȘI DOCUMENTE PIERDUTE SAU FURATE

85. Un tip frecvent de caz este pierderea sau furtul dispozitivelor 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 resursele suport și măsurile luate înainte de breșă, pentru a asigura un nivel adecvat de securitate. Toate aceste elemente afectează impacturile potențiale ale breșei. Evaluarea riscului ar putea fi dificilă, deoarece dispozitivul nu mai este disponibil.

86. Aceste tipuri de breșe pot fi întotdeauna clasificate drept încălcări ale confidențialității. Cu toate acestea, dacă nu există backup pentru baza de date furată, atunci tipul de breșă poate fi, de asemenea, breșă de disponibilitate și breșă de integritate.

87. Scenariile de mai jos demonstrează modul în care circumstanțele menționate mai sus influențează probabilitatea și gravitatea breșelor.

5.1 CAZUL Nr. 10: Material furat care stochează date personale criptate

În timpul unei spargeri într-un centru de zi pentru copii, două tablete au fost furate. Tabletele conțineau o aplicație cu care se prelucrau datele personale ale copiilor care frecventează centrul de zi. Au fost vizate nume, data nașterii și date personale despre educația copiilor. Ambele tablete erau criptate și oprite în momentul spargerii, iar aplicația a fost protejată cu o parolă puternică. Datele de rezervă au fost disponibile operatorului în mod eficient și ușor. După ce a devenit conștientă de spargere, grădinița a emis de la distanță o comandă de ștergere a tabletelor la scurt timp după descoperirea spargerii.

5.1.1 CAZUL Nr. 10 - Măsuri prealabile și evaluarea riscurilor

88. În acest caz particular, operatorul a luat măsuri adecvate pentru a preveni și a atenua impactul potențial al breșei, prin utilizarea criptării dispozitivului, introducerea unei protecții printr-o parolă adecvată și prin securizarea unei copii de rezervă a datelor stocate pe tablete. (O listă a măsurilor recomandate se găsește în secțiunea 5.7).

89. După ce a luat la cunoștință despre breșă, operatorul ar trebui să evalueze sursa de risc, sistemele care suportă prelucrarea datelor, tipul de date cu caracter personal implicate și impacturile potențiale ale breșei asupra indivizii în cauză. Breșa descrisă mai sus ar fi vizat confidențialitatea, disponibilitatea și integritatea datelor în cauză, totuși, datorită procedurilor adecvate ale operatorului, prealabile și ulterioare breșei, nu a avut loc niciuna dintre acestea.

5.1.2 CAZUL Nr. 10 – Atenuare și obligații

90. Confidențialitatea datelor personale de pe dispozitive nu a fost compromisă datorită parolei puternice de protecție, atât pe tablete, cât și pe aplicații. Tabletele au fost configurate în așa fel încât să se stabilească o parolă, ceea ce înseamnă, de asemenea, că datele de pe dispozitiv sunt criptate. Acest lucru a fost îmbunătățit și mai mult de acțiunea operatorului care a încercat să șteargă totul de pe dispozitivele furate, de la distanță.

91. Datorită măsurilor luate confidențialitatea datelor a fost și ea păstrată intactă. În plus, backup-ul a asigurat disponibilitatea continuă a datelor cu caracter personal, deci nu ar putea avea un impact negativ potențial.

92. Datorită acestor fapte, este puțin probabil ca breșa descrisă mai sus să aibă ca rezultat un risc pentru drepturile și libertățile persoanelor vizate, prin urmare nu a fost necesară nicio notificare către AS sau persoanele vizate. În orice caz, această breșă trebuie, de asemenea, să fie documentată în conformitate cu articolul 33 alineatul (5).

Acțiuni necesare pe baza riscurilor identificate		
Documentație internă	Notificare către AS	Comunicare către persoanele vizate
√	X	X

5.2 CAZUL Nr. 11: Material furat care stochează date personale necriptate

Dispozitivul notebook electronic al unui angajat al unei companii prestatoare de servicii a fost furat. Dispozitivul furat conținea nume, prenume, sex, adrese și data nașterii a mai mult de 100.000 de clienți. Din cauza indisponibilității dispozitivului furat nu s-a putut identifica dacă au fost afectate și alte categorii de date cu caracter personal. Accesul la hard disk-ul notebook-ului nu a fost protejat de nicio parolă. Datele personale pot fi restaurate din backup-urile zilnice disponibile.

5.2.1 CAZUL Nr. 11 - Măsuri prealabile și evaluarea riscurilor

93. Nu au fost luate în prealabil măsuri de siguranță de către operator, prin urmare, datele personale stocate pe dispozitivul furat sunt ușor accesibile pentru hoț sau pentru orice altă persoană care intră în posesia dispozitivului după aceea.

94. Această breșă se referă la confidențialitatea datelor stocate pe dispozitivul furat.

95. Dispozitivul în speță era vulnerabil deoarece nu deținea nicio protecție prin parolă sau criptare. Lipsa măsurilor de securitate de bază sporește nivelul de risc pentru persoanele vizate. În plus, identificarea persoanelor vizate în cauză este, de asemenea, problematică, ceea ce mărește și severitatea încălcării. Numărul considerabil de indivizi afectați crește riscul, dar, cu toate acestea, în breșă nu au fost vizate categorii speciale de date cu caracter personal.

96. În timpul evaluării riscurilor[38], operatorul ar trebui să ia în considerare consecințele potențiale și efectele negative ale încălcării confidențialității. Ca urmare a breșei, persoanele vizate pot suferi fraudă de identitate bazându-se pe datele disponibile pe dispozitivul furat, astfel încât riscul este considerat a fi mare.

5.2.2 CAZUL Nr. 11 – Atenuare și obligații

97. Activarea criptării dispozitivului și utilizarea unei protecții puternice cu parolă a bazei de date stocate ar putea împiedica breșa să aibă ca rezultat un risc pentru drepturile și libertățile persoanelor vizate.

98. Din aceste circumstanțe reiese că este necesară notificarea AS, iar notificarea persoanelor vizate este, de asemenea, necesară.

Acțiuni necesare pe baza riscurilor identificate		
Documentație internă	Notificare către AS	Comunicare către persoanele vizate
√	√	√

5.3 CAZ NR. 12: Documente pe hârtie, cu date sensibile, furate

Un registru pe hârtie a fost furat dintr-o unitate de dezintoxicare pentru dependența de droguri. Registrul conținea datele de identitate de bază și datele de sănătate ale pacienților internați în unitatea de dezintoxicare. Datele au fost stocate doar pe hârtie și medicii care tratează pacienții nu au avut la dispoziție date de rezervă. Registrul nu a fost depozitat într-un sertar încuiat sau o cameră, operatorul nu avea nici regim de control al accesului, nici altă măsură de salvgardare pentru documentația pe hârtie.

5.3.1 CAZUL Nr. 12 – Măsuri prealabile și evaluarea riscurilor

99. Nu au fost luate măsuri prealabile de siguranță de către operator, prin urmare datele personale stocate în acest registru au fost ușor accesibile pentru persoana care l-a găsit. Mai

[38] Pentru îndrumări cu privire la operațiunile de prelucrare „probabil să aibă ca rezultat un risc ridicat”, a se vedea nota de subsol 10 de mai sus.

mult, natura datelor personale stocate în registru face din lipsa datelor de rezervă un factor de risc foarte serios.

100. Acest caz servește ca exemplu pentru o breșă cu risc ridicat. Din cauza eșecului unor precauții de siguranță corespunzătoare, s-au pierdut datele sensibile de sănătate în conformitate cu articolul 9 alineatul (1) GDPR. Întrucât în acest caz o categorie specială de date cu caracter personal a fost afectată, riscurile potențiale pentru persoanele vizate au fost crescute, ceea ce ar trebui luat în considerare și de către operatorul care evaluează riscul[39].

101. Această breșă se referă la confidențialitatea, disponibilitatea și integritatea datelor cu caracter personal în cauză. Ca rezultat al breșei, secretul medical este încălcat și terți neautorizați pot avea acces la informațiile medicale private ale pacienților, ceea ce poate avea un impact grav asupra vieții personale a acestora. Breșa de disponibilitate poate perturba, de asemenea, continuitatea tratamentului pacienților. Deoarece modificarea/ștergerea unor părți din conținutul registrului nu poate fi exclusă, integritatea datelor cu caracter personal este, de asemenea, compromisă.

5.3.2 CAZUL Nr. 12 – Atenuare și obligații

102. În timpul evaluării măsurilor de salvgardare ar trebui să se ia în considerare, de asemenea, tipul de suport al datelor personale. Întrucât registrul pacienților era un document fizic, ar fi trebuit să se organizeze protecția acestuia diferit de cea a unui dispozitiv electronic. Pseudonimizarea numelor pacienților, păstrarea registrului într-o locație protejată și într-un sertar încuiat sau într-o cameră cu control adecvat al accesului, cu autentificarea la accesarea acestuia ar fi putut preveni breșa.

103. Breșa descrisă mai sus poate afecta grav persoanele vizate, de aici notificarea AS și comunicarea breșei către persoanele vizate este obligatorie.

Acțiuni necesare pe baza riscurilor identificate		
Documentație internă	Notificare către AS	Comunicare către persoanele vizate
√	√	√

5.4 Măsuri tehnice și organizatorice pentru prevenirea/atenuarea impactului pierderii sau furtului dispozitivelor

104. O combinație a măsurilor menționate mai jos – aplicate în funcție de caracteristicile unice ale cauzei – ar trebui să contribuie la reducerea șanselor ca o încălcare similară să se repete.

105. **Măsuri recomandate**:

(*Lista următoarelor măsuri nu este deloc exclusivă sau cuprinzătoare. Mai degrabă, scopul este de a oferi idei de prevenire și posibile soluții. Fiecare activitate de prelucrare este diferită, deci operatorul ar trebui să ia decizia asupra măsurilor care se potrivesc cel mai mult cu situația dată.*)

- Activați criptarea dispozitivului (cum ar fi Bitlocker, Veracrypt sau DM-Crypt).
- Utilizați coduri de acces/parole pe toate dispozitivele. Criptați toate dispozitivele electronice mobile într-un mod care necesită introducerea unei parole complexe pentru decriptare.
- Utilizați autentificarea cu mai mulți factori.
- Activați funcționalitățile dispozitivelor foarte mobile care permit localizarea acestora în caz de pierdere sau plasare greșită / uitare a locului unde au fost stocate. Utilizați software-ul /

[39] Pentru îndrumări cu privire la operațiunile de prelucrare „probabil să aibă ca rezultat un risc ridicat”, a se vedea nota de subsol 10 de mai sus.

aplicația MDM (Mobile Devices Management) și activați funcția de localizare. Folosiți filtre anti-orbire[40]. Închideți orice dispozitive nesupravegheate.

- Dacă este posibil și adecvat pentru prelucrarea datelor în cauză, salvați datele personale nu pe un dispozitiv mobil, ci pe un server central de back-end.
- Dacă stația de lucru este conectată la rețeaua LAN corporativă, faceți o copie de rezervă automată din folderele de lucru, dacă este inevitabil ca datele personale să fie stocate acolo.
- Utilizați un VPN securizat (de exemplu, care necesită o cheie de autentificare separată în doi factori pentru realizarea unei conexiuni securizate) pentru a conecta dispozitive mobile la servere back-end.
- Furnizați încuietori fizice angajaților pentru a le permite să securizeze fizic dispozitivele mobile pe care le folosesc în timp ce acestea rămân nesupravegheate.
- Reglementarea corectă a utilizării dispozitivului în afara companiei.
- Reglementarea corectă a utilizării dispozitivelor în cadrul companiei.
- Utilizați software-ul/aplicația MDM (Mobile Devices Management) și activați funcția de ștergere de la distanță.
- Utilizați gestionarea centralizată a dispozitivelor, cu drepturi minime pentru utilizatorii finali de a instala software.
- Instalați controale fizice de acces.
- Evitați stocarea informațiilor sensibile pe dispozitive mobile sau hard disk. Dacă este nevoie să accesați sistemul intern al companiei, ar trebui utilizate canale securizate, așa cum s-a menționat anterior.

6 EXPEDIERI GREȘITE

106. Sursa de risc este o eroare umană internă și în acest caz, dar aici nicio acțiune rău intenționată nu a condus la Breșă. Este rezultatul neatenției. Puține pot fi întreprinse de operator după ce s-a întâmplat, deci prevenirea este chiar mai importantă în aceste cazuri decât în alte tipuri de breșe.

6.1 CAZ Nr. 13: Greșeală poștală

Două comenzi de pantofi au fost ambalate de o companie de vânzare cu amănuntul. Din cauza unei erori umane au fost amestecat două facturi de ambalare, rezultatul fiind că ambele produse și facturile de ambalare relevante au fost trimise persoanei greșite. Aceasta înseamnă că cei doi clienți și-au primit comenzile reciproc, inclusiv facturile de ambalare care conțin datele personale. După ce a luat la cunoștință de breșă, operatorul a rechemat comenzile și le-a trimis destinatarilor potriviți.

6.1.1 CAZUL Nr. 13 - Măsuri prealabile și evaluarea riscurilor

107. Facturile conțineau datele personale necesare pentru livrare (nume, adresă, plus articolul cumpărat și prețul acestuia). Este important, în primul rând, să identificăm cum s-ar fi putut produce eroarea umană și, dacă ar fi putut fi prevenită în vreun fel. În cazul specific, riscul este scăzut, deoarece nu au fost implicate categorii speciale de date cu caracter personal sau alte date al căror abuz ar putea duce la efecte negative substanțiale, breșa nu este rezultatul unei erori sistemice din partea operatorului și doar două persoane sunt afectate. Nu a putut fi identificat niciun efect negativ asupra indivizilor.

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 greșiți să distrugă/șteargă toate eventualele copii ale facturilor care conțin datele personale ale celeilalte persoane.

[40] Filtrele anti-orbire sunt folosite pentru a preveni strălucirea pe ecrane. Aceste filtre sunt deosebit de utile atunci când un computer sau un ecran de televizor se află în imediata apropiere a unei ferestre. Filtrele anti-orbire sunt cunoscute și ca filtre de strălucire, filtre de confidențialitate și ecrane de confidențialitate - *n. trad.*

109. Chiar dacă breșa în sine nu prezintă un risc ridicat pentru drepturile și libertățile persoanelor afectate și, prin urmare, comunicarea către persoanele vizate nu este impusă de articolul 34 GDPR, comunicarea breșei către acestea nu poate fi evitată, deoarece cooperarea lor este necesară pentru a atenua riscul.

Acțiuni necesare pe baza riscurilor identificate		
Documentație internă	Notificare către AS	Comunicare către persoanele vizate
√	X	X

6.2 CAZUL Nr. 14: Date personale extrem de confidențiale trimise prin poștă din greșeală

Direcția de angajare a unui birou al unei administrații publice a trimis un mesaj prin e-mail – despre cursuri viitoare - persoanelor înscrise în sistemul său ca persoane aflate în căutarea unui loc de muncă. Din greșeală, un document care conține toate aceste date personale ale persoanelor aflate în căutarea unui loc de muncă (nume, adresă de e-mail, adresă poștală, numărul unic de identificare personală) a fost atașat la acest e-mail.
Numărul persoanelor afectate este mai mare de 60.000. Ulterior, biroul a luat contactat cu toți destinatarii și le-a cerut să șteargă mesajul anterior și să nu utilizeze informațiile conținute în acesta.

6.2.1 CAZ NR. 14 - Măsuri prealabile și evaluarea riscurilor

110. Ar fi trebuit implementate reguli mai stricte pentru trimiterea unor astfel de mesaje. Introducerea unor mecanisme de control suplimentare trebuie luată în considerare.
111. Numărul persoanelor afectate este considerabil, precum și implicarea numărului lor unic de identificare personală cu alte date personale, mai elementare, crește și mai mult riscul, care poate fi identificat ca fiind ridicat[41]. Eventuala distribuire a datelor de către oricare dintre destinatari nu poate fi împiedicată de operator.

6.2.2 CAZUL Nr. 14 – Atenuare și obligații

112. După cum s-a menționat anterior, mijloacele de atenuare efectivă a riscurilor unei breșe similare sunt limitate. Deși operatorul a cerut ștergerea mesajului, nu poate forța destinatarii să facă acest lucru, și ca o consecință, nici nu poate fi sigur că aceștia se conformează cererii.
113. Executarea tuturor celor trei acțiuni indicate mai jos ar trebui să fie evidentă într-un caz ca acesta.

Acțiuni necesare pe baza riscurilor identificate		
Documentație internă	Notificare către AS	Comunicare către persoanele vizate
√	√	√

6.3 CAZUL Nr. 15: Date personale trimise prin poștă din greșeală

O listă de participanți la un curs de engleză juridică care se desfășoară într-un hotel timp de 5 zile este din greșeală trimis la 15 foști participanți la curs, în loc să fie trimisă hotelului. Lista conține nume, e-mail adresele și preferințele alimentare ale celor 15 participanți. Doar doi participanți și-au completat preferințele alimentare, afirmând că sunt intoleranți la lactoză. Niciunul dintre participanți nu are identitatea protejată. Operatorul descoperă greșeala imediat după trimiterea listei și informează destinatarii greșelii și le cere să șteargă lista.

[41] Pentru îndrumări cu privire la operațiunile de prelucrare „probabil să aibă ca rezultat un risc ridicat", a se vedea nota de subsol 10 de mai sus.

6.3.1 CAZ NR. 15 - Măsuri prealabile și evaluarea riscurilor

114. Ar fi trebuit implementate reguli stricte pentru trimiterea de mesaje care conțin date cu caracter personal. Trebuie luată în considerare introducerea unor mecanisme de control suplimentare.

115. Riscurile care decurg din natura, sensibilitatea, volumul și contextul datelor cu caracter personal sunt reduse. Datele personale includ date sensibile despre preferințele alimentare a doi dintre participanți. Chiar dacă informația că cineva are intoleranță la lactoză reprezintă date de sănătate, riscul ca aceste date să fie utilizate într-un mod dăunător ar trebui considerat relativ scăzut. În timp ce în cazul datelor referitoare la sănătate este de obicei de presupus că breșa este susceptibilă de a genera un risc ridicat pentru persoana vizată[42], în același timp, în acest caz particular nu poate fi identificat niciun risc ca breșa să conducă la daune de natură fizică, materială sau nematerială pentru persoana vizată, din cauza dezvăluirii neautorizate a informațiilor despre intoleranța la lactoză. Contrar altor preferințe alimentare, intoleranța la lactoză nu poate fi, în mod normal, legată de vreo religie sau convingeri filozofice. Cantitatea datelor încălcate și numărul persoanelor vizate afectate este foarte scăzută de asemenea.

6.3.2 CAZUL Nr. 15 – Atenuare și obligații

116. Pe scurt, se poate afirma că breșa nu a avut un efect semnificativ asupra persoanelor vizate. Faptul că operatorul a contactat imediat destinatarii după ce a conștientizat greșeala poate fi considerată a factor atenuant.

117. Dacă un e-mail este trimis unui destinatar incorect/neautorizat, se recomandă ca operatorul să trimită un e-mail de urmărire cu destinatarii neintenționați în Bcc, în care își cere scuze, indicând că e-mailul greșit ar trebui să fie șters și avertizând destinatarii că nu au dreptul de a utiliza în continuare adresele de e-mail identificate ale acestora.

118. Datorită acestor fapte, este puțin probabil ca această încălcare a datelor să aibă ca rezultat un risc pentru drepturile și libertățile persoanelor vizate, prin urmare nu a fost necesară nicio notificare către AS sau persoanele vizate. Cu toate acestea, breșa trebuie, de asemenea, să fie documentată în conformitate cu articolul 33 alineatul (5).

Acțiuni necesare pe baza riscurilor identificate		
Documentație internă	Notificare către AS	Comunicare către persoanele vizate
√	X	X

6.4 CAZ Nr. 16: Greșeală poștală

Un grup de asigurări oferă asigurări auto. Pentru a face acest lucru, trimite în mod regulat, prin poștă, politici de contribuții ajustate. Pe lângă numele și adresa deținătorului poliței, scrisoarea conține numărul de înmatriculare al vehiculului fără cifre mascate, tarifele de asigurare ale actualului și următor an de asigurare, kilometrajul anual aproximativ și data nașterii asiguratului. Date de sănătate, conform articolului 9 GDPR, datele de plată (detalii bancare), datele economice și financiare nu sunt incluse.
Scrisorile sunt împachetate de mașini automate de ambalare. Din cauza unei erori mecanice, două scrisori pentru diferiți asigurați sunt introduse într-un singur plic și trimise prin poștă unui singur asigurat. Asiguratul deschide scrisoarea acasă și aruncă o privire și asupra scrisorii sale corect livrate, și la scrisoarea incorect livrată de la alt asigurat.

6.4.1 CAZUL Nr. 16 - Măsuri prealabile și evaluarea riscurilor

119. Scrisoarea incorect livrată conține numele, adresa, data nașterii, numărul de înmatriculare al vehiculului, nemascat și clasificarea ratei de asigurare a anului curent și a anului următor. Efectele asupra persoana afectate trebuie considerată de nivel mediu, deoarece informațiile care nu sunt disponibile publicului, cum ar fi data nașterii sau numerele de

[42] Vezi Ghidul WP 250, p. 23.

înmatriculare nemascate ale vehiculului, precum și detaliile despre creșterea ratelor de asigurare sunt dezvăluite destinatarului neautorizat. Probabilitatea de utilizare greșită a acestor date este evaluată a fi între mică și medie. Cu toate acestea, în timp ce mulți destinatari vor arunca, probabil, scrisoarea primită greșit la gunoi, în cazuri individuale nu se poate exclude complet ca scrisoarea să fie postată pe rețelele de socializare sau ca asiguratul să fie contactat.

6.4.2 CAZUL Nr. 16 – Atenuare și obligații

120. Operatorul trebuie să primească documentul original returnat pe cheltuiala sa. Destinatarul greșit ar trebui, de asemenea, să fie informat că nu poate folosi greșit informațiile citite.

121. Probabil că nu va fi niciodată posibil să se prevină complet o eroare de livrare poștală într-o corespondență în masă folosind complet mașini automatizate. Cu toate acestea, în cazul unei frecvențe crescute, este necesar să se verifice dacă mașinile de învelire sunt setate și întreținute suficient de corect sau dacă vreo altă problemă sistemică duce la această breșă.

Acțiuni necesare pe baza riscurilor identificate		
Documentație internă	Notificare către AS	Comunicare către persoanele vizate
√	√	X

6.5 Măsuri tehnice și organizatorice pentru prevenirea/atenuarea impactului trimiterilor poștale greșite

122. O combinație a măsurilor menționate mai jos - aplicate în funcție de caracteristicile unice ale cauzei - ar trebui să contribuie la reducerea șanselor ca o încălcare similară să se repete.

123. **Măsuri recomandate**:

(*Lista următoarelor măsuri nu este deloc exclusivă sau cuprinzătoare. Mai degrabă, scopul este de a oferi idei de prevenire și posibile soluții. Fiecare activitate de prelucrare este diferită, prin urmare operatorul ar trebui să-l facă luați decizia asupra măsurilor care se potrivesc cel mai mult cu situația dată.*)

- Stabilirea unor standarde exacte – fără loc de interpretare – pentru trimiterea de scrisori/e-mailuri.
- Instruire adecvată a personalului cu privire la modul de trimitere a scrisorilor/e-mail-urilor.
- Când trimiteți e-mailuri către mai mulți destinatari, aceștia trebuie listați în câmpul „BCC” în mod implicit.
- Este necesară o confirmare suplimentară atunci când trimiteți e-mailuri către mai mulți destinatari, iar aceștia nu sunt listați în câmpul „BCC”.
- Aplicarea principiului celor patru ochi[43].
- Adresarea automată, în loc de cea manuală, cu date extrase dintr-un document disponibil și dintr-o bază de date actualizată; sistemul de adresare automată ar trebui revizuit în mod regulat pentru a verifica dacă sunt ascunse erori și setări incorecte.
- Aplicarea întârzierii mesajului (de exemplu, mesajul poate fi șters/editat într-o anumită perioadă de timp după ce faceți clic pe butonul de trimitere).
- Dezactivarea completării automate la introducerea adreselor de e-mail.
- Sesiuni de conștientizare cu privire la cele mai frecvente greșeli care duc la o încălcare a datelor cu caracter personal.
- Sesiuni de instruire și manuale cu privire la modul de gestionare a incidentelor care duc la o încălcare a datelor cu caracter personal și pe cine să informeze (implică DPO).

[43]Regula „celor patru ochi” este un mecanism de control proiectat pentru a atinge un grad ridicat de siguranță, în special pentru documente și operațiuni sensibile. Acest principiu se bazează pe faptul că cel puțin două persoane verifică, independent una de cealaltă, același document / operațiune - *n. trad.*

7 ALTE CAZURI – INGINERIA SOCIALĂ

7.1 CAZUL Nr. 17: Furtul de identitate

Centrul de contact al unei companii de telecomunicații primește un apel telefonic de la cineva care se prezintă ca fiind client. Presupusul client cere companiei să schimbe adresa de e-mail la care informațiile de facturare ar trebui trimise de atunci înainte. Lucrătorul centrului de contact validează identitatea clientului prin solicitarea anumitor date personale, astfel cum sunt definite de procedurile din companie. Apelantul indică corect numărul fiscal și adresa poștală a clientului solicitat (deoarece avea acces la aceste elemente). După validare, operatorul efectuează modificarea solicitată și, din acel moment, informațiile de facturare sunt trimise la noua adresă de e-mail.
Procedura nu prevede nicio notificare către fosta adresă de e-mail. În luna următoare, clientul legitim contactează compania, întrebând de ce nu primește factura la adresa sa de e-mail și se respinge orice apel de la acesta prin care cere schimbarea adresei de e-mail. Mai târziu, compania își dă seama că informațiile au fost trimise unui utilizator nelegitim și anulează modificarea.

7.1.1 CAZUL Nr. 17 - Evaluarea riscurilor, atenuarea și obligații

124. Prezenta cauză servește drept exemplu privind importanța măsurilor prealabile. Breșa, prezintă un nivel ridicat de risc[44], deoarece datele de facturare pot oferi informații despre viața privată a persoanei vizate (de exemplu, obiceiuri, contacte) și ar putea duce la pagube materiale (de exemplu, urmărire, risc pentru integritatea fizică). Datele personale obținute în timpul acestui atac pot fi folosite și pentru a facilita preluarea contului în această organizație sau exploatarea unor măsuri suplimentare de autentificare în alte organizații. Având în vedere aceste riscuri, măsura de autentificare „adecvată" ar trebui să atingă un nivel ridicat, în funcție de ce date cu caracter personal pot fi prelucrate ca rezultat al autentificării.
125. În consecință, atât o notificare către AS, cât și o comunicare către persoana vizată sunt necesare din partea operatorului.
126. Procesul prealabil de validare a clientului trebuie să fie în mod clar îmbunătățit în lumina acestui caz. Metodele folosite pentru autentificare nu au fost suficiente. Partea rău intenționată a putut să pretindă că este utilizatorul vizat, prin utilizarea informațiilor disponibile public și a informațiilor la care avea acces în alt fel.
127. Utilizarea acestui tip de autentificare statică bazată pe cunoștințe (unde răspunsul nu se schimbă și unde informația nu este „secretă", cum ar fi cazul unei parole) nu este recomandată.
128. În schimb, organizația ar trebui să utilizeze o formă de autentificare care ar duce la un grad ridicat de încredere că utilizatorul autentificat este persoana vizată și nu altcineva. Introducerea unei metode „Out of Band Authentication"[45] ar rezolva problema, de ex. pentru a verifica cererea de schimbare, prin trimiterea unei cereri de confirmare către fostul contact; sau 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 funcționării sale interne.

Acțiuni necesare pe baza riscurilor identificate		
Documentație internă	Notificare către AS	Comunicare către persoanele vizate
√	√	√

[44] Pentru îndrumări cu privire la operațiunile de prelucrare „probabil să aibă ca rezultat un risc ridicat", a se vedea nota de subsol 10 de mai sus.
[45] Out of Band Authentication (OOBA) este un proces de autentificare care utilizează un canal de comunicații separat de canalul de comunicare principal a două entități care încearcă să stabilească o conexiune autentificată. Utilizarea unui canal de autentificare separat face mult mai dificil pentru un atacator să intercepteze și să submineze procesul de autentificare (adică prin intermediul unui atac de tip man-in-the-middle), deoarece îi cere atacatorului să compromită două canale de comunicații - *n. trad.*

7.2 CAZUL Nr. 18: Exfiltrarea e-mailului

Un lanț de hipermarketuri a detectat, la trei luni de la configurare, că niște 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", „autentificarea cardului de credit", „detaliile contului bancar") să fie mutate într-un folder neutilizat și, de asemenea, redirecționat către o adresă de e-mail externă. De asemenea, la acel moment, un atac de inginerie socială fusese deja efectuat, adică atacatorul, dându-se drept furnizor, a schimbat detaliile contului bancar al furnizorului cu propriile sale date. În cele din urmă, până la momentul descoperirii breșei, fuseseră trimise mai multe facturi false, care includeau noul detaliu al contului bancar.
Sistemul de monitorizare a platformei de e-mail a ajuns să dea o alertă cu privire la foldere. Compania nu a putut detecta cum atacatorul a reușit să obțină acces la conturile de e-mail pentru început, dar a presupus că un e-mail infectat a fost de vină, pentru că a dat acces grupului de utilizatori care se ocupă de plăți.
Datorită redirecționării e-mailurilor bazate pe cuvinte cheie, atacatorul a primit informații despre 99 angajați: numele și salariul unei anumite luni pentru 89 de persoane vizate; nume, stare civilă, numărul de copii, salariul, orele de lucru și informațiile rămase pe fluturașul de salariu a 10 angajații cărora le-au încetat contractele. Operatorul a anunțat doar cei 10 angajați care aparțin la acest din urmă grup.

7.2.1 CAZUL Nr. 18 - Evaluarea riscurilor, atenuarea și obligații

129. Chiar dacă atacatorul probabil nu urmărea colectarea de date cu caracter personal, deoarece breșa ar putea duce la ambele daune materiale (de exemplu, pierderi financiare) și nemateriale (de exemplu, furt de identitate sau fraudă), sau datele ar putea fi utilizate pentru a facilita alte atacuri (de exemplu, phishing), breșa este probabil să aibă ca rezultat un risc ridicat pentru drepturile și libertățile persoanelor fizice. Prin urmare, breșa ar trebui comunicată tuturor celor 99 de angajați și nu numai celor 10 angajați ale căror informații salariale au fost scurse.
130. După ce a luat la cunoștință de breșă, operatorul a forțat schimbarea parolei pentru conturile compromise, a blocat trimiterea de e-mailuri către contul de e-mail al atacatorului, a notificat furnizorul de servicii despre e-mailul utilizat de către atacator cu privire la acțiunile sale, a eliminat regulile stabilite de atacator și a rafinat alertele sistemului de monitorizare pentru a da o alertă de îndată ce este creată o regulă automată. Alternativ, operatorul ar putea elimina dreptul utilizatorilor de a stabili reguli de redirecționare, impunând necesitatea ca doar echipa de servicii IT să o facă, la cerere sau ar putea introduce o politică pe care utilizatorii ar trebui să o verifice și să raporteze cu privire la setările stabilite în conturile lor o dată pe săptămână sau mai des, în zonele care manipulează date financiare.
131. Faptul că o breșă poate avea loc și rămâne nedetectată atât de mult timp și faptul că, într-un timp mai îndelungat, ingineria ar fi putut fi folosită pentru a modifica mai multe date, a evidențiat probleme semnificative în sistemul de securitate IT al operatorului. Acestea ar trebui abordate fără întârziere, cum ar fi sublinierea revizuirilor automatizării și controale de schimbare, detectarea incidentelor și măsuri de răspuns. Operatori care manipulează date sensibile, informații financiare etc. au o responsabilitate mai mare în ceea ce privește asigurarea securității adecvate a datelor.

Acțiuni necesare pe baza riscurilor identificate		
Documentație internă	Notificare către AS	Comunicare către persoanele vizate
√	√	√