Str. M. Kogălniceanu nr. 1
Cluj-Napoca, RO-400084
Tel.: 0264-40.53.00
Fax: 0264-59.19.06
Mob: 0744423188
Birou: Clădirea Juventus, biroul nr.4,
Parcul Sportiv „Iuliu Hațieganu"
dpo@ubbcluj.ro
www.ubbcluj.ro

GHID

pentru soluționarea unor posibile incidente care pot afecta securitatea prelucrării datelor cu caracter personal

Posibile incidente (definiții):

Compromiterea datelor cu caracter personal (DCP) **–** pierderea sau alterarea, în mod accidental sau intenționat, a integrității, confidențialității și disponibilității DCP;

Confidențialitatea DCP **–** atributul DCP de a nu fi dezvăluite sau divulgate decât persoanelor sau entităților îndreptățite să le cunoască și să le acceseze în conformitate cu principiile legalității, echității, transparenței, a limitărilor legate de scop, a reducerii la minim a datelor, a exactității și a limitărilor legate de stocare;

Disponibilitatea DCP **–** calitatea DCP de a fi accesate de persoanele sau entitățile îndreptățite să le cunoască sau să le dețină în conformitate cu principiile legalității, echității, transparenței, a limitărilor legate de scop, a reducerii la minim a datelor, a exactității și a limitărilor legate de stocare;

Distrugerea neautorizată a DCP **–** situația în care DCP nu mai există sau nu sunt disponibile într-o formă în care să fie posibilă utilizarea de către UBB în conformitate cu scopurile prelucrării;

Integritatea DCP **–** atributul DCP de a nu fi fost modificate sau alterate, accidental sau intenționat, de către operator sau persoanele împuternicite ale acestuia;

Încălcare a prevederilor legale privind PDCP – orice acțiune sau inacțiune contrară prevederilor legale și procedurale în vigoare care reglementează PDCP și care este de natură a pune în pericol integritatea, confidențialitatea și disponibilitatea DCP, fără a compromite DCP;

Încălcarea securității DCP (incident de securitate care implică DCP) - încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a DCP transmise, stocate sau prelucrate entry-un alt mod, sau la accesul neautorizat la acestea;

Pierderea DCP – situația în care DCP nu mai sunt sub controlul sau în posesia UBB sau instituția nu mai are acces la acestea.

Exemple de Incidente de Securitate care pot afecta securitatea datelor cu caracter personal

Securitatea datelor cu caracter personal este crucială, iar încălcările acesteia pot avea consecințe grave atât pentru indivizi, cât și pentru organizație.

1. Atacuri cibernetice

Acestea sunt printre cele mai frecvente și sofisticate amenințări. Ele pot lua diverse forme:

- **Atacuri de tip phishing/spear phishing**: Infractorii cibernetici trimit e-mailuri sau mesaje înșelătoare, pretinzând a fi entități legitime (bănci, instituții guvernamentale, companii) pentru a păcăli utilizatorii să dezvăluie date personale sensibile (parole, numere de card de credit, CNP-uri).
- **Malware (viruși, ransomware, spyware)**: Software-ul malițios poate infecta sistemele, furând date, criptându-le și solicitând răscumpărare (ransomware) sau monitorizând activitatea utilizatorilor (spyware) pentru a colecta informații.
- **Atacuri de tip brute force sau credential stuffing**: Încercări repetate de a ghici parole sau utilizarea unor combinații de credențiale obținute din alte breșe de securitate pentru a obține acces neautorizat la conturi.
- **SQL injection/cross-site scripting (XSS)**: Vulnerabilități în aplicațiile web care permit atacatorilor să injecteze cod malițios pentru a accesa, modifica sau șterge date din baze de date sau pentru a fura cookie-uri de sesiune.

2. Breșe accidentale în bazele de date, generate de erori umane

Nu toate incidentele de securitate sunt rezultatul atacurilor rău-voitoare. Erorile umane și neglijența pot duce, de asemenea, la expunerea datelor:

- **Pierderea sau furtul de dispozitive**: Laptopuri, telefoane, stick-uri USB sau alte dispozitive care conțin date personale pot fi pierdute sau furate, permițând accesul neautorizat la informații.
- **Trimitea e-mailurilor către destinatari greșiți**: Transmiterea accidentală de e-mailuri cu date personale sensibile către persoane neautorizate.
- **Configurații greșite ale sistemelor sau bazelor de date**: Serverele sau bazele de date care conțin date personale pot fi configurate incorect, lăsând datele expuse public pe internet.
- **Eliminarea incorectă a datelor**: ștergerea necorespunzătoare a datelor de pe hard disk-uri sau alte medii de stocare înainte de reutilizare sau dezafectare.

3. Acces neautorizat intern

Amenințările pot proveni și din interiorul unei organizații:

- **Acces abuziv al angajaților**: Angajați care accesează sau divulgă date personale fără o necesitate de serviciu sau cu intenții malițioase.
- **Neglijența angajaților**: Angajați care nu respectă politicile de securitate (ex: lăsarea ecranelor deblocat, partajarea parolelor) sau care cad victime ale atacurilor de inginerie socială.

4. Incidente specific securității fizice

Securitatea fizică este la fel de importantă:

- **Efracții**: Spargeri în spațiile de lucru unde sunt stocate documente fizice sau servere care conțin date personale.
- **Furtul de documente fizice**: Dosare sau documente imprimate care conțin date personale pot fi furate.
- **Incendii, inundații sau alte dezastre naturale**: Evenimente care pot distruge echipamentele și datele stocate fizic, dacă nu există copii de siguranță sau măsuri de recuperare în caz de dezastru.

5. Atacuri specific ingineriei sociale (non-phishing)

Acestea manipulează persoanele pentru a obține informații confidențiale, fără a implica neapărat software rău-intenționat:

- **Pretexting**: Atacatorul inventează un scenariu credibil pentru a convinge victima să dezvăluie informații.
- **Baiting**: Oferirea a ceva atractiv (ex: un stick USB gratuit) pentru a convinge victima să facă o acțiune care compromite securitatea.

Pentru a minimiza riscul acestor incidente, UBB Cluj trebuie să implementeze măsuri robuste de securitate cibernetică și fizică, să efectueze instruiri regulate pentru angajați și să aibă un plan de răspuns la incidente.

Aspecte specifice:

Incidentul de securitate care implică DCP poate să apară ca urmare a unei încălcări a securității DCP sau a măsurilor organizatorice sau tehnice implementate la nivelul structurilor UBB implicate și care are ca rezultat compromiterea DCP.

Încălcarea securității DCP sau a măsurilor organizatorice sau tehnice implementate la nivelul structurilor UBB implicate poate fi rezultatul unei acțiuni sau inacțiuni accidentale sau intenționate și care să conducă la pierderea integrității, disponibilității sau confidențialității DCP.

Compromiterea DCP are loc în situația în care acestea sunt pierdute, distruse sau modificate în mod neautorizat ori divulgate unor persoane sau entități neautorizate sau nu sunt disponibile, în conformitate cu scopurile prelucrării acestora.

În situația în care acțiunile sau inacțiunile menționate mai sus duc la compromiterea DCP, rezultatul este o încălcare a prevederilor legale privind PDCP.

Managementul incidentelor de securitate care implică DCP în cadrul UBB are în vedere parcurgerea mai multor etape care vizează semnalarea incidentului de securitate, numirea unei comisii de investigare a incidentului de securitate, investigarea preliminară a incidentului de securitate, notificarea incidentului de securitate, continuarea investigațiilor, finalizarea investigațiilor și gestionarea consecințelor incidentului de securitate.

a. Semnalarea incidentului:

Încălcarea securității DCP sau a măsurilor organizatorice sau tehnice implementate la nivelul UBB se semnalează de către orice salariat sau structură organizatorică a UBB, respectiv o persoană vizată sau entitate terță, telefonic și în scris, DPO UBB CLUJ Raul-Ciprian Dăncuță (0744559348, raul.dancuta@ubbcluj.ro, 0264405300 int 6028 - centrala UBB).

Sesizarea se va face în timpul cel mai scurt în succesiunea: telefon mobil (sau telefon fix - centrala UBB - solicitându-se legătura cu DPO UBB) - e-mail (cu detalii).

b. Soluționarea incidentului:

DPO UBB CLUJ informează în timpul cel mai scurt conducerea UBB și trece la investigarea incidentului ajutat de personalul din structura unde s-a produs incidentul.

DPO UBB CLUJ prezintă datele și informațiile care au dus la suspiciunea existenței unui incident de securitate, o evaluare inițială a datelor cu caracter personal asupra cărora există suspiciunea compromiterii și structurile organizatorice implicate în fluxurile care conțin datele respective.
DPO UBB CLUJ prezintă opțiunile pentru soluționarea incidentului conducerii UBB.

Întocmit
DPO UBBB CLUJ
Dr. Raul-Ciprian Dăncuță