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

Curs deschis pentru webmasteri

„GDPR pentru Web: Securitate, Conformitate și Privacy by Design"

Realitatea riscurilor în universități
(Bazat pe Raportul DNSC din anul 2026)

Sectorul universitar are un nivel de risc cibernetic MEDIU, dar cu expunere semnificativă și vulnerabilități structurale.
Website-urile universitare sunt expuse atacurilor cibernetice.

TOP 3 RISCURI

1. Securitate IT slabă (resurse + personal)

- subfinanțare IT
- deficit de specialiști
- securitate tratată „la limită": lipsă audit constant pentru site-uri, plugin-uri neactualizate, lipsă testare de securitate.

2. Acces neautorizat & malware (BYOD, USB)

- dispozitive personale necontrolate: upload fișiere infectate, conturi compromise
- medii USB = vector de atac.

3. Exfiltrare date personale

- date studenți și angajați expuse
- lipsă politici unitare
- formulare nesecurizate
- baze de date expuse
- acces necontrolat

Probleme structurale:

- guvernanță informală (fără responsabilități clare)
- securitate REACTIVĂ, nu preventivă

- lipsă procese standardizate.

AMENINȚĂRI REALE

- ransomware
- phishing / spear phishing - folosirea AI în phishing
- acces neautorizat
- erori umane.

Atacuri cibernetice în perioade critice (admitere, examene).

Detectare slabă

23% detectare reactivă/manuală
doar 35% monitorizare continuă
concluzie: atacurile pe site pot rămâne nedetectate.

Planuri de răspuns insuficiente

60% plan informal
doar 3% testat real
când site-ul e compromis → haos operațional.

Backup ≠ siguranță

66% au backup
doar 23% îl testează
concluzie: backup inutil dacă nu poate fi restaurat.

Furnizori = risc major

doar 8% au controale serioase
56% evaluări informale
pentru web: hosting extern, pluginuri, servicii analytics.

FACTORUL UMAN = PRINCIPAL RISC

- instruire ocazională (52%)
- lipsă training real
- utilizatorul = vector principal atac.

LEGĂTURA DIRECTĂ CU PROTECȚIA DATELOR

Raportul spune clar: risc major = exfiltrare date personale
cauze: phishing, acces necontrolat, politici fragmentate.

Nu există GDPR fără:

- control acces
- protecție tehnică
- design corect.

MFA (autentificare multifactor) pentru conturi admin
Control BYOD / USB - securitate endpoint

Training continuu - nu doar ocazional
Detectare incidente - logging + monitorizare
Protecție date - prevenire exfiltrare.

Concluzie

Raportul confirmă că:

✔ mediul universitar este țintă reală
✔ datele personale sunt principalul activ riscant
✔ securitatea web este insuficient matură
✔ factorul uman și lipsa proceselor sunt critice

Universitățile nu sunt protejate - sunt ținte atractive.
- datele personale sunt principala țintă
- webmasterul este actor critic în protecție.