CERT.RO | CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA

# GDPR: Securitatea datelor cu caracter personal.

**Cristian Driga**
Consilier, Compartimentul Analize și Politici – CERT-RO
cristian.driga@cert.ro
+40-745.982.871

# *Incălcarea securității datelor personale*

*”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”*


Equifax 143 mil. victime:
- toate datele la un loc?
- accesibile online?
- companie top 3 mondial?

# Cauze principale

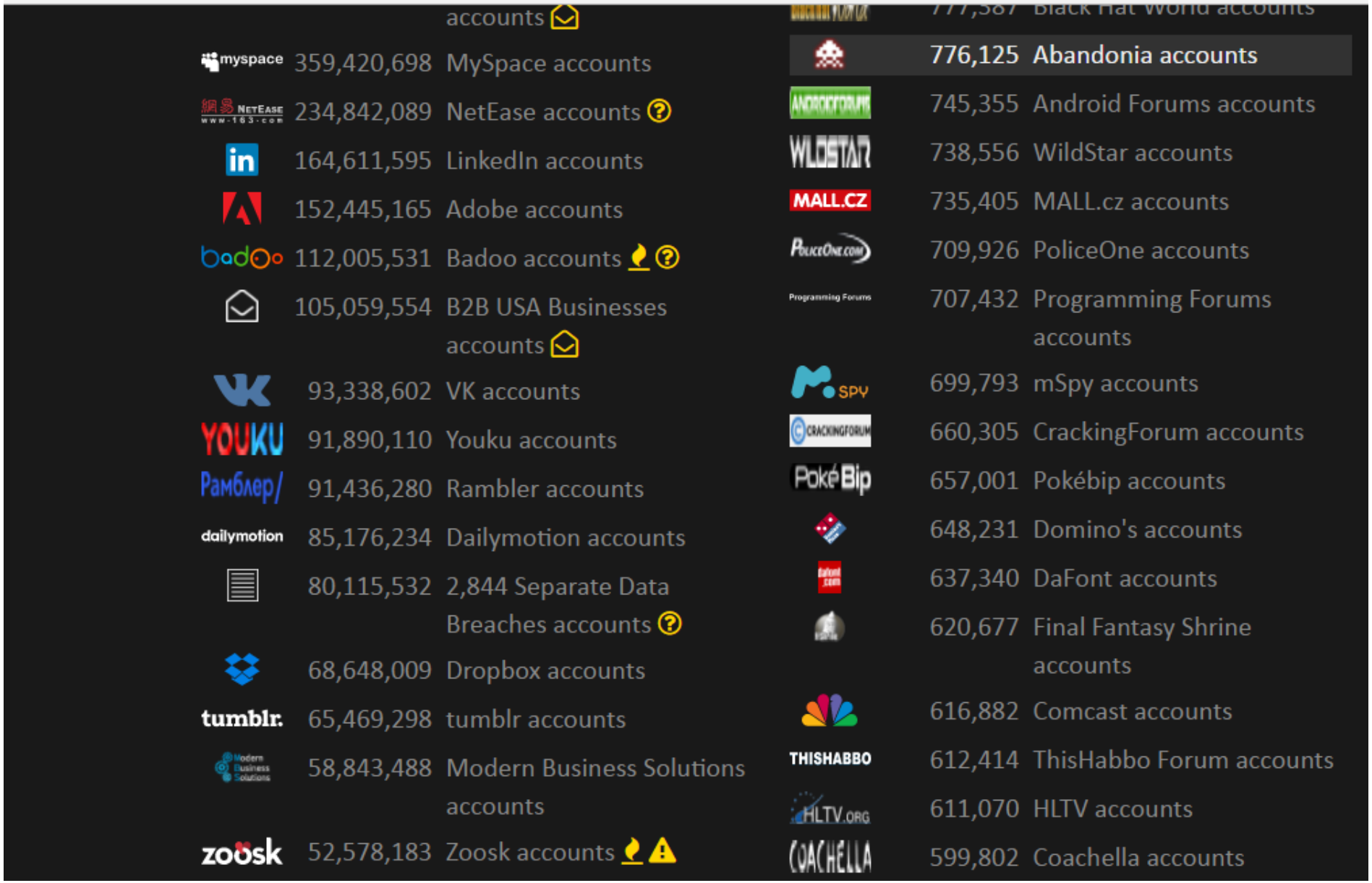
- Publicare accidentală
- Erori de configurare
- Hacking
- Proprii angajați
- Pierderea/furtul sistemului informatic
- Pierderea/furtul mediilor de stocare
- Măsuri de securitate slabe
- Vulnerabilități informatice
- Malware
- Atacuri fizice

# Domenii afectate?

Aproape toate domeniile vieții sociale și economice:

Academia, Bancar, Energie, Financiar, Guvernamental, Sanatate, Juridice, Media, Militar, Comercial, Tehnologie, Telecomunicații, Transporturi, Internet, etc.

Have I Been Pwned (Troy Hunt) [AU] | https://haveibeenpwned.com/PwnedWebsites



CERT.RO | CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA

# *România - statistici CERT-RO 2017:*

- *CERT-RO a colectat și procesat 138.217.026 de alerte de securitate cibernetică, în creștere cu 25% față de anul 2016 (110.194.890)*
- *2.896.269 de adrese IP unice și 1.709 de domenii web „.ro”*
- *33,71% (2,89 mil.) din totalul IP-urilor unice alocate spațiului cibernetic național au fost implicate în cel puțin o alertă*
- *83,63% (115,60 mil.) din alertele procesate vizează sisteme informatice vulnerabile*
- *10,32% (14,33 mil.) din alertele procesate se referă la sisteme informatice compromise*

# *Managementul securității datelor - faze*

- Pregătire
- Identificarea incidentului și a cauzelor
- Izolarea incidentului și limitarea efectelor
- Eradicare
- Recuperare
- Aspectele juridice
- Mijloace de verificare și control
- Protejarea reputației și a brandului
- Lecții învățate

# *Pregătirea*

- Securizarea terminalelor (antimalware, firewall, actualizări, criptare, etc)
- Managementul dispozitivelor personale ale angajaților (BYOD)
- Securizarea rețelei
- Vizibilitatea infrastructurilor și operațiilor
- Restricții utilizator
- Politici de backup (testate regulat)
- Politici de securitate (implementate real, cunoscute de utilizatori)
- Asigurarea răspunsului la incidente și managementul vulnerabilităților
- Audit de securitate regulat (pentesting)
- Pregătirea personalului specializat
- Conștientizarea personalului în domeniul securității informatice

# Notificarea autorității de supraveghere?

Încălcarea poate prezenta **RISCURI** pentru drepturile și libertățile individuale.

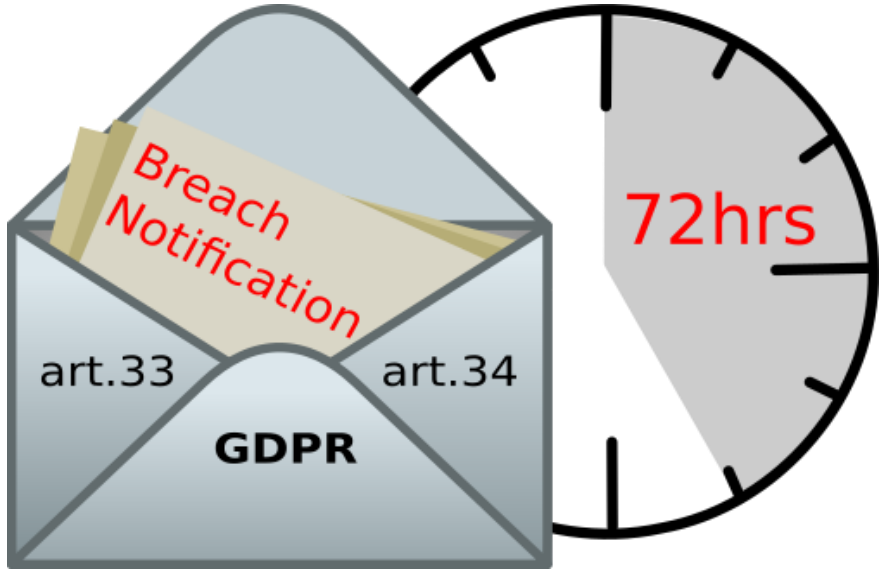
- e.g. discriminare, risc reputațional, pierderi financiare, etc.

Se determină pentru fiecare caz în parte.

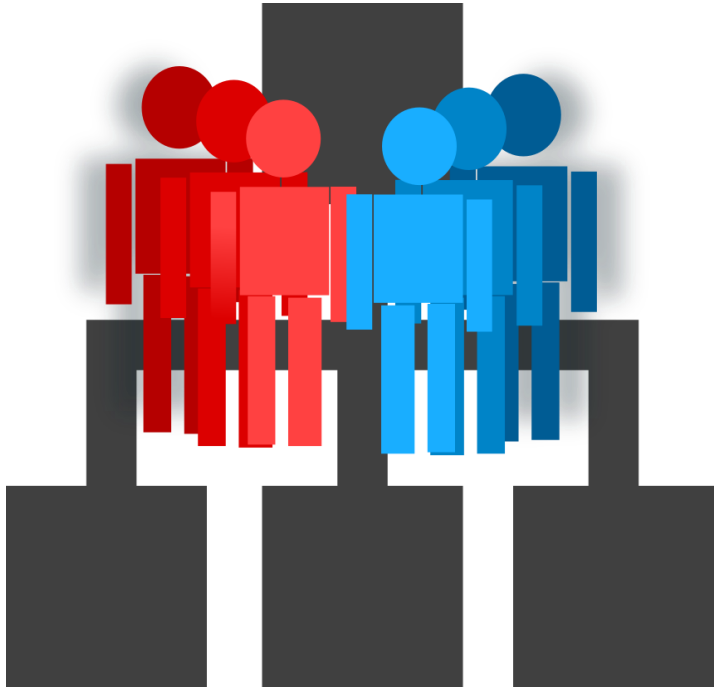
- (ex. riscul furtului de identitate în cazul pierderii datelor de client).

# Notificarea persoanelor?

Încălcarea poate prezenta **RISC CRESCUT** pentru drepturile și libertățile individuale.



# Investigare (1)



- Persoane implicate în afara DPO
  - Echipa de securitate IT/manager IT
  - Resurse umane
  - Departamentul juridic
  - Poliție ?
- Informații necesare
  - Procesele interne (intrare, ieșire, transformare, encriptare, anonimizare, etc.)
  - Tipuri de date stocate sau procesate (riscuri dacă sunt expuse)
  - Log-uri: rețea, acces, procesare, comunicatii?

# Investigare (2)

- Întrebări
  - **Ce date au fost sustrase și ce riscuri prezintă pentru indivizi?**
  - **Cine a lucrat cu aceste date ?**
  - **Unde a avut loc încălcarea securității** (infrastructură/proces)?
  - **Cum a avut loc incidentul ?**
  - **Cum a fost posibil** (motivație/eroare umană/neglijență/protecție insuficientă) ?
- Decizii
  - S-au comis fapte de natură penală?
  - Este necesară notificarea autorității?
  - Este necesară notificarea individuală? Dar a publicului?
- Lecții învățate și schimbări necesare (politici/training/infrastructură/monitorizare)

CERT.RO | CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA

# Vă mulțumesc

**Cristian Driga**
Consilier, Compartimentul Analize și Politici – CERT-RO
cristian.driga@cert.ro
+40-745.982.871