GDPR. STADIUL ACTUAL ȘI PERSPECTIVE. SOLUȚII TITUS

Mat. **Elena Andreea AVRIGEANU**

Crucial Systems & Services SRL, Constanța, România

Rezumat: Securitatea datelor este unul dintre subiectele cele mai intens discutate în acest moment. Datele sunt cele mai importante resurse ale unei companii. Puterea o deține cel ce are informația. Marile companii investesc masiv în a își proteja confidențialitatea datelor. Domeniul IT revoluționează prin instrumente și soluții capabile să prevină scurgerea de informații. 25 mai 2018, este termenul limită pentru cei care lucrează cu datele personale ale membrilor Uniunii Europene, pentru a își pune la punct fluxul de informații și pentru a asigura integritatea datelor pe care le deține și cu care lucrează.

Cuvinte cheie: GDPR, securitate, Regulamentul General Privind Protecția Datelor, IT, Titus, Clasificarea Datelor.

Abstract: Data security is one of the most discussed topics at this time. Data is the most important resource of a company. The power is held by the one who has the information. Big companies are massively investing in protecting their privacy. IT is revolutionized by tools and solutions capable of preventing data breaches. May 25, 2018, is the deadline for those who work with the personal data of EU members, in order to set up the flow of information and to ensure the integrity of the data they own and work with.

Keywords: GDPR, security, IT, Titus, Data Classification.

1. SECURITATEA INFORMATICĂ

Peste 88% dintre directorii executivi intervievați pentru un studiu Deloitte, consideră că firmele lor nu sunt vulnerabile la atacuri informatice, cu toate că peste jumătate dintre ei recunosc că firma pe care o conduc a suferit asemenea incidente în anul precedent.

Nu există organizație protejată în proporție de 100%.

În plus, mai puțin de jumătate dintre respondenți au implementat un plan de reacție în cazul unei breșe de securitate și numai 30% dintre ei consideră că partenerii externi își asumă suficient de multă responsabilitate în ceea ce privește securitatea. Totodată, 74% dintre cei 121 de respondenți au identificat breșele de securitate înregistrate de terți ca fiind în topul amenințărilor; pe locurile următoare se situează atacuri de tipul *denial of service* (menite să supra-solicite destinatarii, ducând la blocarea/ refuzul serviciilor) și eroarea sau omisiunile angajaților.

2. DESPRE GDPR

Regulamentul General de Protecție a Datelor (*GDPR, abrevierea din limba engleza General Data Protection Regulation*) cu caracter personal a fost adoptat în aprilie 2016 și va avea efect începând cu **25 mai 2018**, în toate statele membre UE. GDPR înlocuiește legislația actuală privind protecția datelor, în vigoare în UE și la nivel național.

Regulamentul se aplică companiilor cu sediul în UE, care procesează date cu caracter personal (fie direct, fie prin împuternicit), dar și acelor companii care nu au sediul în UE dar oferă bunuri și servicii direct rezidenților UE și monitorizează comportamentul acestora. De asemenea, GDPR se aplică și instituțiilor publice locale și naționale.

Impactul va fi major pentru majoritatea companiilor care folosesc procesarea datelor cu caracter personal și care vor fi obligate să demonstreze conformitatea cu noile prevederi. Activitatea va fi investigată de către o Autoritate de Supraveghere locală (ANSPDCP în RO). Amenzile pentru încălcarea Regulamentului pot atinge 20 milioane EURO sau 4% din cifra de afaceri (mondială) corespunzătoare exercițiului financiar anterior, luându-se în calcul valoarea cea mai mare.

- *Îmbunătățește drepturile persoanelor cu privirea la datele confidențiale* .
- *Creșterea responsabilității privind protejarea informațiilor.*
- *Raportare obligatorie a incidentelor de securitate.*
- *Sancțiuni semnificative pentru nerespectarea normelor.*

Scopul principal este de a armoniza modul în care sunt protejate datelor personale la nivelul tuturor statelor membre UE.

Zece schimbări critice în contextul GDPR:

1. Amenzile sunt de până la 4% din Cifra de Afaceri a companiei;

2. Organizațiile publice și companiile mari (peste 250 angajati) trebuie să desemneze un responsabil cu protecția datelor (DPO);

3. Raportările incidentelor de securitatea către persoana responsabilă este obligatorie;

4. Sunt desemnate măsurile de răspundere pentru încălcărea vieţii private;

5. Cetăţenii UE au dreptul de a fi uitaţi, de a li se uita datele;

6. Copiii au un drept explicit al vieţii private;

7. Consimţământul trebuie să fie lipsit de ambiguitate;

8. Procesarea datelor în scopul deţinerii lor trebuie să fie specifică;

9. Acordul de confidenţialitate înlocuieşte acordul anterior Safe Harbour cu privire la transferurile de date internaţionale;

10. Accesul la informaţii ale organelor de drept , trebuie să urmeze procedurile specifice.

Cei 4 paşi esenţiali în GDPR

1. **Discovery** *identifică si localizează datele confidenţiale.*

Fundaţia oricărei strategii de securitate a datelor este de a identifica acele informaţii sensibile şi confidenţiale şi de a reglementa acest proces, astfel încât atât utilizatorii, cât şi tehnologia de securitate să fie capabilă să ia decizii informatice deliberate, totul pentru ca informaţiile să fie protejate. Suita de clasificare TITUS ajută organizaţiile să fie conforme cu cerinţele GDPR prin identificarea şi clasificarea fişierelor şi a email-urilor.

2. **Manage** *gestionează modul în care sunt tratate şi procesate datele cu caracter personal*

Clasificare datelor - Conştientizaţi-vă angajaţii de valoarea datelor cu care lucrează

Clasificarea este un pilon central al GDPR, care educă utilizatorii să acorde o atenţie sporită datelor confidenţiale la care au acces. Efectele vizuale aplicate de TITUS şi mesajele de tip pop-up, vin în ajutorul utilizatorului amintindu-i constant de impactul pe care alegerile sale îl poate avea.

Cetăţenii UE au dreptul de a fi uitaţi - *Ştergerea proactivă a datelor după un timp.* Informaţiile personale colectate de către organizaţii sunt menite a fi şterse la un moment dat. Poate fi dificil să garantezi că toate datele personale se pot elimina la o anumită dată, atunci când datele sunt făcute să circule (în interiorul aceleiaşi firme). Imaginaţi-vă că datele unei companii pot fi localizate în diverse locuri – cloud, medii de stocare portabile, fişiere email etc. Prin adăugarea de metadate de retenţie în momentul clasificării, este simplu să identifici fişierele ce trebuie şterse în scopul conformităţii GDPR.

3. **Protect** *stabileşte măsuri şi soluţii de securitate pentru a preveni, detecta şi răspunde la vulnerabilităţile sistemului*

Ştiind unde se află datele tale şi ce valoare au acestea pentru afacerea ta, educând utilizatorii şi îmbunătăţind procesul de lucru pentru a lua cele mai bune decizii cu privire la modul de protejare a informaţiei, aveţi ingredientele esenţiale în managementul riscului.

Educând şi obligând în acelaşi timp utilizatorii să se oprească, să analizeze şi să cântărească valoarea informaţiei cu care lucrează, la care are acces sau pe care o creează, face din soluţia Titus un produs compliant GDPR. Titus, ajută utilizatorii să respectele politicile de securitate ale companiei, oferind un suport interactiv şi target-at în activitatea utilizatorului cu documentele şi emailurile, neafectând în niciun fel modul obişnuit de lucru la birou. Responsabilizaţi-vă utilizatorii pentru a evita încălcări ale normelor impuse de GDPR, şi nu în ultimul rând pentru a evita amenzi usturătoare.

4. Report *păstrează şi gestionează notificările de încălcare a politicilor de securitate*

Data Protection Officer - Ofiţerul responsabil cu protecţia datelor verifică şi monitorizează cum sunt manevrate datele personale, încurajând adoptarea de măsuri capabile să protejeze informaţiile confidenţiale. Acesta are obligaţia de a reporta orice incident autorităţilor competente. Clasificând email-uri, documentele şi fişierele, permite elaborarea de analize şi rapoarte detaliate privind logo-urile create, dar şi a încălcările politicilor de securitate. Aceste rapoarte pot evidenţia către DPO acele situaţii în care utilizatorii tratează cu superficialitate valoarea datelor la care au acces.

Conform articolului 35, toate instituţiile publice sunt obligate să aibă un DPO, precum şi toate companiile cu mai mult de 250 de angajaţi. Acest serviciu poate fi şi externalizat.

Funcţia şi sarcinile responsabilului cu protecţia datelor sunt detaliate in art. 37-39. Sugestiv, responsabilul este indicat ca fiind noul „gardian" al prelucrărilor de date cu caracter personal.

3. CLASIFICAREA DATELOR CU TITUS

Clasificarea datelor educă utilizatorul şi îl determină să lucreze cu atenţie cu informaţiile la care are acces.

Soluţiile de clasificare Titus sunt menite să ajute şi să educe utilizatorul final împotriva propriilor greşeli. Orice companie are date. Fiecare angajat lucrează zilnic cu datele importante şi confidenţiale ale companiei. Orice greşeală poate costa extrem de mult!

Pe de o parte, are de suferit instituţia a căror date confidenţiale pot ajunge în posesia concurenţei, sau în cazul instituţiilor guvernamentale, date secrete ale cetăţenilor pot deveni publice, ceea ce ar aduce un prejudiciu important organizaţiei.

Pe de altă parte, aceste greşeli pot aduce prejudicii şi sancţiuni angajaţilor.

Se poate greşi extrem de uşor, cu voinţă (un angajat rău intenţionat) sau fără voinţă (un angajat începător, oboseala etc).

CLASIFICAREA ESTE FUNDAȚIA PENTRU SECURITATEA DATELOR

Soluțiile TITUS permit organizațiilor să clasifice și să-și protejeze informațiile sensibile, să se supună regulilor interne ale instituției, educând utilizatorul să dimensioneze sensibilitatea informațiilor prin identificarea datelor nestructurate. Soluțiile TITUS sunt menite să protejeze compania împotriva scurgerilor de informații prin implicarea utilizatorilor în clasificarea și protecția informațiilor cu care instituția lucrează.

Aceste informații sunt prezente în emailuri, documente și alte tipuri de fișiere.

În prezent, clasificarea datelor este un element necesar. Este un factor esențial pentru orice companie. Identificând valoarea datelor în momentul creării și conștientizând riscul divulgării accidentale de informații, aducem un plus de valoare la ceea ce înseamnă protecția datelor – în acest fel educăm utilizatorii să identifice datele cu care lucrează și îi forțăm să își asume responsabilitatea pentru acțiunile lor în conformitate cu reglementările companiei.

Beneficiile clasificării:

• **Educă și responsabilizează utilizatorii** – companiile se protejează astfel de neglijența angajaților (atât de cei rău - intenționați cât și de neglijența lor);

• **Crește gradul de securitate a companiei**;

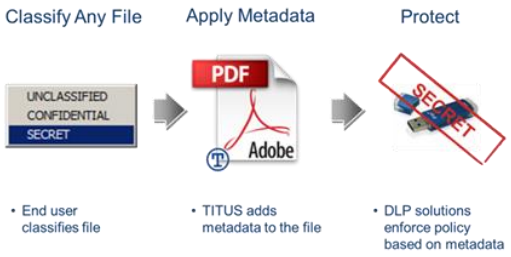
• **Protejarea informațiilor** – se integrează cu soluțiile DLP.

Solutii Titus:

TITUS Classification pentru Microsoft Office – această soluție se adresează documentelor de tip Word, Excel și PowerPoint. Încurajează utilizatorii să clasifice documentele pe care le creează și prin politicile aplicate limitează pierderea de informații prin trimiterea informațiilor către destinatari străini.

TITUS Classification for Desktop – această soluție permite aplicarea de metadate oricărui fișier, utilizatorul asumându-și responsabilitatea pentru fișierele create. TITUS Classification Mobile – numărul utilizatorilor care folosesc dispozitivele mobile proprii pentru a accesa mailul și fișierele de la servici este într-o continuă creștere. Această soluție se adresează protecției mailurilor, documentelor și fișierelor companiei cu care utilizatorul lucrează de pe dispozitivul personal. Totodată, delimitează căsuța de email personală de cea business, împiedicând scurgerea de informații.

TITUS Message Classification – se adresează pentru Microsoft Outlook, Outlook Web App și Lotus Notes. Această soluție educă utilizatorul și îl responsabilizează să clasifice emailurile pe care le trimite (public, intern, confidențial), utilizatorul dimensionând astfel sensibilitatea informațiilor conținute în respectivul mesaj. Cu ajutorul politicilor aplicate, Titus împiedică scurgerea de informații care pot avea loc atât cu bună știință cât și din neatenția utilizatorului.



4. CONCLUZII

GDPR – *numărătoarea inversă a început* - Cu doar câteva luni rămase la dispoziție, organizațiile trebuie să acționeze acum pentru a dezvolta un plan de acțiune pentru protecția datelor și pentru a evita sancțiuni costisitoare. Demersul pentru complianța GDPR, în funcție de companie, poate dura și câteva luni, întrucât vorbim de un audit și implementare soluții de securitate.

Entitățile vizate ar trebui să inițieze cât mai curând posibil demersurile pentru asigurarea conformității. Având în vedere faptul că pregătirea și alinierea la cerințele GDPR va fi un proces diferit pentru fiecare companie în parte și va depinde de o multitudine de factori, vă recomandăm să efectuați un audit capabil să vă ofere consultanță pas-cu-pas pe parcursul întregului proces de pregătire și aliniere, care să vă ajute să înțelegeți riscurile specifice fiecărui domeniu, să determinați nivelele acceptabile de expunere și nu în ultimul rând să implementați sisteme de control și monitorizare permanentă. Programul general de conformitate cu cerințele de protecție a datelor cu caracter personal poate cuprinde:

- Conștientizarea și înțelegerea importanței GDPR;
- Analiza GAP ;
- Notificări și acorduri;
- Cerințe de conformitate;
- Proceduri interne;
- Implementare soluții de securitate & Instruire.

BIBLIOGRAFIE

[1] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016

[2] http://www.businessmagazin.ro/actualitate/securitatea-informatica-lipseste-aproape-complet-din-agenda-executivilor-din-romania-10682416

[3] www.titus.com

Despre autor

Andreea AVRIGEANU,
Director General Crucial Systems, Constanța, România

Cu aproape 20 de experiență managerială, absolventa Facultății de Matematică și Informatică din cadrul Universității „Ovidius“, conduce cu succes una dintre cele mai mari firme de IT din Constanța, o companie ce activează în zona de SE a României. Pasiunea pentru afaceri și perfecțiune, o îndrumă mereu să abordeze direcții noi, lucru care se vede prin inovația tehnologică și de concept pe care o aduce pieței din Constanța, și nu numai. Printre realizările notabile vorbim de cel mai mare eveniment de IT din Dobrogea, ETIC (Evenimentul de Tehnologie Informatica Crucial), care are loc anual în luna mai.