Scandalul Cambridge Analytica a scos la iveală faptul că rețeaua de socializare Facebook accesa și copia lista telefoanelor efectuate de utilizatori sau chiar a mesajelor trimise de aceștia. Datele a peste 50 de milioane de utilizatori ar fi fost folosite în scopuri pentru care aceștia nu știau că și-ar fi dat vreodată acceptul, așa cum ar fi manipularea intenției de vot în cadrul alegerilor din Statele Unite. Nu este, desigur, prima oară când aflăm că giganți din domeniul tehnologiei - așa cum ar fi Google, Apple sau Twitter - sunt acuzați că accesează sau permit altor aplicații să acceseze date confidențiale; protestul pare a fi însă mai virulent de această dată, culminând cu mișcarea #deletefacebook. Printre cei care s-au alăturat este și Elon Musk, care a șters paginile companiilor pe care le deține (Tesla și SpaceX) de pe rețeaua de socializare.

Cu toate că e greu să trasăm o legătură directă între Regulamentul General privind Protecția Datelor Personale și scandalul Cambridge Analytica, pare că normele impuse de Uniunea Europeană au rolul de a preveni, pe viitor, astfel de întâmplări.

Deși s-a tot vorbit de GDPR în ultima vreme, e bine să începem prin a explica trei lucruri esențiale: ce este GDPR, cui se adresează și care sunt consecințele nerespectării regulilor pe care acesta le impune.

„GDPR ARE O ABORDARE NOUĂ A MODULUI ÎN CARE AR TREBUI SĂ SE GESTIONEZE CONFIDENȚIALITATEA ÎNTR-O ORGANIZAȚIE; ORGANIZAȚIILE SUNT RESPONSABILE PENTRU IMPLEMENTAREA ACESTOR MODIFICĂRI, IAR MULTE VA TREBUI SĂ NUMEASCĂ UN RESPONSABIL PENTRU PROTECȚIA DATELOR, INTERN SAU EXTERN."

CĂTĂLIN SĂPAȘU, SENIOR ASSOCIATE, DUNCEA, ȘTEFĂNESCU & ASSOCIATES

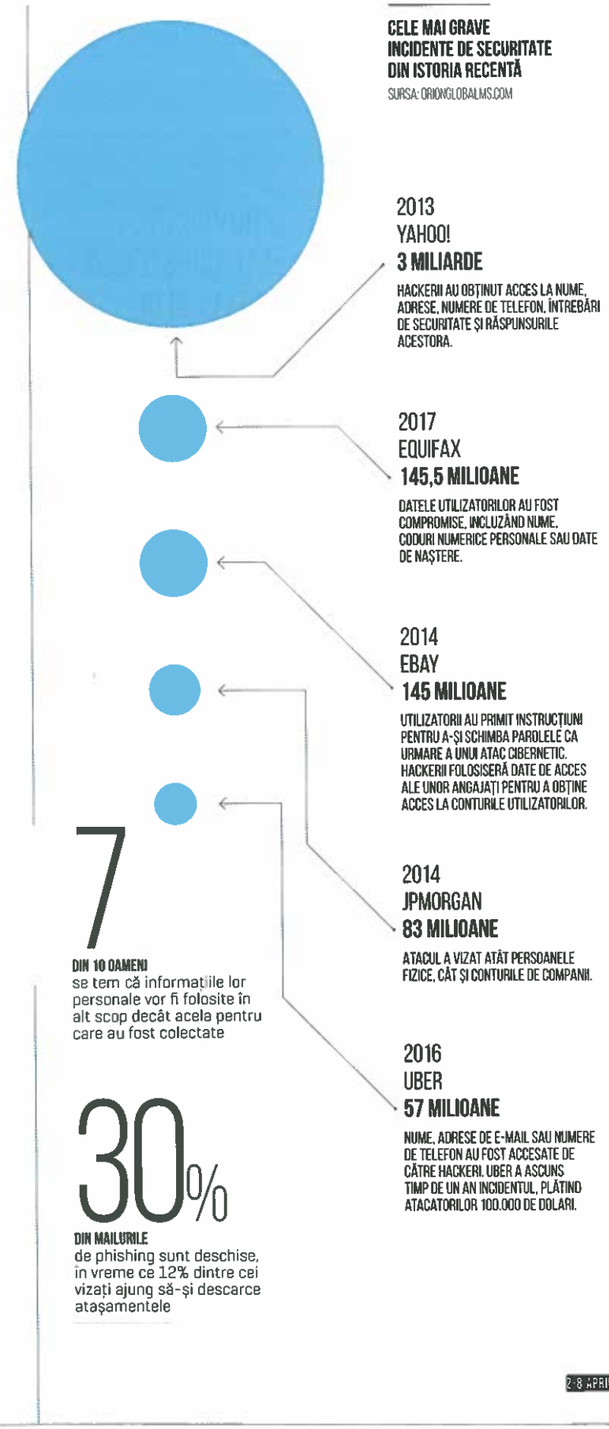
Pentru a răspunde amenințărilor asupra securității cetățenilor și companiilor UE, Comisia Europeană a prezentat în 2012 un pachet de acte legislative privind reforma normelor UE în materie de protecție a datelor, destinat să adapteze Europa la era digitală. Pachetul de reformă a fost adoptat de Parlamentul European la 14 aprilie 2016 și cuprinde două instrumente: Regulamentul general privind protecția datelor (GDPR) și Directiva privind protecția datelor pentru sectoarele poliției și justiției penale. Regulamentul general privind protecția datelor le va permite cetățenilor să exercite un control sporit asupra datelor lor cu caracter personal. Potrivit unui sondaj Eurobarometru, două treimi dintre europeni (67%) au declarat că sunt îngrijorați în legătură cu faptul că nu dețin controlul deplin asupra informațiilor pe care le furnizează online.

GDPR se adresează tuturor persoanelor juridice, indiferent că vorbim de societăți comerciale, persoane fizice autorizate, asociații și fundații (inclusiv asociații de proprietari), cabinete medicale, școli și grădinițe sau autorități publice care prelucrează date personale. Pentru a înțelege dacă GDPR vă afectează sau nu businessul, trebuie să vă puneți următoarele întrebări: am relații comerciale sau contractuale cu persoane fizice (angajați, clienți)? Procesez date cu caracter personal pentru alți parteneri de afaceri (așa cum ar fi o companie ce prestează servicii de contabilitate sau de curierat)? Dacă la oricare din întrebările de mai sus răspunsul este da, atunci GDPR va avea un impact asupra businessului.

Afacerile care nu sunt afectate de Regulamentul general privind protecția datelor sunt cele care desfășoară activități care nu intră sub incidența legilor din Uniunea Europeană sau cele realizate de către autorități competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor. Sunt de asemenea exceptate lucrările efectuate de o persoană fizică în cadrul unei activități exclusiv personale sau domestice: cu alte cuvinte, dacă procesați date acasă doar de dragul de a le procesa, nu veți avea legătură cu noul regulament.

Pentru a explica cel de-al treilea element, și anume care sunt consecințele în urma încălcării GDPR, trebuie înțeles cum modifică acesta fluxul operațional al unei companii.

Noua legislație europeană aduce o serie de elemente de noutate. Astfel, companiile sunt obligate să numească, în anumite condiții, un responsabil cu protecția datelor la nivel de companie sau grup care va acționa în fapt mai mult ca un reprezentant „în teritoriu" al autorității, având rolul de a se asigura că toate procesele și procedurile operatorului sunt conforme cu legea și de a notifica autoritatea competentă în termen de 72 de ore atunci când are loc o încălcare a securității datelor cu caracter personal. Unele drepturi va trebui redefinite, iar altele noi va trebui definite pentru persoanele vizate (de exemplu dreptul de a fi uitat sau dreptul la portabilitatea datelor). Apar condiții mult mai stricte pentru o procesare legală în baza consimțământului persoanei vizate, iar persoanele împuternicite să proceseze date cu caracter personal în numele operatorului vor avea o mai mare răspundere. Companiile va trebui să desfășoare evaluări de impact în cazul în care prelucrează automat date cu caracter personal care produc efecte juridice privind persoana fizică, care o afectează în mod similar într-o măsură semnificativă sau în cazul în care prelucrează pe scară largă anumite categorii speciale de date (cel mai des întâlnit exemplu fiind cele privind sănătatea, datele genetice și biometrice) sau date cu caracter personal privind condamnări penale și infracțiuni. O a treia situație care presupune evaluări de impact este monitorizarea sistematică, pe scară largă, a unei zone accesibile publicului.



PE ULTIMA SUTĂ DE METRI

La începutul anului, mai mult de o treime dintre companiile din România (37%) nu aflaseră încă despre GDPR sau credeau că regulamentul nu li se aplică, conform unui studiu realizat de MKOR Consulting. GDPR va trebui aplicat și respectat de majoritatea companiilor din România, însă doar 62% conștientizau la începutul anului că vor fi afectate de noua reglementare. Dintre acestea, aproape două treimi își actualizaseră sau erau în curs de actualizare a proceselor pentru a fi în acord cu legislația până în 25 mai, dată la care GDPR intră în vigoare în toată Uniunea Europeană. 16% dintre managerii chestionați nu cred că se vor putea alinia cerințelor GDPR până la această dată. „Reglementările GDPR bat la ușa companiilor, în condițiile în care orice societate care colectează date despre clienții și colaboratorii săi va trebui să se conformeze cu cerințele regulamentului european până în 25 mai. Noi, la MKOR, am fost curioși să vedem în ce măsură sunt companiile românești informate și, mai mult, pregătite să își adapteze procesele pentru a se conforma noilor norme de protecție a datelor", precizează Corina Cimpoca, consultant senior și fondator al MKOR Consulting. Aproape o treime (31%) dintre companii doar s-au informat despre GDPR, fără a trece însă la acțiune. Acestora li se adaugă alte 13% care nici măcar nu au încercat să afle detalii despre cum vor fi afectați. Cel mai nepregătite sunt microîntreprinderile: 20% dintre acestea nu au făcut nimic pentru a fi în acord cu noua reglementare, iar alte 44% doar s-au informat.

Pe de altă parte, aproape un sfert dintre companiile respondente și-au identificat procesele de lucru care vor suferi modificări și și-au pregătit un plan de lucru, iar 19% dintre ele au pregătit o echipă internă dedicată implementării GDPR. O parte dintre companiile românești (respectiv 18%) au apelat la servicii de consultanță specializată pentru a se alinia reglementărilor GDPR. În general acestea sunt companii mari și mijlocii, care dispun și de bugete mai generoase. Dacă pentru cea mai mare parte a companiilor respondente (19%) sumele cheltuite pentru a se asigura că respectă reglementările GDPR nu depășesc 1.000 de euro, alții trebuie să asigure bugete mai mari. Bugetele a 9% dintre companiile românești se situează între 1.001 și 3.000 de euro, în timp ce 6% dintre companii vor cheltui peste 10.000 de euro.

„PROVOCAREA ESTE CREȘTEREA NIVELULUI DE CONȘTIENTIZARE A RISCURILOR LA CARE SE EXPUN COMPANIILE, UTILIZATORII INDIVIDUALI, ANGAJAȚII DACĂ NU IAU MĂSURI DE PROTECȚIE ÎMPOTRIVA ATACURILOR CIBERNETICE".

DORU MANEA, CEO, NETSAFE

Implementarea GDPR este o oportunitate pentru a securiza nu doar datele cu caracter personal, ci toate datele sensibile pe care le deține o companie, remarcă Bogdan Tudor, CEO al companiei de consultanță Startech Team. „De cele mai multe ori, în plus față de datele a căror protecție UE vin să o impună, companiile dețin date de o valoare mult mai mare, precum informații despre clienți, parteneri, prețuri de producție sau de vânzare, salariile în companie și multe altele de a căror securitate poate depinde chiar afacerea în sine", spune el. În prezent, cea mai eficientă metodă de protecție a datelor este deconectarea de la internet a sistemelor pe care acestea sunt stocate. „Dacă nu poți face acest lucru, vei avea nevoie de o analiză făcută de un expert capabil să recomande soluția potrivită pentru afacerea ta. Vremurile în care să dețiii un antivirus ca modalitate de securitate au apus de mult. Astăzi, antivirușii clasici sunt neputincioși în fața noilor amenințări și este nevoie de o nouă abordare, care să țină cont atât de noile modalități dinamice de atac, de noile atacturi de tip ransomware dar și de o nouă filosofie a securității IT, aceea că niciun sistem nu poate fi sigur 100% și cel mai important este să poți detecta atacul, minimiza daunele și restaura sistemele la starea inițială fără pierderi considerabile."

Bogdan Tudor consideră că afacerile care se îngrijesc doar de protecția datelor personale sau de teama amenzilor impuse de GDPR „aruncă pe fereastră o parte din investiție. Este cea mai bună ocazie pentru a face o evaluare exhaustivă a tuturor datelor sensibile pe care compania le deține, spune el, și de a le proteja în consecință, maximizând astfel investiția.

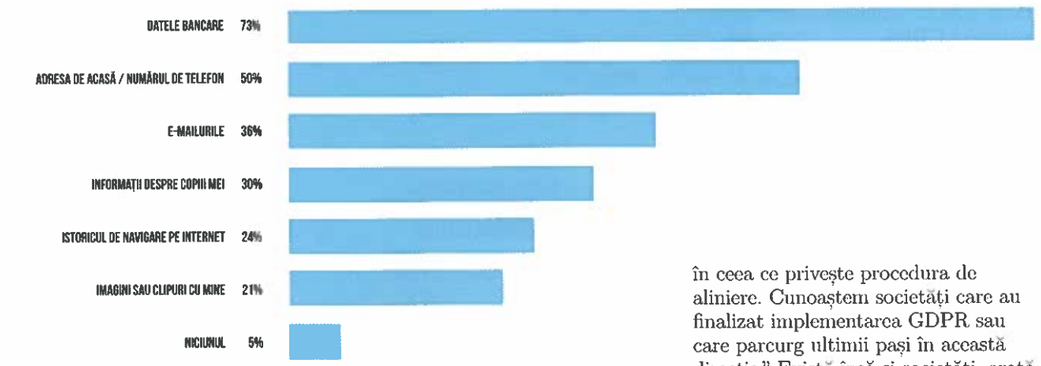
Mai mult, dacă până acum companiile sufereau o breșă de securitate și ascundeau acest lucru, în noile condiții sunt obligate să raporteze acest lucru autorităților. „De aceea, mă aștept ca incidentele de securitate să facă deliciul media în perioada următoare. Cu toate acestea, datele vor fi mai bine protejate și pe termen lung mă aștept ca numărul de incidente să scadă. Orice măsură de protecție a datelor este un pas înainte", subliniază CEO-ul Startech Team.

„Observăm, fără îndoială, o destul de mare efervescență în această materie, cu precădere din partea consultanților care încearcă să conștientizeze publicul cu privire la importanța implementării GDPR în România", spune avocatul Cătălin Săpașu, senior associate în cadrul companiei Duncea, Ștefănescu & Associates. „Credem că mare parte din companiile românești, în special filiale ale multinaționalelor, au reacționat din timp la modificările pe care le presupune GDPR, considerând efectele adverse ale neaplicării acestui regulament, și au început încă de anul trecut pregătirea în ceea ce privește procedura de aliniere. Cunoaștem societăți care au finalizat implementarea GDPR sau care parcurg ultimii pași în această direcție." Există însă și societăți, arată el, care au început relativ de curând pregătirile pentru implementarea GDPR și care acum fac primii pași în vederea actualizării politicilor de confidențialitate și a formularelor de obținere a consimțământului. „A fost esențială informarea repetată a partenerilor de afaceri asupra acestor modificări legislative majore și sprijinirea lor în orice etapă de implementare s-ar afla. Mai mult, considerăm că și start-up-urile ar trebui să implementeze, încă din etapa constituirii firmei, valorile și garanțiile oferite de GDPR. Se poate astfel realiza o formă incipientă a principiului privacy by default."

Raportat evident la dimensiunea acestora, impactul asupra IMM-urilor va fi semnificativ, multe dintre acestea neavând implementate astfel de politici, crede Cătălin Săpașu. Concret, deși IMM-urile nu dețin logistică, resurse și forță de implementare similare cu ale multinaționalelor (care, în multe dintre cazuri, aplică proceduri uniformizate la nivel de grup), managementul acestora va trebui, mai devreme sau mai târziu, să demareze și să finalizeze acțiunile necesare în vederea conformării la GDPR. „Managerii în general va trebui să devină în scurt timp – dacă nu au făcut-o deja – foarte atenți cu procedurile de colectare/stocare a datelor cu caracter personal și cu aplicațiile pe care companiile lor le folosesc în activitatea curentă. Nu în cele din urmă, sancțiunile foarte mari prevăzute de GDPR vor determina

CELE MAI IMPORTANTE TIPURI DE INFORMAȚII PENTRU UTILIZATORI (2017)

SURSA: STATISTA.COM



90%
DIN COMPANIILE din Statele Unite au fost victime ale unui atac cibernetic în 2016

2
TRILIOANE DE DOLARI este valoarea la care vor ajunge pagubele datorate de crime cibernetice în 2019

48%
DIN 10 OAMENI din bretele de securitate au în spate o intenție malițioasă, restul datorându-se erorilor umane sau erorilor în sistem

IMM-urile să se alinieze foarte rapid cerințelor GDPR."

Un prim pas pe care cei responsabili ar trebui să îl facă este informarea tuturor angajaților companiei în legătură cu garanțiile pe care trebuie să le ofere societatea persoanelor vizate. În cadrul acestei etape li se poate explica angajaților și colaboratorilor care sunt datele personale procesate, motivul pentru care sunt procesate, de ce sunt importante, ce garanții trebuie să ofere compania și care sunt sancțiunile corelative. „Această «educare» a angajaților ar trebui să înceapă de la primul angajat care intră în contact cu persoana vizată (cel mai adesea front deskul) și să continue cu personalul care intermediază transmiterea către management a documentelor care conțin date personale. În același timp, un manager ar trebui să solicite tuturor furnizorilor și clienților companiei garanții adecvate în legătură cu respectarea drepturilor persoanelor vizate și, în cazul existenței unor riscuri aferente respectării GDPR din partea acestor furnizori sau clienți sau ca urmare a neconformării ulterioare la cerințele legale, să sisteze colaborarea cu aceștia."

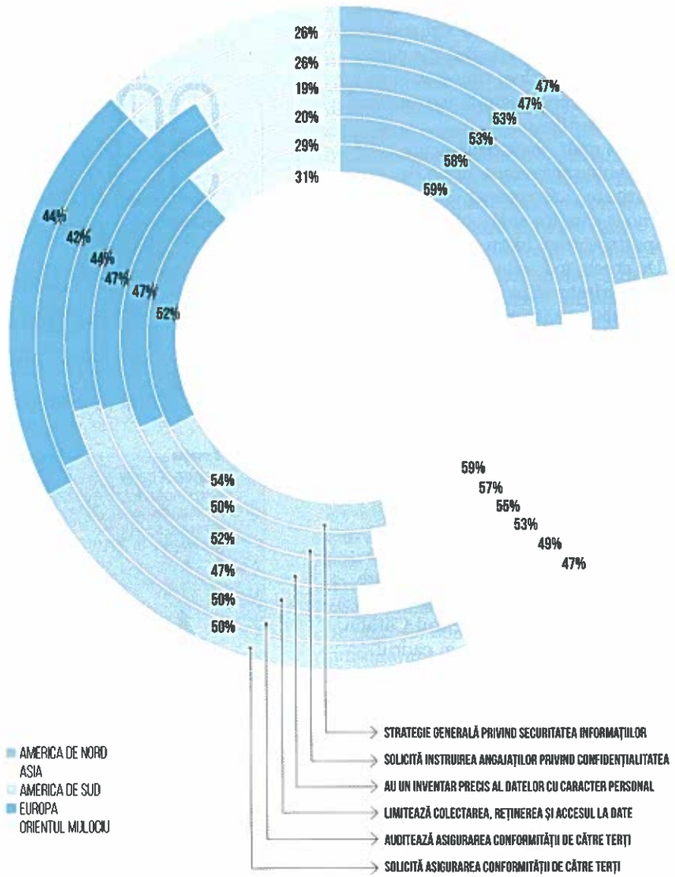
Având în vedere sancțiunile legale considerabile și timpul limitat pe care companiile îl mai au la dispoziție pentru implementarea tuturor aspectelor juridice și tehnice, asistența externă devine importantă pe toată perioada de implementare, cu atât mai mult cu cât schimbările sunt derulate de regulă la nivelul întregii organizații, explică avocatul. Cu toate acestea, asistența juridică este necesară în faza incipientă a procesului de aliniere la standardele GDPR, în mod special pentru efectuarea unui studiu de risc. Acesta constă în identificarea modului de colectare a datelor cu caracter personal, a fluxurilor de date transferate către terți, analiza și definirea procedurilor de lucru, analiza implicațiilor prevederilor GDPR asupra activității companiei, relației cu contractorii, subcontractorii, modului de obținere a consimțământului persoanelor vizate și analiza politicilor și procedurilor interne existente ale companiei pentru asigurarea protecției datelor cu caracter personal.

„Bugetul aferent implementării GDPR este fără îndoială important; acesta este desigur variabil. Pentru a efectua o planificare bugetară în ceea ce privește alinierea companiei la cerințele GDPR trebuie, în primul rând, să înțelegem modificările concrete pe care le va aduce la nivelul organizației. Astfel, acesta aduce o serie de schimbări pentru anumite industrii, de exemplu o schimbare a vârstei la care copiii își pot exprima consimțământul, ceea ce va fi relevant pentru companiile care prestează servicii în domeniul educației, entertainmentului, în general businessuri care se adresează copiilor", spune Cătălin Săpașu. Din punctul de vedere al bugetului, o noutate este faptul că GDPR are o abordare nouă a modului în care ar trebui să se gestioneze confidențialitatea într-o organizație; organizațiile sunt responsabile pentru implementarea acestor modificări, iar multe va trebui să numească un responsabil pentru protecția datelor (data processing officer – DPO), intern sau extern.

GRADUL DE IMPLICARE ÎN PROBLEME CE ȚIN DE SECURITATEA DATELOR

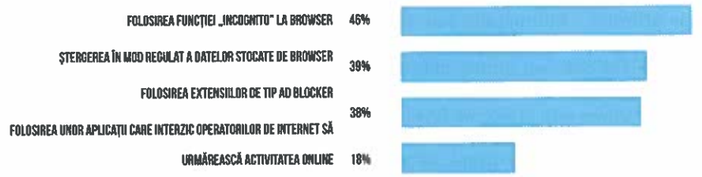
Companiile din Europa și Orientul Mijlociu sunt în general în urma celor din Asia, America de Nord și America de Sud în elaborarea unei strategii globale de securitate a informațiilor.

SURSA: PWC GLOBAL STATE OF SECURITY SURVEY (GSISS), 2018



MĂSURILE DE SECURITATE ADOPTATE DE UTILIZATORII DE INTERNET (GLOBAL, 2016)

SURSA: STATISTA.COM



Încălcarea prevederilor GDPR atrage impunerea unor amenzi de la autoritatea de supraveghere, fiind stabilite două seturi de praguri maxime pentru penalizările care pot fi impuse pentru încălcările relevante. Încălcarea anumitor prevederi ale GDPR, precum cele referitoare la principiile de bază pentru prelucrare, drepturile persoanelor vizate sau transferurile de date către un destinatar dintr-o țară terță este supusă unor amenzi administrative de până la 20 de milioane de euro sau până la 4% din cifra de afaceri globală, în funcție de care dintre acestea este mai mare. Alte încălcări, precum cele referitoare la obligațiile operatorului și ale persoanei împuternicite de operator, obligațiile organismului de certificare sau de monitorizare sunt supuse unor amenzi administrative de până la 10 milioane de euro sau până la 2% din cifra de afaceri mondială totală anuală a unei întreprinderi, oricare dintre acestea este mai mare. „Valoarea crescută a amenzilor administrative impune acordarea unei importanțe deosebite noilor cerințe ale GDPR. Astfel, companiile trebuie să aibă în vedere faptul că aplicarea unei amenzi administrative consistente poate conduce, în unele cazuri, la suspendarea activității acestora sau, în ultimă instanță, la imposibilitatea de a continua activitatea", notează Cătălin Săpașu. „Riscul companiilor nu este însă legat doar de suportarea amenzilor administrative, ci și de reputație. Astfel, în cazul încălcării cerințelor impuse de GDPR, numele companiei poate fi asociat cu lipsa de securitate, iar deteriorarea brandului unei companii este dificil de cuantificat", încheie el.

> „IMPLEMENTAREA GDPR ESTE O OPORTUNITATE PENTRU A SECURIZA NU DOAR DATELE CU CARACTER PERSONAL, CI TOATE DATELE SENSIBILE PE CARE LE DEȚINE O COMPANIE".
>
> **BOGDAN TUDOR, CEO STARTECH TEAM**

GDPR ADUCE PLUSURI PE PIAȚA SERVICIILOR DE SECURITATE IT

Atacurile cibernetice au devenit tot mai sofisticate și mai greu de detectat, crede Doru Manea, CEO al Netsafe, distribuitor de soluții și produse IT cu valoare adăugată pe segmentele de security, networking și wireless. La nivel global, în medie, impactul financiar al unei breșe de securitate a depășit în 2016 4 milioane de dolari, valoare în creștere cu 29% față de 2013. „Mai alarmant este timpul care se scurge până la descoperirea breșei de securitate: în medie, peste 200 de zile, la care se

adaugă o altă perioadă de 70 de zile până la izolarea și rezolvarea acesteia. Soluțiile de securitate au devenit mai complexe și vizează companiile în întregul lor, indiferent că vorbim despre angajați și obiceiurile acestora de utilizare a internetului sau a tehnologiei, despre echipamentele pe care le folosesc sau infrastructura la care sunt conectate", spune Manca. „Provocarea este creșterea nivelului de conștientizare a riscurilor la care se expun companiile, utilizatorii individuali, angajații dacă nu își iau măsuri de protecție împotriva atacurilor cibernetice. În România, principalii investitori în soluții de securitate și infrastructură IT sunt companiile mari din domeniile IT, financiar-bancar, telecomunicații, sănătate, producție și agricultură. Aceste companii conștientizează riscurile la care se expun și iau măsuri pentru a limita atacurile cibernetice. Pe de altă parte, însă, la polul opus se află IMM-urile, care au rămas vulnerabile în fața atacatorilor și care devin ținta hackerilor; scăpările de securitate ale acestora sunt o modalitate prin care infractorii cibernetici pot accesa contracte, listele de contacte sau informațiile legate de conturi."

Doru Manea crede că numărul incidentelor va scădea pe termen lung, dar și că tehnologia nu este întotdeauna suficientă pentru a fi protejați în fața atacurilor și ingeniozității infractorilor cibernetici. Astfel, în ciuda creșterii investițiilor în soluții de securitate IT, companiile rămân vulnerabile, angajații acestora, prin comportament și naivitate, fiind principala slăbiciune. „Aș putea adăuga că firmele ar trebui să investească, în principal, în tehnologii de protecție zero day care, chiar dacă nu cunosc sursa atacului, fac o analiză a traficului în rețea, anticipează eventualele atacuri și le blochează în fază incipientă. De asemenea, în contextul intrării în vigoare a noului Regulament privind Protecția Datelor cu Caracter Personal (GDPR), fiecare companie ar trebui să aibă un sistem de tip SIEM (Security Information and Event Management) care agregă toate alertele de la toate echipamentele din rețea, corelează evenimentele din rețea într-un singur punct și le administrează în consecință", remarcă Doru Manea.

„CHIAR ȘI O COMPANIE DE MICI DIMENSIUNI, CU ȘASE ANGAJAȚI, VA TREBUI SĂ ADOPTE O SERIE DE POLITICI DE SECURITATE PENTRU DATELE PE CARE LE PROCESEAZĂ."

GABRIEL GÎDEA, DIRECTOR DE DEZVOLTARE, KINGSTON TECHNOLOGY ROMÂNIA ȘI BULGARIA

Cheltuielile cu implementarea normelor GDPR vor fi diferite în funcție de sectorul de activitate și de complexitatea activităților desfășurate, fiind vizate aducerea site-ului și a sistemelor interne în conformitate cu regulamentul, prelucrarea datelor angajaților, a datelor clienților în scopuri de marketing, a datelor sensibile ale unor clienți (referitoare la sănătate, cazier fiscal/judiciar) sau a vânzărilor online, arată un studiu al Consiliului Național al Întreprinderilor Private Mici și Mijlocii din România (CNIPMMR). Potrivit studiului „The Economic Costs of the European Union's Cookie Notification Policy" din 2014, politica de notificare a vizitatorilor asupra folosirii cookie-urilor (cea pe care Regulamentul general privind protecția datelor vine să o înlocuiască) genera o cheltuială anuală de peste 2 miliarde de euro în cadrul Uniunii Europene. Costul investit în aducerea site-ului și a sistemelor interne în conformitate cu reglementările în vigoare fusese atunci estimat la 900 de euro/site, sumă ce poate fi un reper și în privința cerințelor Regulamentului general privind protecția datelor, notează același raport.

Ca urmare a creșterii investițiilor din partea companiilor, în contextul numărului tot mai mare de incidente de securitate IT, dar și ca urmare a intrării în vigoare, în luna mai a prevederilor GDPR, Netsafe estimează că segmentul pieței de securitate IT va înregistra o creștere importantă. „Companiile au început deja să se intereseze cu privire la cerințele de securitate IT pe care trebuie să le respecte conform GDPR. În acest context, va urma, cu siguranță, o creștere de cel puțin 30% a pieței de profil, pe segmentul de soluții de securitate IT clasice, pentru că toate companiile vor avea nevoie de sisteme de raportare, securitate și vizibilitate a rețelelor IT", spune Doru Manea, CEO al NetSafe.

Companiile din România stau destul de bine în ceea ce privește protecția datelor față de atacatori externi, dacă ar fi să judecăm după numărul de scurgeri de informații personale raportate de media, crede Bogdan Botezatu, senior cybersecurity analyst în cadrul Bitdefender. „E greu de spus dacă aceste breșe nu se întâmplă, deoarece nu există încă obligativitatea raportării scurgerilor de informații. Cu toate că nu există raportări clare, felul în care companiile colectează informații și felul în care le folosesc lasă de dorit. De exemplu, foarte multe companii colectează informații mult peste ce e cu adevărat necesar pentru oferirea unui serviciu. Altele deturnează scopul informației colectate pentru a promova servicii și oferte sau pentru alte activități de marketing." Un exemplu bun în acest sens îl reprezintă mesajele comerciale trimise prin SMS de diverse companii fără a avea acordul pentru astfel de comunicări, subliniază el.

Bogdan Botezatu crede că introducerea GDPR era necesară, în condițiile în care atacurile cibernetice au început să își facă simțită prezența la nivel global încă din 2007, cu cinci ani înainte ca Parlamentul European să facă primele demersuri în vederea implementării unei legi universale de protejare a datelor. Momentele cheie care au marcat evoluția criminalității cibernetice au fost breșele de securitate suferite de TJ Maxx în SUA (94 de milioane de clienți afectați), T-Mobile în Germania (17 milioane de clienți afectați) sau UK Revenue and Customs (25 de milioane de clienți afectați). Toate aceste breșe, remarcă el, survin din neglijența cu care au fost tratate datele (stocare improprie sau acces discreționar la acestea în interiorul companiei) și ar fi putut fi prevenite cu un set de reguli stricte, precum cele stabilite prin GDPR. „Din nefericire, de atunci și până în prezent nu s-au văzut îmbunătățiri. Noile atacuri informatice sunt mult mai agresive și compromit din ce în ce mai mulți utilizatori: River City Media (1,37 miliarde de clienți expuși), Friend Finder Network (412 milioane de clienți expuși) sau Aadhaar (peste un miliard de clienți expuși) sunt doar câteva exemple. GDPR vine «la pachet» cu amenzi usturătoare în caz de nonconformitate. Acest aspect, printre multe altele, face ca protejarea datelor cu caracter personal să devină nu doar importantă, ci imperativă pentru orice business care se ocupă de colectarea și / sau procesarea datelor cu caracter personal. O astfel de amendă poate afecta grav o afacere mică sau mijlocie, însă la fel putem spune și despre o breșă. Astfel, începând cu 25 mai, riscurile de a nu fi în acord cu GDPR devin relativ egale cu riscurile asociate unui atac", afirmă Botezatu.

Indiferent de industria în care activează compania sau de cât de mare este businessul, toți colectorii și procesatorii de date sunt nevoiți să implementeze nu doar politici noi de securitate, ci și să efectueze traininguri și, în unele cazuri, să achiziționeze tehnologii noi, atât pentru a adăuga straturi noi de protecție în vederea protejării informației, cât și pentru a face dovada conformității cu GDPR – aceasta din urmă fiind o cerință cheie, explică analistul de la Bitdefender. „Scopul principal al implementării GDPR este tocmai acesta – să se reducă considerabil riscul ca datele cu caracter personal ale cetățenilor Uniunii Europene să ajungă în mâinile răufăcătorilor. Nu numai că cetățenii UE pot «păși» mai liniștiți pe internet ca urmare a implementării legii, dar ne putem aștepta ca și riscurile asociate cu atacuri finanțate de actori statali să scadă", opinează Bogdan Botezatu.

Bogdan Tudor, CEO-ul Startech Team, este însă de altă părere: „Din păcate, companiile locale sunt foarte slab pregătite să facă față amenințărilor informatice. Provocările mediului de afaceri la noi sunt încă concentrate pe nevoile de bază cum ar fi lipsa infrastructurii, ceea ce este o greșeală. Într-o lume în schimbare în care digitalizarea afacerilor va transforma industrii întregi este cel mai bun moment să ne concentrăm pe a exploata această oportunitate. Mai devreme sau mai târziu se vor face autostrăzi în România; beneficiem acum de unele din cele mai rapide autostrăzi informaționale prin viteză și calitatea internetului – e un lucru de care toate afacerile ar trebui să profite acum. Întregi industrii se redefinesc folosind tehnologia și cea mai bună investiție pe care o poate face o companie acum este în digitalizare și, evident, în asigurarea protecției sistemelor pe care se bazează afacerea ta."

Pe fondul progresului tehnologic înregistrat în ultimii ani, se poate observa și o creștere a gradului de complexitate a amenințărilor cibernetice, care pot avea impact asupra unui număr tot mai mare de utilizatori; în acest context, o standardizare a măsurilor de securizare a datelor este binevenită, crede Gabriel Gîdea, director de dezvoltare la Kingston Technology România și Bulgaria. „Mă aștept ca politicile de securitate să devină mai consistente; se vor lua măsuri extinse pentru alinierea la standardele prevăzute în GDPR, începând de la cele mai mari companii și până la IMM-uri. Chiar și o companie de mici dimensiuni, cu șase angajați, va trebui să adopte o serie de politici de securitate pentru datele pe care le procesează. Companiile de mari dimensiuni aveau deja un anumit set de reguli implementat, doar că acestea vor fi ajustate, aliniate cu GDPR și implementate mai riguros."

Corporațiile își vor crea sau consolida departamente de tip Security Office, ceea ce poate duce la apariția de noi joburi, datorită GDPR, este de părere Gîdea. „Chief information security officer-ul va fi principalul responsabil în ceea ce privește securitatea datelor pe care compania le procesează. Stickurile USB cu criptare sunt una din principalele soluții de securitate, în special pentru companiile medii și cele de mici dimensiuni, dar, bineînțeles, și în companii

de mari dimensiuni ar prezenta avantaje majore implementarea unei politici de securizare prin utilizarea de stickuri cu criptare." O astfel de politică de securizare ar crea un mediu de lucru flexibil, crede directorul de dezvoltare de la Kingston, spre deosebire de alternativa de a bloca toate posturile USB din companie în încercarea pentru a evita complet transferul de date pe stickuri USB sau medii externe. Cabinetele de avocatură, cabinetele medicale, cu cinci - șase angajați, IMM-urile sunt exemple de companii care pot beneficia de avantajele criptării hardware disponibile pe stickuri USB.

Companiile fac constant eforturi pentru a se proteja de atacurile cibernetice, pe măsură ce tehnologia evoluează, dar, în același timp, atacurile devin din ce în ce mai complexe și mai greu de evitat. Cu toate acestea, companiile românești sunt din ce în ce mai pregătite, fiind și forțate să facă progrese, din cauza gradului de complexitate tot mai ridicat al atacurilor, crede Gabriel Gîdea. Companiile care nu își protejează datele corespunzător riscă nu numai pierderi cauzate direct de eventuale răscumpărări solicitate de atacatori, ci și pierderi cauzate de amenzi. „Dialogul pe tema GDPR este mai intens comparativ cu anul trecut, când 70% dintre oameni nu auziseră de acest subiect; astăzi, probabil că mai sunt 20-30% care nu sunt familiarizați cu directiva europeană. Remarc o evoluție în nivelul de conștientizare, dar e loc de progres la capitolul implementare. Cred că în prima fază nu vom remarca o scădere semnificativă a numărului incidentelor. Mă aștept și ca alinierea la prevederile GDPR să nu se facă din prima zi, adică începând cu 26 mai. Vorbim de un proces de durată; observ că tot mai multe companii se străduiesc să se alinieze la prevederi pe ultima sută de metri. Însă pe termen mediu și lung am încredere că GDPR va avea un impact pozitiv în acest sens", concluzionează el. GDPR nu este însă singura schimbare de anul acesta: directiva UE privind Securitatea Rețelelor și a Sistemelor Informatice (directiva NIS), care urmărește să sporească rezistența cibernetică, intră de asemenea în vigoare în mai 2018. Organizațiile identificate de statele membre ca operatori de servicii esențiale (infrastructură critică), precum și furnizorii de servicii digitale (motoare de căutare, servicii de cloud computing și piețe online), se confruntă cu noi cerințe în temeiul directivei în materie de securitate și de raportare a incidentelor la autoritățile naționale. Ca și în cazul GDPR, companiile ar putea suferi consecințe grave în cazul neconformării, arată studiul PwC Global State of Security Survey (GSISS) pe anul 2018. „Directorii executivi ar trebui să vadă Directiva GDPR și Directiva NIS nu doar ca exerciții de asigurare a conformității, ci mai degrabă drept oportunități strategice de a-și adapta afacerea într-o lume a datelor. În plus, companiile ar trebui să se adreseze autorităților de reglementare pentru a construi relații și linii de comunicare înainte de a ajunge la termenele limită de conformitate", notează în raport Manuela Guia, partener la D&B David și Baias, liderul echipei de servicii juridice de conformitate și protecție a datelor.

Europa și-a dat seama târziu că datele cetățenilor europeni sunt folosite fără niciun cadru legal, ba chiar sunt exploatate pentru profit, în special de către companiile de peste ocean, și încearcă în al 12-lea ceas să repare această problemă, opinează Bogdan Tudor. Tot el conchide: „Deși legea este adresată giganților Facebook, Google sau Apple, din păcate acest lucru creează costuri suplimentare, în special pentru companiile din Uniunea Europeană. Lumea nu a început și nici nu se va termina odată cu GDPR, așa cum încearcă să sugereze o parte din consultanții în GDPR, apăruți ca ciupercile după ploaie, și în special cei care nu au altă activitate de bază și încearcă să profite de această oportunitate".

„NU NUMAI CĂ CETĂȚENII UE POT «PĂȘI» MAI LINIȘTIȚI PE INTERNET CA URMARE A IMPLEMENTĂRII LEGII, DAR NE PUTEM AȘTEPTA CA ȘI RISCURILE ASOCIATE CU ATACURI FINANȚATE DE ACTORI STATALI SĂ SCADĂ."

BOGDAN BOTEZATU, SENIOR CYBERSECURITY ANALYST, BITDEFENDER