Organizațiile nu asigură măsuri suficiente pentru protejarea confidențialității datelor

Investițiile în soluții avansate de autentificare și criptare vor crește în 2018

- *Numai 51% dintre directorii executivi au un inventar precis al datelor personale ale angajaților și clienților;*
- *53% efectuează audituri de conformitate ale terțelor părți care gestionează date despre clienți și angajați;*
- *48% spun că soluțiile de autentificare avansată au contribuit la reducerea fraudei; 46% intenționează să mărească investițiile în acest domeniu în 2018;*
- *Doar 31% spun că consiliul director se implică direct în analiza riscurilor curente de securitate și confidențialitate;*
- *32% dintre respondenți au început evaluarea de conformitate cu GDPR în 2017.*

În societatea de astăzi, bazată pe date, concepte precum confidențialitatea, securitatea și încrederea sunt vitale și mai interconectate ca oricând. Cu toate acestea, multe organizații nu iau toate măsurile necesare pentru a proteja confidențialitatea datelor, potrivit celor mai recente concluzii publicate în studiul PwC Global State of Security Survey (GSISS) pe anul 2018.

Mai puțin de jumătate dintre respondenți (49%) declară că organizația lor limitează colectarea, păstrarea și accesarea informațiilor personale la minimul necesar pentru a îndeplini scopul legitim pentru care sunt colectate. Doar 51% dintre

respondenți au un inventar precis cu privire la modul în care datele personale ale angajaților și clienților sunt colectate, transmise și stocate. Și doar 53% solicită angajaților să urmeze o instruire în domeniul politicii și practicilor de protecție a datelor personale.

În ceea ce privește terțele părți care gestionează datele personale ale clienților și angajaților, mai puțin de jumătate (46%) dintre aceștia efectuează audituri de conformitate pentru a se asigura că au capacitatea de a proteja astfel de informații. Un număr similar (46%) declară că organizația lor le cere terților să respecte politicile de confidențialitate.

Sondajul se bazează pe răspunsurile a 9.500 de oameni de afaceri și directori de tehnologie din 122 de țări.

"*Noile modalități în care datele personale, și nu doar acestea, pot fi folosite, deschid calea către mai multe oportunități, dar și mai multe riscuri. Sunt puține companii care integrează managementul riscurilor cibernetice și de confidențialitate în strategia lor de transformare digitală. Înțelegerea celor mai frecvente riscuri, inclusiv lipsa conștientizării în privința activităților de colectare și de păstrare a datelor, reprezintă un punct de pornire pentru dezvoltarea unui cadru de guvernanță a utilizării datelor*", a declarat **Mircea Bozga, Partener, Liderul Echipei de Servicii de Risk Assurance, PwC România**.

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 și în implementarea practicilor de guvernanță a utilizării datelor, conform rezultatelor GSISS pe anul 2018 (vezi tabelul de mai jos).

	Strategie generală privind securitatea informațiilor	Solicită instruirea angajaților privind confidențialitatea	Au un inventar precis al datelor cu caracter personal	Limitează colectarea, reținerea și accesul la date	Auditează asigurarea conformității de către terți	Solicită asigurarea conformității de către terți
America de Nord	59%	58%	53%	53%	47%	47%
Asia	59%	57%	55%	53%	49%	47%
America de Sud	54%	50%	52%	47%	50%	50%
Europa	52%	47%	47%	44%	42%	44%
Orientul Mijlociu	31%	29%	20%	19%	26%	26%

Miza este mare – și există loc pentru îmbunătățire

Directorii generali sunt conștienți de mizele tot mai mari ale insecurității cibernetice. În cadrul celui de-al XXI-lea raport global PwC CEO Survey, amenințările cibernetice au intrat în top cinci amenințări la adresa dezvoltării pentru al treilea an la rând. 40% dintre directorii executivi recunosc că sunt extrem de îngrijorați de acest lucru, față de 25% anul trecut.

Există totuși motive să fim optimiști. 87% dintre executivii la nivel global declară că investesc în securitatea informatică pentru a construi încrederea în relațiile cu clienții. Aproape la fel de mulți (81%) spun că iau măsuri pentru a crește transparența privind utilizarea și stocarea datelor. Dar mai puțin de jumătate spun că iau aceste acțiuni "pe o scară largă". Și mai îngrijorător este faptul că mai puțin de o treime dintre executivii din Africa și aproape un sfert dintre cei din America de Nord (22%) declară că nu iau nicio măsură pentru a crește transparența privind utilizarea și stocarea datelor.

Importanța construirii încrederii

Consumatorii au o încredere relativ scăzută în companii că acestea vor utiliza datele cu caracter personal într-o manieră

responsabilă. În SUA, de exemplu, numai 25% dintre consumatori sunt de părere că majoritatea companiilor gestionează datele personale sensibile în mod responsabil (conform sondajului PwC din 2017 US Consumer Intelligence Series).

PwC se așteaptă ca îmbunătățirile la nivelul tehnologiilor de autentificare, printre care identificarea biometrică și criptarea datelor, vor ajuta din ce în ce mai mult companiile să construiască rețele de încredere.

Jumătate dintre respondenți declară că utilizarea autentificării avansate a îmbunătățit încrederea clienților și a partenerilor de afaceri în capacitatea organizației de a asigura securitate și confidențialitate datelor. De asemenea, 48% spun că autentificarea avansată a contribuit la reducerea fraudei și 41% spun că a îmbunătățit experiența clienților. În plus, 46% declară că intenționează să stimuleze investițiile în tehnologiile biometrice și de autentificare avansată în acest an.

Cu toate acestea, utilizarea tehnologiilor biometrice este vulnerabilă în fața reglementărilor în materie de confidențialitate și nivelului de încredere general, deoarece este strâns corelată cu nevoia organizațiilor de a urmări informațiile biometrice. Având în vedere că autentificarea se bazează pe obținerea unor informații – atunci când utilizatorii furnizează, de exemplu, numele de domnișoară al mamei – o organizație ar putea deveni vulnerabilă la atac dacă această informație este furată printr-o breșă de securitate.

De asemenea, experții PwC se așteaptă la o presiune sporită asupra metodelor de criptare a datelor în vederea asigurării securității acestora, ceea ce va conduce la investiții conexe în domeniu. Printre respondenții din sectorul financiar, 46% declară că intenționează să majoreze investițiile în criptare în acest an.

Securitatea datelor: o problemă pe agenda consiliul director

Mai puțin de o treime (31%) dintre respondenții sondajului GSISS 2018 declară că consiliul director se implică direct în analiza riscurilor curente privind securitatea și confidențialitatea. Pentru organizațiile cu o valoare de peste 25 de miliarde de dolari, cifra este doar puțin mai mare (36%).

"*Organizațiile de toate dimensiunile ar trebui să stimuleze implicarea consiliilor de administrație în supravegherea gestionării riscurilor cibernetice și celor asociate informațiilor confidențiale. Fără o înțelegere solidă a riscurilor, consiliile nu își pot exercita în mod corespunzător responsabilitățile de supraveghere a protecției datelor și asigurarea confidențialității*", a adăugat **Mircea Bozga**.

Cum să privim GDPR și NIS ca o oportunitate

Regulamentul UE privind Protecția Generală a Datelor (GDPR), care se aplică oricărei organizații care își desfășoară activitatea în spațiul UE, va intra în vigoare în mai 2018. O parte dintre respondenții GISS 2018 din întreaga lume spun că au luat unele măsuri în vederea pregătirii pentru GDPR încă din prima jumătate a anului 2017, cu un an înaintea termenului limită de conformitate. Aproximativ o treime dintre respondenți (32%) au început de exemplu, evaluarea GDPR, iar acest procent a fost puțin mai mare în Asia (37%) decât în alte părți.

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.

“*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 pentru succes, 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*“, a declarat **Manuela Guia, Partener, D&B David și Baias**, liderul echipei de servicii juridice de conformitate și protecție a datelor.

Despre raport:

1. *Global State of Information Security® Survey 2018* este un studiu la nivel mondial realizat de PwC, CIO și CSO. A fost efectuat online, în perioada 24 aprilie 2017 – 26 mai 2017.
2. Sondajul se bazează pe răspunsurile a peste 9.500 de directori executivi și IT, inclusiv CEOs, CFOs, CISOs, CIOs, OSCs, vicepreședinți și directori de IT și securitate informatică, din 122 de țări. 38% dintre respondenți au fost din America de Nord, 29% din Europa, 18% din Asia Pacific, 14% din America de Sud și 1% din Orientul Mijlociu și Africa.
3. Noul raport poate fi descărcat aici: https://www.pwc.com/us/gsissprivacy