Comunicat de presă

Data	29 mai 2017
Contact	Mihnea Anastasiu Media Relations Manager Tel: +40 21 225 3546 Email: mihnea.anastasiu@ro.pwc.com

Investiţiile în securitatea informatică sunt impulsionate în principal de cerinţele de reglementare, în loc de conştientizarea la nivelul organizaţiilor a ameninţărilor IT, arată un sondaj efectuat de PwC România şi Microsoft România

Potrivit unui sondaj realizat în comun de PwC România şi Microsoft România, lansat astăzi, *„Security in the Digital World" şi derulat în intervalul martie- aprilie 2017,* investiţiile în securitatea informatică sunt impulsionate în principal de cerinţele de reglementare şi într-o măsură mai mică de conştientizarea la nivelul organizaţiilor a ameninţărilor de securitate cibernetică. În schimb, companiile care sunt active pe pieţe puternic reglementate, aşa cum este sectorul financiar spre exemplu, sunt de obicei mai bine pregătite pentru a face faţă unor ameninţări cibernetice.

Aproape 60% dintre companiile intervievate aveau în plan să majoreze bugetul de securitate informatică în următorul an financiar, iar 20% mizau pe menţinerea bugetului la nivelul actual, în vreme ce 23% dintre companii nu aveau încă o idee clară despre bugetul viitor.

Având în vedere că 40% dintre companiile româneşti intervievate au arătat că nu au o strategie de securitate informatică formal adoptată, în vreme ce doar 10% au atins nivelul necesar de maturitate organizaţională în care strategia este definită, implementată şi optimizată, sondajul arată că securitatea informatică este un subiect încă nu pe deplin înţeles şi susţinut la nivelul Consiliilor de Administraţie ale companiilor.

„Directorul de securitate informatică pare că nu este auzit la nivelul Consiliilor de Administraţie, cu excepţia situaţiilor în care organizaţia se confruntă cu o criză sau cu o reglementare legislativă în domeniu. Aceştia au nevoie de mai mult sprijin, inclusiv prin angajarea mai multor resurse sau servicii de securitate informatică din partea unor furnizori specializaţi, având în vedere că, în prezent, tehnologia este un subiect care priveşte întreaga organizaţie, iar riscurile de securitate informatică sunt de fapt riscuri pentru întreaga afacere", a declarat Mircea Bozga, Partener, Servicii de Risk Assurance, PwC România.

Expertiza de securitate informatică este de asemenea limitată, ca urmare a faptului că organizaţiile din România se bazează în continuare preponderent pe resursele interne, inerent limitate. Acest lucru este o caracteristică a pieţelor emergente, în vreme ce organizaţiile mai mature din economiile dezvoltate se bazează mai mult pe furnizori specializaţi de servicii de securitate informatică. Pe măsură ce companiile din România se dezvoltă şi se confruntă cu ameninţări de securitate informatică din ce în ce mai sofisticate, precum şi cu cerinţe de reglementare din ce în ce mai stricte, este probabil să vedem tot mai multe companii să adreseze aceste provocări apelând la serviciile unor firme specializate de securitate informatică, sau să exploreze beneficiile oferite de serviciile de cloud computing.

În ceea ce priveşte provocările de securitate informatică, 87% dintre respondenţi au declarat că sunt preocupaţi de scurgerile de date, 73% sunt îngrijoraţi de atacurile de tip malware (inclusiv ransomware), 70% de potenţialele întreruperi ale activităţii companiei ca urmare a unor incidente de securitate informatică, iar 70% sunt preocupaţi să asigure protecţia organizaţiei de atacurile ţintite.

„Cu mai puţin de 1 an până la intrarea în vigoare a Directivei Europene pentru Protecţia Datelor (GDPR), aceasta a început să devină o preocupare pentru companiile locale. Cu toate acestea, foarte puţini respondenţi au creat deja un plan de acţiune în ceea ce priveşte conformarea cu cerinţele GDPR", a declarat Oana Terteleac, Digital Sales Incubation Unit Lead Microsoft Romania.

În privinţa factorilor care pot avea un impact pozitiv asupra securităţii informatice a organizaţiilor, marea majoritate a respondenţilor s-a concentrat pe creşterea nivelului de conştientizare în rândul angajaţilor în privinţa ameninţărilor informatice (inclusiv prin programe de training), şi de asemenea pe creşterea nivelul de înţelegere şi de sprijin al consiliilor de administraţie pentru îmbunătăţirea securităţii informatice. Un alt factor pozitiv este considerat aplicarea cerinţelor cadrului de reglementare specific (77%). Acest lucru ar putea să reflecte cerinţele de reglementare tot mai stricte cu care se confruntă organizaţiile, îndeosebi pe pieţele puternic reglementate.

Nevoia de a angaja resurse adiţionale (67%) şi de a face schimb de informaţii şi de bune practici cu alţi jucători din domeniu (57%) au fost de asemenea invocate de către o bună parte dintre respondenţi ca fiind factori importanţi sau foarte importanţi pentru îmbunătăţirea securităţii informatice. Acest lucru pare să reflecte faptul că echipele de securitate informatică din companiile româneşti se confruntă cu un deficit de personal specializat, precum şi speranţa că se poate învăţa din experienţa altor organizaţii.

În privinţa infrastructurii de securitate informatică, se disting 3 zone prioritare pentru respondenţi, cu accent pe data backup şi data recovery, DLP şi IAM.

Cei mai mulţi respondenţi ar prefera să investească în sisteme de data backup şi data recovery (20%), în îmbunătăţirea accesului pentru sistemele de management al accesului la reţelele informatice (19%), în soluţii de prevenţie a scurgerilor de date (16%). Acest lucru poate să reflecte preferinţa respondenţilor de a investi în domenii care au un impact major şi rapid în situaţia lor de securitate informatică, sistemul de protecţie şi acces la date.

Mai bine de două treimi dintre respondenţi folosesc o soluţie de Data Loss Prevention (DLP), iar acest lucru arată că DLP a devenit o măsură standard de securitate informatică, similară sistemelor antivirus. Pe de altă parte, aproape o cincime dintre respondenţi au indicat că nu folosesc o soluţie DLP. O posibilă explicaţie pentru acest lucru poate să fie lipsa unei politici interne de securizare a informaţiei.

O provocare care concentrează interesul respondenţilor este modul în care companiile adresează controlul accesului la reţele. În întreaga organizaţie, gestionarea identităţilor şi controlul accesului la reţea încurajează tot mai multe companii să implementeze soluţii de Identity Access Management « IAM », aproape două treimi dintre respondenţi precizând că au implementat sau intenţionează să implementeze astfel de soluţii pentru a gestiona accesul la reţelele informatice în întregul „ecosistem" tehnologic.

Pentru a-şi îmbunătăţi securitatea informatică, PwC şi Microsoft recomandă organizaţiilor luarea în considerare a următoarelor măsuri:

- **Să aibă resurse adecvate (personal specializat, folosind tehnologia adecvată şi acţionând conform unor procese validate) cât şi tehnologie şi procese testate) care să raporteze Directorului de Securitate Informatică (CISO – Chief Information Security Officer)**. Acest CISO ar trebui să raporteze direct Consiliului de Administraţie sau unuia dintre membrii Consiliului de Administraţie.
- **Să deruleze evaluări periodice ale riscurilor şi vulnerabilităţilor de securitate informatică, inclusiv ale strategiei de securitate informatică**, folosind furnizori independenţi specializaţi.

- **Să facă o evaluare atentă a serviciilor de cloud computing** pentru a identifica beneficiile potenţiale de securitate, confidenţialitate şi conformitate cu standardele legale şi recomăndările cele mai actuale.
- **Să investească în trainingul angajaţilor şi în programe de informare a acestora în privinţa riscurilor de securitate informatică.** Acest lucru este un factor crucial în orice program de securitate IT.
- **Să existe un plan robust de continuitate a activităţii companiei şi exerciţii periodice –** pentru a se asigura că sistemele şi serverele cheie pot fi repornite rapid folosind back-up-uri, iar frecvenţa acestor procese de back-up să fie aliniată volumului de date pe care organizaţia dumneavoastră este pregătită să-l piardă în cazul în care un sistem devine inutilizabil.
- **Să existe un plan de criză şi de răspuns la incidentele de securitate informatică –** asigurându-se că există proceduri standard prin care angajaţii şi cei responsabili de gestionarea incidentelor critice sunt pregătiţi să implementeze reacţia standard a organizaţiei la evenimente neprevăzute şi să repornească în cel mai scurt timp activitatea, atât pentru angajaţi, cât şi pentru clienţi.
- **Politici puternice de „igienă" a securităţii informatice şi de creştere a gradului de conştientizare al angajaţilor -** prevenirea atacurilor de tip malware care pot afecta sistemul IT prin cel mai frecvent instrument de răspândire, atacurile de tip phishing, prin adoptarea unor reglementări stricte a sistemelor de e-mail şi prin alertarea angajaţilor prin campanii de conştientizare şi informare.
- **Un management riguros şi robust al update-**urilor programelor software (patch-uri şi versiuni actuale) pentru a reduce posibilitatea utilizării unor vulnerabilităţi.

Despre sondaj

Raportul "Security in the Digital World" a fost realizat de echipa de securitate informatică a PwC la cererea Microsoft România. Sondajul se bazează pe răspunsurile venite din partea a 30 de companii active în România au fost colectate în perioada martie-aprilie 2017. 76% dintre companiile respondente au mai mult de 500 de angajaţi.

Despre Microsoft

Fondată în 1975, compania Microsoft (NASDAQ "MSFT") este liderul mondial în software, servicii şi soluţii ce ajută oamenii şi companiile să îşi atingă pe deplin potenţialul.

În România, Microsoft şi cei peste 3.000 de parteneri comerciali locali oferă companiilor un set bogat de soluţii de mobilitate şi creştere a eficienţei în afaceri. Totodată, firmele mici şi mijlocii au la dispoziţie un serviciu de contact specializat la Microsoft România pentru informaţii suplimentare şi consultanţă (021 529 7174), iar pe www.microsoft.ro/studiidecaz sunt disponibile exemple de companii româneşti care folosesc soluţii de mobilitate şi cloud pentru a-şi creşte competitivitatea

Despre PwC

Scopul PwC este de a construi încredere în sânul societăţii şi de a contribui la rezolvarea unor probleme importante. Firmele din reţeaua PwC ajută organizaţiile şi indivizii să creeze valoarea adăugată de care au nevoie. Suntem o reţea de firme prezentă în 157 de ţări cu mai mult de 223.000 de specialişti dedicaţi oferirii de servicii de calitate de audit, consultanţă fiscală şi consultanţă pentru afaceri. Spuneţi-ne care sunt lucrurile importante pentru dumneavoastră şi descoperiţi mai multe informaţii despre noi vizitând site-ul www.pwc.ro.