ABORDAREA CARE ȚINE DE BUNELE PRACTICI PUNE LA ADĂPOST ORGANIZAȚIILE

Riscurile tehnologiei informației, de la operațional la sistemic

Criminalitatea informatică ține de sistemele informatice? Majoritatea ar răspunde că da. Dar este un răspuns complet? În nici un caz. În industria financiară, riscurile generate de utilizarea sistemelor informatice sunt generate de oameni, care nu respectă procesele de lucru. La care se adaugă contribuția mediului extern, interconectarea din ce în ce mai puternică cu exteriorul, utilizarea canalelor alternative de tranzacționare, dematerializarea, externalizările informatice masive, de la dezvoltarea de software până la cloud-computing.

Călin M. Rangu
Director adjunct
Direcţia Supraveghere Integrată
Autoritatea de Supraveghere Financiară

La o întrebare generală despre riscurile generate de IT, multe firme se opresc în aspectele popularizate de presă – viruşi sau atacuri externe, din interior nefiind ameninţări, iar dacă sunt, ele sunt acoperite de contractele de confidenţialitate, eludând statisticile care prezintă că 80% dintre evenimentele de criminalitate informatică sunt generate de factori interni.

Dacă întrebi cum se realizează segregarea atribuţiilor la nivelul administratorilor de baze de date, dacă cei din IT au acces la datele clienţilor, dacă ar putea să le modifice, răspunsul este da, cei din IT trebuie să ştie tot deoarece ei fac totul. Iar dacă întrebi dacă acelaşi personal IT (în general unul, doi oameni) poate avea acces la logurile care înregistrează modificările realizate chiar de aceştia, după răspunsul primar că nu e posibil, la o discuţie mai detaliată, este foarte posibil.

Când li se sugerează că doar cei din business ar trebui să aibă acces la informaţiile clienţilor, pentru cei din IT aceste informaţii trebuind să fie inaccesibile, IT-ul ocupându-se cu parametrizarea şi administrarea sistemelor informatice, nu cu administrarea produselor de business şi nici a clienţilor, lucrurile încep să se contureze. Managementul începe să-şi pună întrebări. Iar când sistemele IT sunt administrate de personal extern, atât în zona de dezvoltare, cât şi în cea de administrare, lucrurile capătă o conotaţie periculoasă.

Astfel, datele, informaţiile circulă, ies în afară şi, la un moment dat, apar atacurile externe. Se ajunge în domeniul riscurilor potenţial sistemice, care pot crea riscuri reputaţionale şi legale majore, capabile să destabilizeze încrederea oamenilor în sistemul financiar, să ducă la afectarea unui sector sau, prin contagiune, la implicaţii asupra mai multor sectoare financiare. Dacă sunt afectate instituţii esenţiale, infrastructuri financiare critice, noduri esenţiale în funcţionarea pieţelor, cum sunt sistemele de plăţi, bursele de valori, depozitarii etc., riscurile devin cu adevărat sistemice.

Cum se poate preveni şi nu doar reacționa post-factum?

Destul de simplu, dacă ai o abordare care ţine de bunele practici. Trebuie stabilite şi documentate procesele de lucru esenţiale pentru a asigura un cadru de lucru care să controleze riscurile, să identifice vulnerabilităţile şi să susţină luarea de măsuri. Nimic nu e mai simplu decât o evaluare proprie, răspunsul la ce riscuri te expui şi ce procese trebuie să documentezi pentru a le diminua.

Dezvoltarea unui plan de creştere a maturităţii companiei durează ani, riscurile nu se diminuează brusc, dar îmbunătăţirile trebuie să fie continue şi controlate. Pentru a le controla, ai nevoie de obiective de control, puncte de control, măsurarea punctelor de control, indicatori de performanţă şi, în final, de indicatorii de risc care să te atenţioneze dacă ai ieşit din apetitul de risc pe care ţi l-ai stabilit pentru propria afacere.

Balanţa între riscuri şi măsuri şi-o stabileşte fiecare companie, dar în mod conştient şi voit, pe baze continue, iar indicatorii de risc sunt ca un sistem de avertizare timpurie că ceva nu mai funcţionează bine.

Lucrând cu mediul extern, managementul serviciilor externe trebuie să respecte cel puţin aceleaşi criterii ca şi cele interne, dar cu un plus prin profesionismul specializat al furnizorului extern, care să fie certificat în ceea ce face conform practicilor internaţionale. Furnizorilor externi trebuie să le fie cerute garanţiile minime care să asigure suportul IT necesar mai bine şi mai ieftin. De ce mai ieftin? La prima vedere, aplicarea de standarde implică nişte costuri. În realitate, aplicarea reală de standarde şi bune practici simplifică şi susţine economiile de scară şi duce la reducerea costurilor pe unitatea de serviciu sau produs oferit. Dacă un furnizor nu poate fi mai ieftin ca tine, în interiorul companiei, problema este la furnizor şi nu la client, iar riscul intern operaţional se multiplică în exterior, plecând de la ideea că externalizarea unei probleme interne nu rezolvă problema, ci o multiplică dacă furnizorul nu este pregătit, putând genera riscuri sistemice neaşteptate.