

Complexitatea inutila în companii poate deveni o tinta pentru atacurile cibernetice (studiu)

Trei sferturi dintre organizatii spun ca operatiunile lor de afaceri sunt foarte complexe, ceea ce implica riscuri ridicate de securitate cibernetica, arata cel mai recent raport Digital Trust Insights 2022, realizat de PwC la nivel global.

De aceea, consecintele unui atac cibernetic, precum pierderile financiare sau o revenire dificila la normal, sunt principalele temeri ale respondentilor cu privire la complexitatea modelelor de afaceri.

"Complexitatea nu este o problema în sine, fiind adesea un rezultat al dezvoltarii afacerii. Cu cât o organizatie este mai mare, cu atât va fi mai complexa, având nevoie de mai multi oameni si tehnologii pentru a servi o baza de clienti în crestere. Nu în ultimul rând, unele complexitati sunt necesare - cum ar fi cele impuse de cerintele de reglementare sau raportare, asigurarea sigurantei si a calitatii, managementul riscului, etc.", se mentioneaza într-un material semnat de Mircea Bozga, Partener servicii de audit al riscului PwC România.

Astfel, un proces de simplificare a activitatilor, a proceselor, a tehnologiei care le sustine, trebuie sa urmeze o strategie bine pusa la punct. "Dar din pacate costurile crearii unei complexitati inutile nu sunt evidente si de regula optimizarea proceselor nu este privita ca prioritate zilnica. Mai putin în cazul unui atac cibernetic", precizeaza cercetarea.

Potrivit raportului, datele par a fi principalul motiv de îngrijorare. Guvernanta datelor si infrastructura aferenta ocupa primul loc în topul domeniilor de complexitate "inutila si evitabila" din punct de vedere securitate, mai ales în rândul companiilor mari. Spre exemplu, pastrarea inutila a datelor sensibile ale persoanelor cu care o companie nu mai face afaceri - organizatia continua sa consume resurse pentru a le proteja deoarece ele pot o constitui o tinta pentru hackeri.

De asemenea, arhitectura IT a multor companii cuprind sisteme vechi si dificil de integrat. Iar presiunile asupra acestor structuri s-au intensificat pe masura ce companiile au vrut sa tina pasul cu nativii digitali, dar si din cauza pandemiei COVID-19, care a impus adoptarea rapida de solutii digitale noi, multe operate din afara organizatiei.

"Din aceasta perspectiva, lipsa integrarii solutiilor tehnologice, nerespectarea proceselor de gestionare a datelor sau asumarea riscurilor cu tertii fara a le cuantifica sau mitiga sunt obiceiuri nefericite astazi. Companiile dezvolta aceste obiceiuri în numele vitezei sau le accepta si le asimileaza din rezistenta la schimbare", mai arata studiul.

În schimb, companiile denumite "nativi digitali", care opereaza în întregime online, tind sa utilizeze cele mai noi tehnologii, care sunt concepute pentru a se conecta si a opera împreuna.

"Companiile cunosc riscurile complexitatii, dar cu toate aceste doar 35% dintre respondentii studiului au implementat o simplificare a operatiunilor lor si un sfert spun ca nu au facut nimic sau ca de acum încep sa puna în aplicare aceasta strategie.

Organizatiile au nevoie, în acest moment, de consolidarea aplicatiilor din tehnologie astfel încât sa nu mai fie vulnerabile în fata atacurilor cibernetice si au început sa fie tot mai atente la investitiile lor în tehnologie", se mai precizeaza în material.

De exemplu, folosirea serviciilor de cloud poate ajuta în simplificarea proceselor din cadrul afacerii si în simplificarea arhitecturii IT. De asemenea, o astfel de miscare ofera flexibilitate si poate accelera inovarea. Facute corect, transformarile digitale bazate pe cloud pot fi sigure, eficiente si de succes, securitatea în cloud fiind

principala prioritate de investitii a respondentilor la sondaj.

"Este de cinci ori mai probabil ca organizatiile care au obtinut cele mai bune rezultate în materie de securitate cibernetica în ultimii doi ani sa aiba operatiuni simplificate la nivelul companiei. Aceste organizatiile s-au concentrat pe consolidarea relatiei cu furnizorii de tehnologie, definirea sau realinierea mixului intern si a serviciilor gestionate, reorganizarea functiilor si modalitati de lucru si crearea unui cadru integrat de administrare a datelor.", mai sustin autorii studiului.

Global Digital Trust Insights 2022 a fost realizat în perioada iulie si august 2021 în rândul a 3.602 de directori generali, de tehnologie si securitate din industrii precum tehnologia, mass-media, telecomunicatii, productie industrială, servicii financiare, retail, energie, utilitati si energie, sanatate si servicii publice si guvernamentale.