PwC | Securitatea cibernetica a depaşit pandemia în topul îngrijorarilor CEO la nivel global. Ce industrii sunt ameninţate?

Aproape jumatate dintre directorii generali de la nivel global sunt foarte îngrijoraţi ca un potenţial atac cibernetic le va submina atingerea obiectivelor financiare şi de dezvoltare în urmatoarele 12 luni, riscurile de securitate cibernetica devansând anul acesta situaţia sanitara şi volatilitatea macroeconomica (inclusiv inflaţia, şomajul şi fluctuaţia PIB), arata cea de-a 25-a ediţie a *PwC CEO Survey 2022*.

Întrebaţi cum le pot impacta activitatea aceste riscuri, circa doua treimi dintre directorii generali intervievaţi cred ca le vor reduce vânzarile de produse şi servicii, iar 56% ca le vor afecta capacitatea de inovare. În acelaşi timp, 19% considera ca riscurile de securitate cibernetica îi pot împiedica sa atraga finanţari, iar 17% ca le vor afecta procesul de atragere şi retenţie a angajaţilor cheie.

Directorii generali din sectorul serviciilor financiare şi din cel de tehnologie, media şi telecomunicaţii sunt cei mai îngrijoraţi ca riscurile de securitate cibernetica le pot ameninţa atingerea obiectivelor companiilor pe care le conduc în urmatoarele 12 luni şi le plaseaza pe primul loc în top. În sectorul de sanatate, securitatea cibernetica ocupa locul secund pe lista preocuparilor, dupa criza globala de sanatate.

Este interesant însa faptul ca directorii executivi din sectoarele de producţie şi de consum au afişat niveluri mai scazute de îngrijorare cu privire la riscurile cibernetice (locul trei), în ciuda volumului ridicat de atacuri din aceste sectoare.

Rezultatele sondajului subliniaza înca o data intensificarea şi agresivitatea atacurilor cibernetice din ultimii doi ani de pandemie, care au generat pierderi exponenţial mai mari pentru companii decât în trecut.

Cum a aparut aceasta situaţie? Graba digitalizarii a crescut expunerea la riscuri

Ca reacţie la raspunsurile la COVID-19 şi la schimbarile comportamentale ulterioare, multe organizaţii au comprimat ani de transformare digitala în doar câteva luni, ceea le-a modificat profilul de risc în materie de securitate cibernetica.

Hackerii nu au pierdut timpul, exploatând la maxim vectorii noi de atac care au aparut odata cu creşterea numarului de conexiuni, dispozitive, aplicaţii şi date. Cel puţin jumatate dintre organizaţii la nivel global au raportat ca au fost ”lovite” de programe malware prin actualizari de software, atacuri asupra lanţului de aprovizionare cu software şi compromiterea e-mailurilor de afaceri.

De asemenea, cererile de ransomware - şi plaţile - sunt în creştere. Atacatorii cer de obicei o suma pentru a furniza o cheie digitala pentru a debloca fişierele şi serverele pe care le-au criptat şi o rascumparare separata pentru a nu distribui datele pe care le-au furat. În 2020, cea mai mare rascumparare se dublase faţa de anul anterior, ajungând la 10 milioane de dolari, record doborât rapid în martie 2021, când a ajuns 40 de milioane de dolari.

În aceste condiţii, este esenţial ca obiectivele de afaceri sa includa şi strategii de securitate cibernetica, iar unele organizaţii au început sa dezvolte proiecte de ”companii securizate”. Acestea se concentreaza pe stabilirea securitaţii şi a confidenţialitaţii ca obiective esenţiale operaţionale şi de afaceri, pe angajarea unui responsabil principal cu securitatea informaţiilor, pe împuternicirea acestei persoane pentru a crea echipe interfuncţionale, pe includerea securitaţii cibernetice în alte decizii cheie, cum ar fi achiziţiile şi lansarile de produse şi pe reducerea complexitaţii prin masuri precum consolidarea furnizorilor, pentru a minimiza vulnerabilitaţile.