# Noua din zece organizatii au raportat, în 2022, cel putin un incident sau o bresa de securitate cibernetica (studiu)

**Noua din zece organizatii (91%) au raportat cel putin un incident sau o bresa de securitate cibernetica anul trecut si mai mult de o treime (38%) între sase si zece evenimente, potrivit studiului Deloitte 2023 Global Future of Cyber.**

Conform unui comunicat remis, marti, AGERPRES, studiul mai arata ca frecventa incidentelor de acest gen variaza în functie de nivelul de maturitate cibernetica, organizatiile cu maturitate cibernetica mai scazuta confruntându-se cu peste zece evenimente (21%) comparativ cu cele mature (13%).

Preocuparile de natura cibernetica ale organizatiilor difera, de asemenea, în functie de nivelul acestora de maturitate, cele mai avansate fiind îngrijorate în principal de infractorii si teroristii cibernetici, precum si de atacurile de tip phishing, malware si ransomware, în timp ce companiile cu maturitate scazuta si medie sunt mai preocupate de atacurile de tip denial-of-service, initiate cu scopul de a restrictiona în mod intentionat retelele, website-ul si resursele online ale unei companii.

În contextul acestor incidente, perturbarea operationala (58%) este principalul impact resimtit de organizatii, urmata de pierderea veniturilor, a încrederii clientilor si de impactul negativ asupra marcii, 56% dintre respondenti mentionând ca au avut parte de astfel de efecte într-o masura moderata sau mare.

"Amenintarile cibernetice devin din ce în ce mai complexe în fiecare an si variaza de la atacuri de tip ransomware, considerate în continuare una dintre principalele amenintari, potrivit agentiei UE pentru securitate cibernetica ENISA, malware si atacuri care vizeaza lanturile de aprovizionare, pâna la amenintari de tip social engineering. Domeniile cele mai afectate sunt administratia publica si institutiile guvernamentale, furnizorii de servicii digitale, serviciile financiare, precum si publicul larg, potrivit aceleiasi surse. Organizatiile cresc investitiile pentru a deveni mai mature din punctul de vedere al securitatii cibernetice, o tendinta vizibila si în tara noastra si care se estimeaza ca va continua. Dar investitiile trebuie sa fie însotite de eforturi pentru construirea unei culturi adecvate în interiorul organizatiilor prin actiuni de constientizare si comunicare a masurilor de securitate cibernetica, prin planificarea unei strategii de aparare în domeniul cibernetic si prin actiuni de retentie a specialistilor din domeniu", a declarat Andrei Ionescu, partener coordonator Consultanta si Managementul Riscului, Deloitte România, si lider al practicii locale de securitate cibernetica.

Studiul mai semnaleaza ca organizatiile sunt constiente de importanta planificarii în vederea crearii de strategii de aparare în domeniul cibernetic care sa diminueze eficient riscurile si sa genereze cresteri ale businessului, aproape doua treimi dintre acestea (62%) având un plan operational si strategic de aparare împotriva amenintarilor cibernetice. Cele foarte mature se remarca în acest sens, ajungând la o pondere de 91%, subliniaza studiul. În plus, mai mult de jumatate dintre companii au organizat un curs anual de constientizare asupra masurilor de securitate cibernetica în rândul angajatilor (59%) si un plan de raspuns la incidente cibernetice care este actualizat si testat anual (58%).

Dincolo de planificare, atragerea si retentia specialistilor din domeniu reprezinta factori importanti în crearea unor strategii de aparare de succes în domeniul cibernetic, iar companiile iau masuri în acest sens, arata studiul. Pentru a implica, retine si dezvolta expertii angajati, organizatiile ofera în principal acces la programe de dezvoltare profesionala si certificari (54%), optiuni de lucru flexibile si hibride (50%) si parcursuri profesionale specializate (45%).

Raportul arata, de asemenea, o legatura clara între actiunile cibernetice si o serie de beneficii, inclusiv încrederea.

Pentru organizatiile cu un nivel ridicat de maturitate cibernetica, o mai buna reputatie a marcii (64%) si a încrederii clientilor si angajatilor în instrumentele digitale (62%) se numara printre principalele beneficii ale actiunilor lor din zona securitatii cibernetice. La polul opus, companiile cu maturitate cibernetica scazuta vad avantaje semnificative în domenii precum încrederea în integritatea tehnologiei (35%) si încrederea clientilor si impactul asupra marcii (31%).

Cea mai recenta editie a studiului Deloitte Global Future of Cyber este efectuata în rândul a peste 1.000 de decidenti în domeniul securitatii cibernetice din 20 de tari din regiuni precum Europa, Orientul Mijlociu si Africa, America de Nord si de Sud si Asia-Pacific. Raportul surprinde impactul sporit pe care securitatea cibernetica îl are asupra organizatiilor.

Echipa de securitate cibernetica a Deloitte România este specializata în oferirea de servicii de strategie, incluzând exercitii de simulare a crizelor cibernetice si evaluari de tip deep dive, servicii de aparare, inclusiv managementul identitatii si accesului, operatiuni de securitate, procese si tehnologii de pregatire si de raspuns la incidente, precum si servicii de atac, vizând în special efectuarea de teste de penetrare, precum exercitiile de tip red-teaming (TIBER-EU).

Deloitte furnizeaza la nivel global servicii de audit, consultanta fiscala si juridica, consultanta, consultanta financiara si managementul riscului catre aproximativ 90% din companiile prezente în topul Fortune Global 500 si catre mii de companii din sectorul privat. Cu o istorie de peste 175 de ani, Deloitte acopera peste 150 de tari si teritorii.

Deloitte România este una dintre cele mai mari firme de servicii profesionale din tara noastra si ofera, în cooperare cu Reff & Asociatii | Deloitte Legal, servicii de audit, de consultanta fiscala, servicii juridice, de consultanta si managementul riscului, consultanta financiara, solutii de servicii si consultanta în tehnologie, precum si alte servicii adiacente, prin intermediul a peste 3.000 de profesionisti.