

Noua din zece organizatii au raportat, în 2022, cel puțin un incident sau o breșă de securitate cibernetică (studiu)

Noua din zece organizatii (91%) au raportat cel puțin un incident sau o breșă de securitate cibernetică anul trecut și mai mult de o treime (38%) între șase și zece evenimente, potrivit studiului Deloitte 2023 Global Future of Cyber.

Conform unui comunicat remis, marți, AGERPRES, studiul mai arată că frecvența incidentelor de acest gen variază în funcție de nivelul de maturitate cibernetică, organizațiile cu maturitate cibernetică mai scăzută confruntându-se cu peste zece evenimente (21%) comparativ cu cele mature (13%).

Preocupările de natură cibernetică ale organizațiilor diferă, de asemenea, în funcție de nivelul acestora de maturitate, cele mai avansate fiind îngrijorate în principal de infractorii și teroristii ciberneticici, precum și de atacurile de tip phishing, malware și ransomware, în timp ce companiile cu maturitate scăzută și medie sunt mai preocupate de atacurile de tip denial-of-service, inițiate cu scopul de a restricționa în mod intenționat rețelele, website-ul și resursele online ale unei companii.

În contextul acestor incidente, perturbarea operațională (58%) este principalul impact resimțit de organizații, urmată de pierderea veniturilor, a încrederii clienților și de impactul negativ asupra mărcii, 56% dintre respondenți menționând că au avut parte de astfel de efecte într-o măsură moderată sau mare.

"Amenințările cibernetice devin din ce în ce mai complexe în fiecare an și variază de la atacuri de tip ransomware, considerate în continuare una dintre principalele amenințări, potrivit agenției UE pentru securitate cibernetică ENISA, malware și atacuri care vizează lanțurile de aprovizionare, până la amenințări de tip social engineering. Domeniile cele mai afectate sunt administrația publică și instituțiile guvernamentale, furnizorii de servicii digitale, serviciile financiare, precum și publicul larg, potrivit aceleiași surse. Organizațiile cresc investițiile pentru a deveni mai mature din punctul de vedere al securității cibernetice, o tendință vizibilă și în țara noastră și care se estimează că va continua. Dar investițiile trebuie să fie însoțite de eforturi pentru construirea unei culturi adecvate în interiorul organizațiilor prin acțiuni de conștientizare și comunicare a măsurilor de securitate cibernetică, prin planificarea unei strategii de apărare în domeniul cibernetic și prin acțiuni de retenție a specialiștilor din domeniu", a declarat Andrei Ionescu, partener coordonator Consultanță și Managementul Riscului, Deloitte România, și lider al practicii locale de securitate cibernetică.

Studiul mai semnalează că organizațiile sunt conștiente de importanța planificării în vederea creării de strategii de apărare în domeniul cibernetic care să diminueze eficient riscurile și să genereze creșteri ale businessului, aproape două treimi dintre acestea (62%) având un plan operațional și strategic de apărare împotriva amenințărilor cibernetice. Cele foarte mature se remarcă în acest sens, ajungând la o pondere de 91%, subliniază studiul. În plus, mai mult de jumătate dintre companii au organizat un curs anual de conștientizare asupra măsurilor de securitate cibernetică în rândul angajaților (59%) și un plan de răspuns la incidente cibernetice care este actualizat și testat anual (58%).

Dincolo de planificare, atragerea și retenția specialiștilor din domeniu reprezintă factori importanți în crearea unor strategii de apărare de succes în domeniul cibernetic, iar companiile iau măsuri în acest sens, arată studiul. Pentru a implica, reține și dezvoltă expertii angajați, organizațiile oferă în principal acces la programe de dezvoltare profesională și certificări (54%), opțiuni de lucru flexibile și hibride (50%) și parcursuri profesionale specializate (45%).

Raportul arată, de asemenea, o legătură clară între acțiunile cibernetice și 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 profesioniști.