Adoptarea telemuncii în pandemie evidentiaza problemele legate de subfinantarea zonei de aparare cibernetica (studiu)

Peste jumatate dintre respondenti (56%) sunt de parere ca organizatiile lor au ocolit procesele de securitate cibernetica pentru a facilita implementarea noilor cerinte legate de telemunca si de un regim de munca flexibil, potrivit raportului EY Global Information Security Survey 2021.

"Adoptarea noilor practici de munca în contextul pandemiei a expus companiile la atacuri cibernetice tot mai numeroase si mai sofisticate si a adus în prim plan subfinantarea mijloacelor de aparare cibernetica", sustin autorii cercetarii.

Raportul EY Global Information Security Survey 2021 a sondat opiniile a peste 1.000 de lideri din domeniul securitatii cibernetice din cadrul companiilor din toata lumea.

În acelasi timp, liderii în securitate cibernetica declara ca nu au fost niciodata mai preocupati ca acum de capacitatea lor de a gestiona amenintarile cibernetice (43%). Peste trei sferturi dintre acestia (77% fata de 59% conform editiei anterioare a GISS) avertizeaza în privinta cresterii numarului de atacuri cibernetice cu impact puternic în ultimele 12 luni, cum ar fi cele de tip "ransomware".

În pofida amenintarii tot mai mari a atacurilor cibernetice, bugetele pentru securitatea cibernetica ramân la un nivel redus în raport cu cheltuielile totale cu tehnologia informatiei, potrivit editiei din acest an a GISS. "Desi organizatiile respondentilor au înregistrat venituri medii de 11 miliarde de dolari în ultimul exercitiu financiar, valoarea medie a cheltuielilor cu securitatea cibernetica a fost de doar 5,28 milioane de dolari", sustin autorii studiului.

Aproape patru din zece respondenti (38%) atrag atentia ca bugetul organizatiei lor este sub nivelul necesar gestionarii noilor provocari aparute în ultimele 12 luni. Acelasi procent de respondenti declara ca cheltuielile cu securitatea cibernetica nu sunt integrate corespunzator în costul investitiilor strategice, cum ar fi transformarea lantului de aprovizionare IT. În acelasi timp, mai bine de o treime (36%) spun ca este doar o chestiune de timp pâna când organizatia lor va suferi o bresa de securitate majora care ar fi putut fi evitata, daca ar fi existat investitii de un nivel adecvat în mijloacele de aparare cibernetica.

Totodata, relatiile esentiale dintre liderii în securitate cibernetica si cei care detin pozitii importante în cadrul organizatiei sunt lipsite de deschidere si de forta, potrivit editiei 2021 a raportului GISS.

Aproximativ 41% dintre liderii în securitate cibernetica sondati au descris relatia lor cu zona de marketing drept negativa, în timp ce 28% au mentionat ca relatia cu proprietarii companiei lasa de dorit. Drept urmare, în timp ce 36% dintre respondentii din 2020 aveau convingerea ca echipele de securitate cibernetica sunt consultate înca din faza de planificare a noilor initiative comerciale, acest procent a scazut la 19% în 2021. Mai mult, doar 25% considera ca liderii de business ar descrie functia de securitate cibernetica a organizatiei lor drept una comerciala.

În contextul în care liderii de companii vad în tehnologie mijlocul prin care îsi pot realiza viziunea si transforma compania, acestia nu îsi pot permite sa întoarca spatele riscurilor cibernetice care vin la pachet cu aceste demersuri. Misiunea directorilor de securitate cibernetica va fi sa se asigure ca liderii de companii vor întelege valoarea adusa de investitiile în securitatea cibernetica si vor constientiza faptul ca acestea reprezinta o parte integranta a procesului de transformare.

"Investitiile majore din ultimii 10 ani, care au avut loc în zona de IT din România, au dus la o uniformizare a practicilor si procedurilor de lucru pe zona securitatii cibernetice specifice celor din vestul Europei si SUA. Practica ultimelor luni a aratat ca si în cazul companiilor din România investitiile în zona de aparare contra atacurilor informatice au crescut, chiar daca per total nu ne aflam la un nivel rezonabil de rezilienta nici în mediul public si nici în cel privat. Solutiile antivirus ramân în continuare cel mai utilizat mijloc de protectie, însa acest lucru s-a dovedit a fi insuficient daca nu vine în completare cu alte solutii", a afirmat Cristian Zaharia, Manager, Forensic Technnologies and Discovery Services, EY România.

Potrivit acestuia, nu trebuie neglijata nici implementarea directivei NIS (Network Internet Security, n.r.), transpusa în legislatia din România prin legea nr. 362/2018. "Noi acte normative si regulamente adoptate în ultima perioada contureaza cadrul necesar implementarii directivei NIS. Asemanator cu situatia în care a fost implementata legislatia GDPR, în viitorul apropiat vom asista la momentul în care si normativele care vin în completarea legii 362/2018 vor fi finalizate. Acesta va însemna o borna importanta la care companiile din România ar trebui sa se gândeasca întrucât nerespectarea acestei legislatii poate atrage dupa sine sanctiuni importante. Astfel, cu cât masurile în zona apararii împotriva atacurilor informatice vor fi luate mai din timp, cu atât companiile se vor pune la adapost atât de eventuale riscuri generate de expunerea la amenintarile cibernetice, dar si de eventuale sanctiuni legislative", a mentionat Cristian Zaharia.

Datele din raportul GISS din acest an se bazeaza pe un sondaj în rândul liderilor în securitate cibernetica (Chief Information Security Officer sau CISO) si alti membri ai consiliilor de administratie din 1.010 organizatii, derulat în perioada martie - mai 2021. CISO si alti membri ai conducerilor executive superioare au reprezentat 50% dintre respondenti; restul respondentilor au fost profesionisti în domeniul securitatii cibernetice de nivel C-1.

EY are 298.000 de angajati în peste 700 de birouri în 150 de tari si venituri de aproximativ 37,2 miliarde de dolari în anul fiscal încheiat la 30 iunie 2020. Cei peste 800 de angajati din România si Republica Moldova furnizeaza servicii integrate de audit, asistenta fiscala, juridica, strategie si tranzactii, consultanta catre companii multinationale si locale.