Costurile globale ale criminalitatii cibernetice vor ajunge la 10,5 trilioane de dolari, în 2025 (analiza)

Deficitul de personal calificat în securitate cibernetica, munca de la distanta si în sistem hibrid, ransomware sau metaverse-ul sunt câteva dintre principalele provocari cu care se confrunta, la ora actuala, mediul cyber, în conditiile în care costurile globale ale criminalitatii cibernetice vor creste cu 15% pe an, pâna la 10,5 trilioane de dolari, în 2025, arata o analiza întocmita de specialistii Eset.

Conform datelor centralizate si publicate recent pe blogul din România al producatorului de solutii antivirus, o prima problema identificata se refera la cresterea criminalitatii cibernetice la nivel global. În acest context, un raport al Cybersecurity Ventures arata ca totalul costurilor globale ale criminalitatii cibernetice vor creste cu 15% pe an, din 2021 pâna în 2025, si ar putea ajunge la 10,5 trilioane de dolari pe an. "Acesta reprezinta mai mult decât profiturile realizate de întregul comert ilegal de droguri combinat. Cresterea poate fi atribuita extinderii semnificative a activitatii grupurilor infractionale cibernetice si a grupurilor sustinute de guvern. În acelasi timp, suprafata de atac a unei companii (zona ei expusa) este din ce în ce mai extinsa, consecinta directa a proceselor de transformare digitala stimulate de progresul unei lumi din ce în ce mai tehnologizate virtual", sustin expertii.

În ceea ce priveste deficitul de personal certificat - a doua provocare din domeniu - exista un decalaj global al fortei de munca în domeniul securitatii cibernetice de 3,4 milioane si 70% dintre organizatii au posturi neocupate în domeniul IT, dupa cum releva studiul ISC, valabil pentru trimestrul II privind Forta de Munca în domeniul Cibernetic. "Multe guverne încearca sa gaseasca solutii pentru a reduce acest deficit, iar companii importante precum Google, Microsoft sau IBM lanseaza diverse initiative care vizeaza formarea si îmbunatatirea competentelor angajatilor sau potentialilor candidati în domeniul securitatii. Între timp, Forumul Economic Mondial, în colaborare cu mai multe companii, a lansat o platforma de educatie online destinata atât persoanelor fizice cât si organizatiilor numita Cybersecurity Learning Hub. Scopul acestui proiect este de a forma si de a îmbunatati abilitatile profesionistilor în securitate, astfel încât tot mai multi oameni sa obtina locuri de munca de calitate în acest domeniu în plina dezvoltare", noteaza sursa citata.

Analiza de specialitate Eset vorbeste, totodata, despre incluziune si diversitate ca fiind prezente în lista provocarilor de pe piata. Specialistii considera ca este necesar sa fie dezvoltate initiative si politici pentru a atrage o mai mare participare din partea grupurilor si minoritatilor slab reprezentate în domeniul acesta de nisa din IT. "Astfel, atragerea catre domeniul securitatii cibernetice a unor grupuri subreprezentate (femeile în special) poate contribui nu doar la cresterea performantelor cât si la reducerea lipsei de profesionisti calificati", se precizeaza în cercetare.

O alta problema majora ce poate afecta mediul securitatii cibernetice este munca de la distanta si în sistem hibrid. În viziunea Eset, transformarea digitala, accelerata de pandemia de COVID-19, a aratat foarte clar companiilor ca trebuie sa acorde prioritate securitatii digitale, iar în cazul lucrului "remote" si a celui în sistem hibrid, organizatiile din întreaga lume nu se mai pot baza doar pe consolidarea protectiei perimetrului interior folosind infrastructura tehnologica locala. "Dimpotriva, trebuie sa se asigure ca angajatii care acceseaza sistemele companiei de la distanta au pregatirea potrivita si dispun de tehnologia adecvata pentru a evita riscurile pe care infractorii cibernetici sunt atât de dornici sa le exploateze", sunt de parere reprezentantii Eset.

Extinderea retelelor de tip "dark web" reprezinta un alt punct nevralgic major si aduce în prim-plan importanta efectuarii activitatilor de informare despre amenintarile posibile din aceste colturi întunecate ale internetului. "Monitorizarea retelelor underground îi ajuta pe aparatorii cibernetici sa previna atacurile, sa înteleaga cum gândesc fraudatorii si grupurile de criminali informatici, ce vulnerabilitati sunt vizate si tranzactionate, ce instrumente malitioase folosesc actorii rau intentionati pentru a accesa sistemele organizatiilor sau pentru a efectua

fraude sau ce informatii despre o anumita organizatie circula în aceste piete subterane", se mentioneaza în analiza.

Pe lista provocarilor cu care se confrunta mediul online se mai afla: noile forme de inginerie sociala, securitatea în ecosistemul de criptomonede, atacurile de tip ransomware, adoptarea metaverse si dezvoltarea educatiei si proceselor de constientizare

Cele mai recente rapoarte de specialitate arata ca, din 2020 pâna în 2021, numarul atacurilor ransomware s-a dublat, iar pentru 2023 acest tip de atacuri vor ramâne o amenintare semnificativa.

În ceea ce priveste metaverse-ul, proiectiile despre adoptarea acestuia releva faptul ca, pâna în 2026, un sfert (25%) din populatia lumii va petrece cel putin o ora pe zi în aceasta lume virtuala si, prin urmare, securitatea în acest univers reprezinta o provocare pentru viitor, apreciaza specialistii.

Eset a fost fondata în anul 1992 în Bratislava (Slovacia) si se situeaza în topul companiilor care ofera servicii de detectie si analiza a continutul malware, fiind prezenta în peste 180 de tari.