Riscurile cibernetice cresc în contextul geopolitic actual. Companiile trebuie sa-și revizuiasca strategiile și sa aloce eficient investițiile



Riscul global al amenințarii cibernetice se intensifica atunci când exista conflicte sau tensiuni geopolitice, atacurile cibernetice sponsorizate de state escaladând în astfel de situații. Recent, președintele SUA a facut apel la companiile și organizațiile private din SUA sa-și „blocheze porțile digitale" fiind foarte posibile atacuri cibernetice în contextul razboiului dintre Rusia și Ucraina. Însa avertismentul este valabil pentru toate organizațiile la nivel mondial, fiind esențial ca acestea sa ia masuri conforme cu gravitatea situației.

Astfel, companiile trebuie sa monitorizeze permanent expunerea la riscurile cibernetice, sa-și consolideze capacitațile de detectare a amenințarilor, sa utilizeze o politica de parole puternice, sa se asigure ca patch-urile de securitate pot fi aplicate la timp și corespunzator și sa securizeze backup-ul datelor.

De asemenea, definirea unor planuri adecvate de continuitate a afacerii și recuperare în caz de crize este primordiala în gestionarea acestora. La fel de importante sunt și instruirea angajaților cu privire la rolul lor în prevenirea atacurilor cibernetice și raportarea oricarei activitați cibernetice anormale sau rau intenționate catre instituțiile locale de reglementare.

Având experiența ultimilor doi de pandemie în care atacurile cibernetice s-au intensificat și au devenit din ce în ce mai sofisticate, companiile sunt mai conștiente de riscuri, multe dintre ele și-au elaborat strategii și aloca bugete mai mari de investiții. Întrebarea este însa daca aceste investiții sunt eficiente și pot raspunde tuturor vulnerabilitaților care pot aparea.

Cum ar trebui alocate investițiile, pentru a fi eficiente în orice situație?

Potrivit raportului *Digital Trust Insights 2022* realizat de PwC, 69% dintre organizațiile la nivel global au bugete mai mari pentru investiții în securitatea cibernetica în acest an, fața de 55% în 2021. Totuși, deși investițiile în securitatea cibernetica au crescut foarte mult, cel mai adesea ele au fost defensive și reactive la multitudinea de amenințari din mediul digital, iar randamentele nu au fost cele scontate. Spre exemplu, doar 20% dintre companiile din Europa Centrala și de Est (ECE) spun ca au vazut beneficii pâna în prezent în urma investițiilor efectuate, arata același raport.

Concluzia este ca soluțiile de securitate cibernetice nu trebuie sa raspunda doar provocarilor de azi, ci trebuie sa

adreseze vulnerabilitaţile pe termen lung şi la urmatoarea generaţie de ameninţari. Deşi deciziile de finanţare trebuie bazate pe propriul set de riscuri şi nevoi, strategiile de investiţii cibernetice nu sunt neaparat intuitive. Experienţa PwC arata ca 30-40% din investiţiile cibernetice ar trebui sa fie cheltuite pentru protecţie, aproximativ 30% pentru detectare şi aproximativ 30% pentru raspuns şi recuperare. Aceasta abordare echilibrata a investiţiilor constituie un punct de plecare în ceea ce priveşte modul în care ar trebui prioritizate investiţiile şi de ce.

Experţii PwC recomanda câteva strategii de investiţii cibernetice eficiente:

Utilizarea iniţiativelor cibernetice pentru a contribui la crearea şi susţinerea valorii, mai degraba decât la simpla protecţie a valorii.

În timp ce multe organizaţii se concentreaza în continuare pe protecţia valorii, exista o nevoie tot mai mare de creare de valoare. Organizaţiile care leaga strategia de afaceri de riscurile cibernetice se concentreaza pe îmbunataţirea experienţei clienţilor/angajaţilor, pe creşterea veniturilor şi pe îmbunataţirea gestionarii costurilor. Raportul Global Digital Trust Insights 2022 arata ca mai mult de jumatate dintre directorii executivi au stabilit obiective mai largi, legate de creştere, pentru echipele lor de securitate, în comparaţie cu aşteptarile mai restrânse, pe termen scurt, de aparare şi control.

Tehnologiile nu trebuie sa determine strategiile de investiţii.
Achiziţia de produse sau soluţii individuale fara a avea un plan general de utilizare a acestora ar putea avea ca rezultat un amalgam de instrumente, cu funcţii redundante, care nu se pot sincroniza în mod corespunzator sau nu pot oferi o acoperire adecvata, ceea ce ar putea duce la o pierdere de timp şi de bani. În ansamblu, investiţiile ar trebui sa asigure acoperirea celor mai mari riscuri ale companiei şi atenuarea lacunelor majore şi sa construiasca agilitatea pentru a lupta împotriva urmatoarei ameninţari, potenţial necunoscute.

Abordarea investiţiilor bazata pe date.
Când vine vorba de investiţii cibernetice, nu exista o strategie unica pentru toate companiile. Acestea pot opta pentru programe şi procese concepute special pentru a raspunde nevoilor lor de securitate, indiferent de ceea ce fac concurenţii sau de ce tehnologii sunt în prim plan.

Dar mai puţin de unul din trei respondenţi la sondajul Global Digital Trust Insights 2022 realizat de PwC spun ca au integrat instrumente de analiza şi de business intelligence în modelul lor operaţional pentru a lua decizii privind investiţiile cibernetice şi gestionarea riscurilor. Aceşti respondenţi au obţinut cel mai mic punctaj în ceea ce priveşte capacitatea lor de a transforma datele în insight-uri pentru cuantificarea riscurilor cibernetice, modelarea ameninţarilor, crearea de scenarii şi analiza predictiva - toate acestea fiind esenţiale pentru decizii inteligente în materie de securitate cibernetica.

Cuantificarea riscului cibernetic ajuta companiile sa adopte o abordare sistematica pentru evaluarea noilor ameninţari. De exemplu, permite unei companii orientate spre achiziţii sa evalueze oportunitaţile de tranzacţii mai rapid şi mai sistematic, iar o instituţie financiara poate evalua ameninţarile şi vulnerabilitaţile zilnic sau saptamânal pentru a proteja milioane de tranzacţii pe zi şi pentru a ramâne alerta daca controalele lor sunt eficiente.

În concluzie, strategia de securitate cibernetica trebuie sa fie vizionara, anticipând ceea ce va urma şi pregatind terenul astfel încât iniţiativele viitoare sa fie implementate în siguranţa. Şi presupune regândirea bugetelor cibernetice, cuantificarea riscurilor cibernetice, construirea rezilienţei şi pregatirea echipelor de securitate pentru viitor.