Investiția în securitatea informației, o schimbare de paradigma

Perioada pandemica prin care trecem a pus o presiune și mai mare asupra echipelor de raspuns la incidente informatice. Ca și cum aceasta situație nu era suficienta, tacticile și metodele folosite de atacatorii cibernetici s-au diversificat și au crescut în complexitate. Toate acestea au dus la o creștere fara precedent a cazurilor în care date informatice ale unor companii foarte mari au fost expuse public, iar consecințele au fost în multe cazuri foarte grave: sancțiuni din partea statelor unde activau, prestigiul afectat ori pierderi financiare ca urmare a acțiunilor întreprinse pentru remediere.

Aceasta realitate a dus catre o conștientizare și mai mare a importanței care trebuie oferita protecției securității informațiilor iar acest lucru s-a vazut deja prin plasarea acestui departament printre locurile fruntașe în ceea ce privește investițiile.

Analizând evoluția celor mai bune practici în vederea creșterii rezilienței împotriva atacurilor informatice, se observa o schimbare în strategia factorilor decidenți dintr-o companie prin implementarea unor masuri menite sa sporeasca securitatea datelor informatice. Acest lucru reprezinta un pas foarte important marcând o tranziție de la o strategie prin care aceasta zona era una daca nu ignorata, în cel mai bun caz aflata în coada prioritaților. Accentul se punea pe rapiditatea cu care informația circula și nu pe asigurarea confidențialității și integrității acesteia.

Pâna nu demult, într-una din cele mai sensibile industrii, cea bancara, simpla deținere a unui cont de utilizator și a unei parole era suficienta pentru a efectua operațiuni financiare. Evident ca aceasta situație a dus în timp la dezvoltarea unei întregi cazuistici constând în transferuri neautorizate de sume de bani din contul unor persoane de buna credința în altele deținute de atacatori. Luând doar acest exemplu se observa ca lucrurile au evoluat foarte mult, în prezent

fiind necesar un numar de operațiuni suplimentare pentru a efectua o simpla plata, autentificarea facând-se în mai mulți pași, simpla deținere a unui cont de autentificare și a unei parole nemaifiind suficienta. Ca masura de siguranța suplimentara și bancile au investit în echipe care monitorizeaza tranzacțiile suspecte și alerteaza clientul în momentul în care detecteaza o potențiala activitate frauduloasa.

Toate aceste schimbari au fost posibile și printr-o colaborare mai puternica între persoanele îndreptațite cu securitatea datelor informatice, precum CIO sau CISO, cu departamentele de business, cele din urma conștientizând importanța protejarii datelor cu care ei lucreaza precum și ale clienților. Se poate observa ca în ultimii doi ani au crescut raportarile cu privire la situația securității informației catre consiliile de conducere,

demers solicitat, în cele mai multe cazuri, chiar de catre acestea pentru a fi la curent cu riscurile la care se expun pe aceasta arie.

O consecința logica a acestei schimbari de strategie este și creșterea bugetului alocat pentru investiții în zona de protecție a informației. Deloc surprinzator este faptul ca acele companii care au experimentat deja un atac informatic, chiar și unul relativ minor, se așteapta ca în urmatorii ani sa-și creasca investițiile în aceasta zona. Piața se mișca însa diferit în funcție de experiențele pe care le-au avut companiile. Daca unele au decis sa investeasca în soluții de detectare a intruziunilor în rețeaua lor ori masuri de prevenire și stopare a e-mail-urilor daunatoare, altele s-au orientat catre soluții de „Multi-Factor Authentication" (autentificare în mai mulți pași) sau catre tehnologii care sa îmbunatațeasca autorizarea și controlul accesului la resursele companiei.

Poate cea mai întâlnita situație este cea a externalizarii serviciilor de raspuns la incidentele informatice. Companiile au realizat ca eficiența investiției masive în soluții de securitate este mult diminuata daca nu este dublata și de profesioniști care sa știe cum sa le integreze și interconecteze astfel încât sa maximizeze avantajele acestora.

Un alt exemplu relevant pentru modul în care factorii decidenți au început sa puna accent pe investiția în domeniul securității informației este întâlnit în cazul achiziției unei alte entități. Se observa astfel, din ce în ce mai des, o cerere pentru verificarea posibilelor antecedente de natura sa scoata la iveala vulnerabilități din trecut pentru compania care este achiziționata.

Cunoscute în domeniu ca „cyber due dilligence", aceste activități sunt solicitate tocmai pentru a se cunoaște riscurile la care companiile se expun, din punctul de vedere al securității informatice, odata cu achiziționarea unei alte entități și integrarea acesteia în infrastructura deja existenta.

Este celebru cazul unui mare lanț hotelier care a achiziționat unul dintre competitorii sai, iar la o perioada de timp au suferit o exfiltrare a datelor cauzata tocmai de o vulnerabilitate care se regasea în sistemele companiei pe care au cumparat-o. Astfel, în toate titlurile aparute pe acest subiect în acea perioada se menționa numele lanțului hotelier ca fiind cel responsabil de incident, deși problema inițiala a plecat de la compania achiziționata și, din lipsa unui „cyber due dilligence", a ramas nedescoperita la momentul la care au cumparat-o.

Spre deosebire de alte departamente, cel de raspuns la incidente de securitate nu are perioade mai puțin aglomerate, fiind supus permanent amenințarilor cibernetice și într-o continua stare de alerta. Persoanele care au putere de decizie într-o companie sunt, așadar, din ce în ce mai mult în postura de a lua o decizie: implementeaza o serie de pași simpli spre îmbunatațirea capacității de aparare împotriva atacurilor informatice alocând o parte din investiții în acest sens sau doresc sa continue cu o strategie bazata pe reactivitate în care sunt nevoiți sa stea în expectativa și sa intervina doar când apare un incident. În cel de-al doilea scenariu, s-a dovedit ca riscurile asumate sunt uriașe întrucât în foarte multe cazuri prejudiciile cauzate sunt iremediabile.