

Bancile, asiguratorii și societățile de investiții trebuie să-și adapteze strategiile de securitate cibernetică la noile norme privind reziliența operațională digitală, adoptate de UE



Numărându-se printre țintele preferate ale hackerilor, bancile, societățile de asigurări și firmele de investiții trebuie să-și întărească mai mult securitatea cibernetică până la finalul anului 2024, pentru a se conforma cerințelor Actului legislativ privind reziliența operațională digitală (DORA), adoptat de Consiliul European la finele lunii noiembrie. DORA este cea mai importantă inițiativă de reglementare a UE privind reziliența operațională și securitatea cibernetică în sectorul serviciilor financiare, pentru a se asigura că sectorul financiar european este capabil să reziste în cazul unor perturbări operaționale grave.

Publicată pentru prima dată în septembrie 2020, ca parte a Pachetului privind finanțele digitale (DFP) al Uniunii, perioada de punere în aplicare a DORA va dura 24 de luni, ceea ce înseamnă că firmele trebuie să se conformeze cerințelor până la sfârșitul anului 2024.

Care sunt cerințele DORA?

Aproape fiecare tip de instituție financiară din UE va trebui să se asigure că furnizorii săi și controalele de securitate ale acestora respectă standardele de reziliență, iar eforturile solicitate entităților financiare vor fi proporționale cu riscurile potențiale. Totodată, DORA stabilește cerințe uniforme pentru securitatea rețelelor și a sistemelor informatice ale companiilor din sectorul financiar, precum și ale părților terțe critice care le furnizează servicii legate de TIC (tehnologii ale informației și comunicațiilor), cum ar fi platformele cloud sau serviciile de analiză a datelor. Mai mult, furnizorii de servicii TIC din țări terțe vor trebui să-și înființeze filiale pe teritoriul UE, astfel încât supravegherea să poată fi pusă în aplicare în mod corespunzător.

În ceea ce privește Directiva NIS, aceasta continuă să se aplice, DORA abordând posibilele suprapuneri prin derogări.

Aspectele care necesită transpunere la nivel național vor fi adoptate în legislația fiecărui stat membru al UE. În același timp, autoritățile europene de supraveghere relevante din domeniul bancar, al valorilor mobiliare și al asigurărilor vor elabora standarde tehnice care vor trebui respectate de toate instituțiile din domeniul serviciilor financiare.

Contextul cibernetic. La ce trebuie să fie atente companiile?

Breșele de securitate a datelor reprezintă o amenințare omniprezentă în lumea digitală, chiar dacă au fost făcute progrese în ultimii ani, iar anul 2023 se profilează ca un nou test de reziliență pentru companii și cu presiuni tot mai mari pentru a asigura securitatea și confidențialitatea datelor, potrivit studiului Digital Trust Insights Survey

2023 realizat de PwC. În acest context, este nevoie de un nivel mai ridicat de colaborare între sectorul public și cel privat pentru o raportare mai clară a incidentelor, gestionarea riscurilor și planificarea continuității afacerii și a recuperării în caz de dezastru.

Impactul atacurilor cibernetice merge mult mai departe de costul financiar direct, prejudiciile menționate de organizațiile afectate de un astfel de incident în ultimii trei ani fiind pierderea clienților, pierderea datelor clienților și daune aduse reputației sau marcii. În pofida faptului ca atacurile cibernetice continua sa coste companiile milioane de dolari, mai puțin de 40% dintre directorii chestionați în cadrul Digital Trust Insights afirma ca au atenuat complet expunerea la riscurile de securitate cibernetica într-o serie de domenii critice, precum munca la distanță și hibridă (38% spun ca riscul cibernetice este pe deplin atenuat), adoptarea accelerata a cloud-ului (35%), utilizarea IOT (34%), digitalizarea lanțului de aprovizionare (32%) și a operațiunilor de back-office (31%).

În același timp, doua treimi dintre directori considera ca infracțiunile cibernetice reprezinta cea mai importanta amenințare pentru anul viitor. Infractorii cibernetici, care folosesc din ce în ce mai mult resurse disponibile comercial, pot comite și orchestra o varietate de atacuri.

Companiile trebuie sa monitorizeze permanent expunerea la riscurile cibernetice, sa-și consolideze capacitățile de detecție și raspuns la amenințari, 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 atac 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 activități 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 alocat bugete mai mari de investiții. Întrebarea este însă daca aceste investiții sunt eficiente și pot raspunde atacurilor viitoare.

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. Strategia de aparare cibernetica este definita, printre altele, pe baza analizei mai multor scenarii ce încearca sa prevada manifestarea amenințărilor. Iar capacitatea de analiza ramâne în continuare limitata, din cauza unor factori precum complexitatea interna a organizațiilor (procesne funcționale sau ineficiente, mediul tehnologic eterogen și, de multe ori, lipsa unei comunicari interne adecvate), ecosistemul de afaceri (numarul mare de parteneri de afaceri, direcți sau indirecti) și viteza cu care evolueaza complexitatea amenințărilor cibernetice și resursele disponibile atacatorilor.

De aceea, companiile din domeniul serviciilor financiare, dar nu numai, trebuie sa își asigure reziliența operaționala prin adoptarea unor strategii de securitate cibernetica holistice, care sa raspunda și provocarilor de mâine, nu doar celor de azi. Aceste strategii sunt operaționalizate odata cu dezvoltarea unor programe de securitate adecvate, care dispun de resursele necesare implementarii tehnologiilor relevante și a proceselor eficiente de identificare și raspuns la amenințari, precum și dezvoltarii capabilităților la nivelul resurselor umane specializate.

Nu în ultimul rând, riscurile cibernetice sistemice trebuie monitorizate la nivel de societate, iar adresarea acestora poate fi facuta prin crearea unor mecanisme de partajare securizata a indicatorilor tehnici sau tehnologici cu privire la incidentele de securitate, mecanisme construite pe relații de încredere, la nivelul comunităților profesionale ale specialiștilor în securitate sau în cadrul cooperarilor dintre companii și autoritățile specializate.