Bancile, asiguratorii și societățile de investiții trebuie sa-și adapteze strategiile de securitate cibernetica la noile norme privind reziliența operațională digitala, adoptate de UE

Numarându-se printre țintele preferate ale hackerilor, bancile, societățile de asigurari și firmele de investiții trebuie sa-și întareasca mai mult securitatea cibernetica pâna la finalul anului 2024, pentru a se conforma cerințelor Actului legislativ privind reziliența operațională digitala (DORA), adoptat de Consiliul European la finele lunii noiembrie. DORA este cea mai importanta inițiativa de reglementare a UE privind reziliența operațională și securitatea cibernetica în sectorul serviciilor financiare, pentru a se asigura ca sectorul financiar european este capabil sa reziste în cazul unor perturbari operaționale grave.

Publicata pentru prima data 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 înseamna ca firmele trebuie sa se conformeze cerințelor pâna la sfârșitul anului 2024.

Care sunt cerințele DORA?

Aproape fiecare tip de instituție financiara din UE va trebui sa se asigure ca furnizorii sai și controalele de securitate ale acestora respecta standardele de reziliența, iar eforturile solicitate entităților financiare vor fi proporționale cu riscurile potențiale. Totodata, DORA stabilește cerințe uniforme pentru securitatea rețelelor și a sistemelor informatice ale companiilor din sectorul financiar, precum și ale părților terțe critice care le furnizeaza servicii legate de TIC (tehnologii ale informației și comunicațiilor), cum ar fi platformele cloud sau serviciile de analiza a datelor. Mai mult, furnizorii de servicii TIC din țari terțe vor trebui sa-și înființeze filiale pe teritoriul UE, astfel încât supravegherea sa poata fi pusa în aplicare în mod corespunzator.

În ceea ce privește Directiva NIS, aceasta continua sa se aplice, DORA abordând posibilele suprapuneri prin derogari.

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

Contextul cibernetic. La ce trebuie sa fie atente companiile?

Breșele de securitate a datelor reprezinta o amenințare omniprezenta în lumea digitala, chiar daca au fost facute progrese în ultimii ani, iar anul 2023 se profileaza ca un nou test de reziliența 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 şi cel privat pentru o raportare mai clara a incidentelor, gestionarea riscurilor şi planificarea continuitaţii afacerii şi a recuperarii în caz de dezastru.

Impactul atacurilor cibernetice merge mult mai departe de costul financiar direct, prejudiciile menţionate de organizaţiile afectate de un astfel de incident în ultimii trei ani fiind pierderea clienţilor, pierderea datelor clienţilor şi daune aduse reputaţiei sau marcii. În pofida faptului ca atacurile cibernetice continua sa coste companiile milioane de dolari, mai puţin de 40% dintre directorii chestionaţi 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 distanţa şi hibrida (38% spun ca riscul cibernetic este pe deplin atenuat), adoptarea accelerata a cloud-ului (35%), utilizarea IOT (34%), digitalizarea lanţului de aprovizionare (32%) şi a operaţiunilor de back-office (31%).

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

Companiile trebuie sa monitorizeze permanent expunerea la riscurile cibernetice, sa-şi consolideze capacitaţile de detecţie şi raspuns la ameninţari, sa utilizeze o politica de parole puternice, sa se asigure ca patch-urile de securitate pot fi aplicate la timp şi corespunzator şi sa securizeze backup-ul datelor.

De asemenea, definirea unor planuri adecvate de continuitate a afacerii şi recuperare în caz de atac este primordiala în gestionarea acestora. La fel de importante sunt şi instruirea angajaţilor cu privire la rolul lor în prevenirea atacurilor cibernetice şi raportarea oricarei activitaţi cibernetice anormale sau rau intenţionate catre instituţiile locale de reglementare.

Având experienţa ultimilor doi de pandemie în care atacurile cibernetice s-au intensificat şi au devenit din ce în ce mai sofisticate, companiile sunt mai conştiente de riscuri, multe dintre ele şi-au elaborat strategii şi aloca bugete mai mari de investiţii. Întrebarea este însa daca aceste investiţii sunt eficiente şi pot raspunde atacurilor viitoare.

Deşi investiţiile în securitatea cibernetica au crescut foarte mult, cel mai adesea ele au fost defensive şi reactive la multitudinea de ameninţari 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 ameninţarilor. Iar capacitatea de analiza ramâne în continuare limitata, din cauza unor factori precum complexitatea interna a organizaţiilor(procese nefuncţionale sau ineficiente, mediul tehnologic eterogen şi, de multe ori, lipsa unei comunicari interne adecvate), ecosistemul de afaceri (numarul mare de parteneri de afaceri, direcţi sau indirecţi) şi viteza cu care evolueaza complexitatea ameninţarilor cibernetice şi resursele disponibile atacatorilor.

De aceea, companiile din domeniul serviciilor financiare, dar nu numai, trebuie sa îşi asigure rezilienţa operaţionala prin adoptarea unor strategii de securitate cibernetica holistice, care sa raspunda şi provocarilor de mâine, nu doar celor de azi. Aceste strategii sunt operaţionalizate odata cu dezvoltarea unor programe de securitate adecvate, care dispun de resursele necesare implementarii tehnologiilor relevante şi a proceselor eficiente de identificare şi raspuns la ameninţari, precum şi dezvoltarii capabilitaţilor 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 relaţii de încredere, la nivelul comunitaţilor profesionale ale specialiştilor în securitate sau în cadrul cooperarilor dintre companii şi autoritaţile specializate.