Şase din zece IMM-uri îsi încheie activitatea în 6 luni de la încalcarea securitatii datelor (analiza)

Întreprinderile Mici si Mijlocii (IMM) sunt, în prezent, cele mai expuse la atacuri cibernetice, în timp ce 60% dintre acestea sunt nevoite sa îsi încheie activitatea în termen de sase luni de la încalcarea securitatii datelor, sunt de parere expertii în securitate informatica din cadrul Zytel, într-o analiza publicata miercuri.

Conform specialistilor, un prim sfat de care ar trebui sa tina cont IMM-urile se refera la întelegerea peisajului amenintarilor, în conditiile în care pâna si marile corporatii au fost tinta principala a hackerilor si actorilor rau intentionati (de exemplu: Marriott Hotels si Organizatia Mondiala a Sanatatii - atacate în aprilie 2020).

"Cu toate acestea, pe parcursul anului trecut, aceasta tendinta s-a schimbat, iar studiile arata ca IMM-urile sunt acum cele mai expuse la atacuri cibernetice. Aceasta schimbare poate fi atribuita în mare masura faptului ca organizatiile mai mici au, de obicei, cel mai mult de pierdut daca sunt expuse la un atac, rapoartele indicate sustin ca 60% dintre IMM-uri îsi încheie activitatea în termen de sase luni de la încalcarea securitatii datelor. Acest lucru, împreuna cu faptul ca organizatiile mici nu dispun adesea de apararea sofisticata de securitate la care au acces marile corporatii, face ca IMM-urile sa fie tinta perfecta pentru infractorii cibernetici. Pe masura ce aceste organizatii înteleg ca au devenit tinta principala pentru infractorii cibernetici, 2022 va înregistra o crestere a numarului de IMM-uri care cauta solutii care sa le protejeze retelele. Spre deosebire de organizatiile mari care au departamente de securitate în infrastructura afacerilor, IMM-urile vor cauta furnizori si MSP (Managed Service Provider) care pot oferi solutii de securitate usor de gestionat si accesibile", se arata în analiza de specialitate.

Potrivit sursei citate, cercetari recente releva faptul ca 97% dintre organizatii au implementat sau intentioneaza sa implementeze lucrul hibrid în structura lor de afaceri.

"Ca atare, exista orientarea spre un mod mai distribuit de lucru. În loc sa aiba o singura retea centralizata, angajatii se conecteaza dintr-o varietate de locatii, cu diferite niveluri de masuri de securitate specifice (...) Pentru a aborda aceasta problema, IMM-urile vor trebui sa adopte o abordare a "încrederii zero", prin verificarea întotdeauna a conectivitatii, prin care orice persoana care încearca sa acceseze reteaua va trebui sa verifice daca este cine spune ca este. În 2022, acest lucru va avea loc printr-o adoptare sporita a autentificarii multi-factor, ceea ce va permite companiilor sa verifice daca persoanele din reteaua lor o acceseaza corect si nu sunt actori rau intentionati. Acest lucru le va permite sa protejeze datele pentru ei însisi si clientii lor", noteaza Zytel.

Un alt aspect important face referire la confidentialitatea datelor, "un subiect fierbinte de conversatie pentru guvern si întreprinderile mari prin aparitia Regulamentului general al UE privind protectia datelor si reformele legislative ulterioare".

"Cu toate acestea, având în vedere ca încalcarile securitatii datelor au înregistrat o crestere de 14% în 2021 pâna în 2020, IMM-urile au fost obligate sa actioneze mai vigilent pentru a proteja datele clientilor. Acest lucru a cauzat o multime de probleme pentru IMM-urile care nu dispun de departamentele dedicate de politica si securitate la carle au acces marile corporatii. Confruntate cu plângeri din ce în ce mai mari din partea clientilor preocupati de datele lor cu caracter personal, aceste întreprinderi mai mici vor trebui sa gaseasca si sa adopte solutii usoare care pot ajuta la limitarea si gestionarea datelor. În cele din urma, pe masura ce încalcarile securitatii datelor devin mai proeminente, IMM-urile vor trebui sa plaseze securitatea ca prioritate de vârf în cadrul modelelor lor de afaceri pentru a supravietui. În lipsa infrastructurii interne pentru a implementa masuri de securitate mai avansate, în 2022, IMM-urile vor apela la furnizori si MSP-uri pentru a acumula cunostinte, echipamente si infrastructura pentru a se apara împotriva atacatorilor", afirma expertii în securitate cibernetica.

Zyxel Networks conecteaza de peste 30 de ani la Internet organizatii si utilizatori casnici, punând accent din prima zi de activitate pe inovatie si servicii orientate catre clienti. Compania are operatiuni pe 150 de piete nationale, iar 100 de milioane de echipamente Zyxel creeaza conexiuni la nivel global.