60% dintre IMM-uri îsi înceteaza activitatea dupa 6 luni de la aparitia unei brese de date (raport)

Întreprinderile Mici si Mijlocii (IMM) sunt, în prezent, cel mai expuse riscului de atacuri cibernetice, iar la sase luni de la aparitia unei brese de date 60% dintre aceste organizatii îsi înceteaza activitatea, arata o serie de rapoarte de specialitate, citate de unul dintre jucatorii importanti de pe piata mondiala de networking.

"Pâna în aprilie 2020, atacatorii cibernetici au început sa profite de instabilitatea pe care pandemia a provocat-o afacerilor, piratând mari corporatii multinationale, inclusiv Magellan Health, Marriott Hotels si Organizatia Mondiala a Sanatatii (...) Desi marile corporatii au fost tinta principala pentru hackeri în timpul valului initial al pandemiei, rapoartele indica faptul ca aceasta tendinta s-a schimbat, iar IMM-urile sunt acum cel mai expuse riscului de atacuri cibernetice. Hackerii au început sa pivoteze catre organizatii mai mici, deoarece, desi exista un câstig maxim mai mic, ei au sanse mai mari de succes din cauza lipsei de aparare de securitate sofisticate pe care IMM-urile le au de obicei. În plus, IMM-urile risca sa piarda cel mai mult daca sunt expuse unui atac. Rapoartele arata ca în sase luni de la aparitia unei brese de date 60% dintre IMM-uri îsi înceteaza activitatea. Drept urmare, companiile mai mici nu au de ales decât sa accepte cererile de ransomware, facându-le tinta principala pentru hackeri", precizeaza reprezentantii Zyxel Networks, într-un comunicat de presa transmis, luni, AGERPRES.

Un exemplu referitor la atacurile asupra IMM releva faptul ca proportia traficului de e-mail rau intentionat a crescut de la 12% la niveluri înainte de pandemie, la peste 60% la doar sase saptamâni dupa anuntarea primului lockdown din Marea Britanie.

Potrivit unui raport WatchGuard, primul trimestru din 2021 a înregistrat cel mai înalt nivel de detectie de malware "zero-day" înregistrat vreodata, aproximativ 74% dintre amenintari fiind capabile sa ocoleasca solutiile antivirus conventionale.

Pe acest fond, specialistii Zyxel avanseaza solutia de tip sandboxing, o tehnica Advanced Threat Protection (ATP) în care tiparele utilizatorului de fisiere necunoscute sunt preluate într-un mediu izolat si sigur pentru a fi continute, emulate si inspectate. Acest proces protejeaza afacerile de amenintarile zero-day, deoarece executa comanda de trafic într-un mediu izolat, separat de reteaua de baza, pentru a testa daca este rau intentionat sau nu. Daca sandbox-ul detecteaza o amenintare, aceasta va fi stearsa sau pusa în carantina.

"Sandboxing-ul este o resursa de securitate de nepretuit pentru IMM-uri, deoarece împiedica malware-ul sa intre vreodata într-o retea, oferind un nivel cuprinzator de protectie care nu poate fi obtinut de la un UTM standard. În ciuda acestui fapt, de obicei companiile mai mici au trecut cu vederea sandboxing-ul din cauza costurilor ridicate asociate. Dar, cu amenintarile tintite zero-day care devin din ce în ce mai populare, balanta s-a înclinat. IMM-urile nu îsi mai permit sa nu îmbratiseze o solutie de tip sandboxing. Pandemia a demonstrat, de asemenea, superioritatea sandboxing-ului în cloud fata de solutiile bazate pe dispozitive, deoarece o solutie de cloud sandboxing permite organizatiilor sa-si protejeze forta de munca de la distanta. O solutie de sandboxing bazata pe cloud va împiedica actorii rau intentionati sa acceseze reteaua de baza a unei companii prin protejarea retelei edge. Prin urmare, IMM-urile cu angajati care lucreaza de la distanta ar trebui sa opteze pentru o solutie de sandboxing bazata pe cloud, deoarece creeaza o retea sigura, indiferent de locatia angajatului", explica expertii.

Zyxel Networks conecteaza la Internet, de peste 30 de ani, organizatii si utilizatori casnici, si este, în prezent, unul dintre jucatorii importanti de pe piata mondiala de networking, cu o prezenta internationala ce include: operatiuni pe 150 de piete nationale, un milion de organizatii care lucreaza mai inteligent utilizând solutiile Zyxel si 100 de milioane de echipamente Zyxel care creeaza conexiuni la nivel global.