Scris de newsreporter pe 31 decembrie 2020, 10:37

Kit de securitate cibernetica in pandemie. Cum sa te protejezi de atacuri in 2021

De la atacuri de tip ransomware, care iti blocheaza sistemele pana cand platesti recompensa, la atacuri in lant care tintesc intai companiile mici, si pana la amenintari de tip „sextorsion”, pericolele din mediul cibernetic s-au inmultit in ultimii ani si au capatat noi dimensiuni in 2020. Odata cu trecerea la scoala online, munca online, viata online, s-au deschis mai multe „ferestre” prin care atacatorii pot intra in „casa” noastra si in compania noastra, scrie ZF.

joan-gamell-zs67i1hlllo-unsplash.jpg

Cea mai sigura tinta a unui atac cibernetic este angajatul din companie, din perspectiva unui hacker. Prin tintirea unui singur angajat, hackerul poate introduce cu usurinta sisteme malitioase care duc la pierderi de date sau la atacuri mai grave.

Totusi, un angajat care nu a fost instruit sau lasat fara mijloace de aparare in fata unor astfel de atacuri care evolueaza in mod constant nu poate fi acuzat, neaparat, in contextul in care atacurile cibernetice au devenit din ce in ce mai complexe.

Iar daca in trecut, atacurile de tip „printul nigerian” erau foarte usor de identificat (adica cele in care primeai un e-mail prin care se presupunea ca esti contactat sau contactata de un print exotic

care vrea dintr-un motiv sau altul sa iti dea bani), acum, situatia a devenit mai dificila, este de parere Andrei Avadanei, general manager al companiei romanesti de securitate cibernetica Bit Sentinel.

„Pentru angajati este foarte dificil sa identifice si sa clasifice un astfel de e-mail ca fiind spam pentru ca, daca in trecut atacurile de tip «print nigerian» erau o dovada clara ca un e-mail are malware, acum acestea sunt atat de sofisticate incat pot fi considerate legitime. De exemplu, pot veni de pe adrese de e-mail foarte similare cu cele ale unor furnizori cunoscuti, singura diferenta fiind inversarea de litere sau alte detalii pe care nu le observi decat la o analiza amanuntita sau poate cand este deja prea tarziu”, a explicat el, intr-un interviu acordat Business MAGAZIN.

Anul 2020 si inceputul pandemiei au inmultit fronturile pe un camp de lupta care devenea deja din ce in ce mai sofisticat, cel cibernetic. Schimbarile rapide pe care au fost nevoite sa le faca firmele de toate dimensiunile, de la microintreprinderi si pana la corporatii, toate sub umbrela mult iubitei „digitalizari”, au adus cu sine riscuri din ce in ce mai mari. „Principalul motiv este legat de digitalizarea fortata a businessurilor si adaptarea acestora la sistemul de telemunca intr-un timp foarte scurt. Extinderea perimetrului infrastructurii informatice aduce cu sine canale noi de comunicare si, implicit, usi deschise pentru potentialii atacatori cibernetici. Astfel, hackerii au avut noi oportunitati de a lansa valuri de atacuri cibernetice, in principiu, de tip «ransomware»”, a punctat Avadanei.

Citeste continuarea articolului pe www.businessmagazin.ro

ADRESA: http://crct.ro/nxaQ