PwC România: Organizatiile si populatia devin mai vulnerabile la riscurile cibernetice, pe fondul epidemiei COVID-19

Cererea ridicata de echipamente medicale, precum mastile chirurgicale, a dus la aparitia multor magazine online false, website-uri si conturi de social media care pretind ca vând aceste produse online, atentioneaza specialisti PwC România, într-o analiza publicata vineri.

"În fata unei crize neasteptate, cum este cea generata de pandemia COVID-19 care domina atentia, organizatiile si populatia devin mai vulnerabile la alte riscuri, precum schemele de frauda din ce în ce mai elaborate ale hackerilor/criminalilor informatici care profita de îngrijorarea instaurata la nivel global. Deoarece s-a observat deja o crestere a atacurilor de tip phishing, este important sa intensificam gradul de constientizare a securitatii digitale în aceasta perioada. De exemplu, mentionam cererea ridicata de echipamente medicale, precum mastile chirurgicale, care au dus la aparitia multor magazine online false, website-uri si conturi de social media care pretind ca vând aceste produse online. Inclusiv Interpol, CERT-RO si Agentia pentru Securitate Cibernetica a Uniunii Europene (ENISA) au atentionat public ca s-au înmultit cazurile în care se profita de situatia generata de pandemia COVID-19, având loc diverse înselatorii financiare, îndeosebi criminalitate cibernetica. Iar sumele pot depasi în unele cazuri 100.000 de dolari", explica sursa citata.

Potrivit companiei de consultanta, printre cele mai comune metode folosite de infractori sunt frauda telefonica si e-mail-urile de tip phishing.

Astfel, în cazul fraudei telefonice, hackerul poate pretinde ca suna din partea unui spital sau al unei clinici unde un apropiat a fost internat si necesita plata unor tratamente urgente.

De asemenea, e-mail-urile de tip phishing pot parea ca vin din partea autoritatilor, cu scopul de a obtine date de identificare, date financiare sau contin un atasament virusat.

O alta modalitate implica hartile care indica gradul de raspândire a virusului COVID-19 si care, de fapt, ascund site-uri unde oamenii sunt încurajati sa instaleze diverse aplicatii pentru a avea acces la informatii. În acest mod este facilitat furtul de date de autentificare ale utilizatorilor.

Specialistii recomanda angajatilor sa nu amestece, pe cât posibil, activitatile de munca cu cele de divertisment si timp liber pe acelasi dispozitiv si sa fie deosebit de atenti la orice e-mail care face referire la coronavirus.

În acest context, pentru a preveni fraude de acest fel, institutiile abilitate a realizat o serie de recomandari care trebuie avute în vedere, printre care: verificati istoricul companiilor care pretind ca ofera servicii si echipamente medicale pentru a confirma legitimitatea acestora, evaluati cu atentie e-mail-urile prin care vi se ofera echipament medical sau vi se cer informatii personale în vederea consulturilor medicale, deoarece, în mod normal, autoritatile nu contacteaza publicul prin astfel de mijloace, verificati veridicitatea site-urilor care par a fi oficiale (ex: abc.com vs abc.org).

PwC România mai face referire la recomandarea de a nu accesa link-uri incerte si de a nu deschide atasamente care nu sunt asteptate. În plus, se recomanda verificarea a cel putin înca o sursa în situatia în care sunt primite e-mail-uri care pun presiune asupra utilizatorului sau care invoca o serie de consecinte neplacute daca nu se efectueaza activitatea solicitata în e-mail.

În ceea ce priveste angajatorul, al carui angajati lucreaza de acasa, este vital sa abordeze masuri, precum: stabilirea de proceduri clare cu privire la munca de acasa, instruirea angajatilor sa fie vigilenti la posibile atacuri sociale si

cibernetice, oferirea de solutii de acces eficiente si securizate la sistemele interne, verificari daca software-ul folosit este actualizat si ca schimbarile în infrastructura IT aferente lucrului de acasa nu cresc riscul unui atac cibernetic, folosirea semnaturilor electronice în favoarea celor fizice pentru documentele oficiale.