Previziuni HP: Securitatea organizationala va fi pusa greu la încercare de catre atacatorii cibernetici, în 2021

Organizatiile se vor confrunta cu o provocare uriasa de securitate în acest an, pe masura ce atacatorii cibernetici devin tot mai specializati, iar amenintarile de tip thread hijacking, whaling si ransomware se vor intensifica în urmatoarele 12 luni, arata previziunilor HP în domeniul securitatii cibernetice, publicate luni.

"Pandemia COVID-19 si trecerea la munca de acasa au slabit securitatea organizationala. Problemele aparute în urma conexiunilor la distanta, vulnerabilitatile dispozitivelor VPN si lipsa de personal care sa ajute compania sa se adapteze, toate acestea fac ca datele sa nu fie complet protejate. Din perspectiva atacatorilor cibernetici, oferta este acum mult mai generoasa. Expertii atrag atentia ca echipamentele de acasa nu sunt protejate, iar infrastructura folosita va deveni, în mod sigur, o tinta pentru atacatorii cibernetici care astfel pot accesa reteaua companiei. O vulnerabilitate este si faptul ca angajatii nu beneficiaza acasa de ajutorul departamentului IT pentru a remedia problemele aparute la echipamentele personale", sunt de parere expertii în securitate cibernetica.

În 2021, echipele de securitate IT vor merge pe principiul Zero Încredere, dar este important sa ofere transparenta pentru utilizator.

"Zero Încredere este un concept relativ nou. Dar, cu un numar tot mai mare de angajati care lucreaza de acasa, companiile trebuie sa accepte aceasta realitate pentru a se asigura ca munca la distanta este securizata. Metodele securizate de autentificare si acces la reteaua organizatiei sunt un factor cheie în implementarea conceptului Zero Încredere", se mentioneaza în raport.

O alta estimare a celor de HP face referire la atacurile de tip ransomware, dar si la noile metode de phishing pentru atacurile de tip thread hijacking si whaling.

Astfel, atacurile de tip ransomware - care cripteaza fisierele pentru a solicita, apoi, rascumparare - nu vor mai consta în furtul de informatii, ci în dezvaluirea publica a acestora.

"Aceasta tendinta este îngrijoratoare în special pentru organizatiile sau institutiile din sectorul public, care proceseaza informatii cu caracter personal. Chiar daca rascumpararea este platita, nu exista nicio garantie ca hackerii nu vor încerca mai târziu sa obtina profit din datele furate", sustin specialistii.

Pe de alta parte, în acest an, vor aparea noi "momeli phishing", mult mai greu de descoperit, menite sa pacaleasca utilizatorii.

"Cea mai inovatoare tehnica de phishing masiv este metoda e-mail threat hijacking, utilizata de reteaua Emotet. Aceasta presupune crearea automata a momelilor de tip spear-phishing furând date din sistemele compromise. Aceste informatii sunt apoi folosite pentru a raspunde unor conversatii cu mesaje care contin malware, dar care par veridice. Atacul de tip whaling - o forma de phishing foarte tintit care vizeaza manageri - va fi mai proeminent, iar atacatorii cibernetici vor putea folosi informatiile personale din online pentru a crea momeli convingatoare cu care sa compromita conturi business de e-mail. Un alt scenariu foarte plauzibil este exploatarea fricilor oamenilor, care vor fi mult mai dispusi sa deschida e-mailuri compromise în speranta ca vor afla mai multe despre vaccinul anti-COVID, despre masurile de izolare, insecuritate financiara sau instabilitate politica", noteaza HP.

De asemenea, anul 2021 va aduce în prim-plan personalizarea atacurilor ce vor viza infrastructura critica, precum sectorul farmaceutic si cel de sanatate, educatia, IoT (Internet of Things - Internetul lucrurilor) industrial.

"Organizatiile se vor confrunta cu o provocare uriasa de securitate în acest an, pe masura ce atacatorii cibernetici devin tot mai specializati. Daca se vor baza doar pe metodele de detectare a atacurilor, organizatiile vor avea doar jumatate de solutie pentru aceasta problema. Sfatul specialistilor: este necesara o abordare arhitecturala robusta în ceea ce priveste securitatea cibernetica, o abordare care sa protejeze începând cu hardware-ul. Organizatiile trebuie sa-si regândesca arhitectura de securitate si gestionarea acesteia si sa implementeze inovatiile tehnologice necesare", avertizeaza expertii în securitate cibernetica.

Previziunile în domeniul securitatii cibernetice pentru anul 2021 au fost compilate de experti din cadrul HP, în cooperare cu specialistii din cadrul HP Security Advisory Board.