Riscuri asociate revenirii la munca de la birou – o altă față a monedei

Masurile de relaxare resimțite aproape în întreaga Europa își au ecoul și în România, astfel încât din ce în ce mai multe companii le permit angajaților sa se reîntoarca la birou adoptând, așa cum este normal, anumite măsuri sporite de protecție sanitară.

Un factor care poate să treaca adesea neobservat este riscul la care se expun companiile din punct de vedere al atacurilor informatice. Acest risc era unul ridicat încă dinainte de pandemia de COVID-19, iar un raport al FBI arată că, la nivel global, pe întreg anul 2019 pierderile cauzate de atacuri informatice s-au ridicat la 3,5 miliarde USD, iar de la începutul anului 2020 până în prezent, aceste activități ilicite au crescut cu 37% lunar.

În multe cazuri, masurile de securitate informatica implementate funcţioneaza atât timp cât utilizatorul se afla în aria lor de protecție. Nu de puține ori se întâmpla ca o conexiune către mediul atacatorului să fie detectată și oprită de una dintre tehnologiile folosite de companii pentru a-și proteja datele: servere proxy, firewall, sistem de prevenire a intruziunilor (IPS) și lista poate continua, afișându-i utilizatorului și un eventual mesaj prin care îl anunță că traficul generat a fost blocat din motive de siguranță.

În momentul în care angajatul se conectează din altă locație, de acasă, de exemplu, adeseori aceste măsuri nu mai sunt eficiente, iar riscul de a fi ținta victima unui atac informatic crește exponențial, cu atât mai mult cu cât vorbim de o perioada mare de timp. Mai îngrijorător este faptul că nu toate atacurile informatice anunță utilizatorul că sistemul acestuia a fost compromis, astfel încât să se poată lua măsuri pentru remedierea acestei situații.

Dacă, în cazul unui atac de tip Ransomware, scopul este tocmai de a-l înștiința pe utilizator că datele lui au fost criptate urmând să plătească o sumă de bani pentru a le recupera, altele au ca metode de operare instalarea unor mecanisme de persistență pe stația infectată, pentru a putea fi ulterior exploatată în alte scopuri: participarea la o rețea de tip botnet, exfiltrarea de date, identificarea altor sisteme din rețea, mișcare laterală către acestea etc. Este de la sine înțeles că în cazul acestor scenarii atacatorul dorește să treacă neobservat pentru a beneficia de cât mai mult timp de resursele sistemului exploatat, datele din acesta și nu numai.

Este mai important ca niciodată acum pentru companiile care își reprimesc angații la birou ca, odată ce stațiile de lucru ale acestora se vor conecta din nou din aceeași rețea, sub aceeași „umbrelă", să fie pregătite din punct de vedere logistic și administrativ pentru a reduce suprafața de atac și riscul de a fi ținta unor atacuri informatice. Implementarea unor politici și procese de răspuns chiar de la primele semne ale unei anomalii în traficul generat este vitală dar trebuie completată și cu alte măsuri care să le dea substanță și aplicabilitate: achiziționarea unor tehnologii avansate care să automatizeze detecția și răspunsul la aceste incidente sau măcar actualizarea tehnologiilor de protecție deja existente sunt doar câteva dintre măsurile pe care ar trebui să le ia în considerare companiile.

La fel de importantă este pregătirea angajaților pentru a identifica semnele unui atac informatic și pașii pe care trebuie să îi urmeze pentru a-l evita. Aici trebuie avut în vedere atât o pregătire generală a întregului personal cu privire la riscurile la care se expun în mediul online, dar mai ales a celor care sunt îndreptățiți să răspundă și să stopeze aceste atacuri, activitate pe care companiile nu puneau foarte mult accent înainte de 2020.