Microsoft Security Intelligence | Tendințele anului 2018 în materie de securitate IT. România înregistreaza procentaje mai ridicate decât mediile mondiale la toate categoriile de atacuri

Microsoft a publicat raportul Microsoft Security Intelligence (SIR), ediția numarul 24, care ofera o perspectiva de ansamblu asupra evenimentelor și amenințarilor globale de securitate cibernetica ale anului 2018 și include o imagine a peisajului de securitate în domeniul IT, lecțiile învațate de specialiștii din domeniu și cele mai bune practici recomandate.

Pentru a crea acest raport, echipa SIR a analizat tendințele rezultate din datele colectate anonim la nivel global pe parcursul întregului an, prin numeroasele servicii și produse Microsoft. Au fost analizate peste 6,5 miliarde de incidente de securitate care trec prin cloud-ul Microsoft în fiecare zi și au fost adunate informații de la mii de cercetatori din domeniul securității din întreaga lume.

“Cunoaștem riscurile și investim anual peste 1 miliard de dolari pentru a înclina balanța în razboiul cibernetic, concentrându-ne în mod deosebit asupra a trei domenii: aplicarea acelor operațiuni de securitate care se potrivesc cel mai bine clienților noștri, dezvoltarea unei tehnologii de securitate de tip enterprise-class și stabilirea unor parteneriate în domeniul securității cibernetice, necesare pentru o lume eterogena.”, Adrian Georgescu, National Technology Officer, Microsoft Romania.

Raportul Microsoft Security Intelligence ofera date și pentru România, țara noastra înregistrând procentaje mai ridicate decât mediile mondiale la toate categoriile: atacuri tip pishing, minare ilicita de criptomonede, atacuri ransomware și atacuri prin malware.

Diferența cea mai mare fața de mediana înregistrata la nivelul Europei este la capitolul ratei de atacuri malware, România atingând un procentaj de 7,46%, cu 2,13 puncte procentuale mai mare decât rata medie la nivelul Europei. România întrece cu mult Cehia (3,44%), dar și Ungaria (6,21%) și Bulgaria (7,10%) la categoria atacurilor malware. O poziție și mai neplacuta la acest capitol o ocupa Serbia care înregistreaza o rata medie de 8,13% în ceea ce privește procentul mediu lunar al dispozitivelor afectate prin malware, depașind media la nivelul Europei cu 2,8 puncte procentuale.

A doua categorie la care România se poziționeaza deasupra mediei mondiale este procentul mediu lunar al dispozitivelor care s-au confruntat cu minarea ilicita de criptomonede. Media la nivel mondial atinge un procent de 0,11%, în timp ce în România rata ajunge la 0,26%. La acest capitol, Cehia pare ca se poziționeaza mult mai bine, cu o rata de doar 0,09%, în timp ce Serbia, de exemplu, depașește media la nivel mondial cu 0,23 puncte procentuale.

Principalele patru tendințe relevate în acest an de raportul Microsoft Security Intelligence sunt:

1. Atacurile ransomware sunt în scadere

Declinul atacurilor ransomware, observat în datele din 2018, este un exemplu relevant al modului în care comunitatea de securitate impune limitari atacatorilor cibernetici care sunt forțați sa își regândeasca metodele de atac.
Atacurile ransomware au scazut la nivel mondial cu pâna la 73% din luna ianuarie pâna în decembrie 2018. Ransomware-ul a reprezentat o amenințare uriașa pentru datele din 2017, iar declinul fața de anul 2018 este unul ușor de remarcat.

2. Minarea ilicita de criptomonede devine o amenințare

Declinul ransomware-ului apare ca fiind rezultatul trecerilor la noi metode de a monetiza atacurile cibernetice, iar minarea de criptomonede este una dintre metodele pe care atacatorii cibernetici le-au folosit pentru a-l înlocui. Minarea profitabila de monede necesita o cantitate imensa de putere de calcul, de aceea atacatorii instaleaza programe malware pe computerele utilizatorilor pentru a „sustrage" puterea de calcul necesara.
O tendința relevata este aceea ca pe masura ce crește sau scade valoarea criptomonedelor, la fel se întâmpla și cu rata de minare a acestora. Martie 2018 este luna care înregistreaza cel mai mare procent mediu lunar al dispozitivelor care s-au confruntat cu aceasta amenințare, cu o rata de 0,28% din totalul dispozitivelor fața de august 2018, luna în care rata scade pâna la un procent de 0,08%, în continuare semnificativ având în vedere miliardele de dispozitive conectate la internet în acest moment.

3. Sistemele digitale de livrare de software sunt în pericol

Atacurile asupra lanțului de aprovizionare software sunt o alta tendința pe care Microsoft o monitorizeaza de câțiva ani. O tactica utilizata de atacatori este aceea de a încorpora o componenta compromisa în pachetul de instalare al unei aplicații legitime sau într-o actualizare de software, care este apoi distribuita utilizatorilor prin intermediul canalelor oficiale. Aceste atacuri pot fi foarte greu de detectat, deoarece profita de încrederea pe care o au utilizatorii în furnizorii de software. Raportul conține câteva exemple care ilustreaza cât de mare poate fi amploarea acestor tipuri de atacuri, de exemplu utilizarea unui software neautorizat și/ sau piratat.
Creșterea adopției de Windows 10 și a utilizarii Windows Defender pentru protecție, înregistrate în anul 2018, sunt considerate motive potențiale în ceea ce privește scaderea globala a ratelor de atacuri de tip malware din cursul anului trecut.

4. Phishing-ul ramâne printre metodele de atac cele mai frecvente

Phishing-ul continua sa fie o metoda preferata de atacatorii din mediul cibernetic. La fel ca în cazul ransomware, se poate spune ca raufacatorii au schimbat tactica datorita instrumentelor și tehnicilor mai sofisticate care au fost implementate pentru a proteja utilizatorii. O metoda de pishing întâlnita este aceea cunoscuta sub denumirea de „domain spoofing", prin care un atacator utilizeaza un domeniu al unei companii pentru a-i folosi identitatea. Acest lucru se poate face prin trimiterea de e-mailuri cu nume de domenii false care în aparența sunt legitime sau prin crearea de site-uri web înșelatoare.
Graficul oferit de SIR în ceea ce privește procentajul de e-mailuri de pishing detectate din volumul total de e-mailuri analizate în mod anonim de Microsoft în întreaga lume arata o medie de 0,38% în anul 2018, cu o creștere spre finalul anului, luna noiembrie înregistrând o medie de 0,55% din totalul comunicarii pe e-mail la nivel global.