Atacurile tip ransomware au crescut cu **35% în 2015**, față de anul precedent.

(BSA Global Software Survey, Mai 2016)

Codurile de tip ransomware sunt softuri malițioase, care după ce se instalează în PC-ul victimei, îi criptează datele, ținându-le "ostatice" în scop de șantaj. Victima e adesea amenințată că i se vor publica datele, dacă nu plătește o răscumpărare.

Iată o listă cu acțiuni de urmat pentru a-ți securiza afacerea:

Securizează-ți dispozitivele.

Asigură-te că toate computerele, telefoanele, tabletele și serverele au instalate programe antivirus și firewall eficiente și la zi. Actualizează-ți cu regularitate sistemul de operare și aplicațiile. Monitorizează-le cu ajutorul unui software de management, precum Microsoft Enterprise Mobility + Security.

Monitorizează-ți rețeaua.

Instalează software de prevenire și detecție a atacurilor asupra rețelei interne, pentru a identifica orice comportament neobișnuit și pentru a îngreuna accesul hackerilor la sistemele firmei. Atacatorii pot rămâne nedetectați timp de peste șase luni, așa că trebuie să cauți semnele incipiente de intruziune, cum ar fi conectări din locații necunoscute, comportament automat sau repetitiv și să verifici accesul prin autentificarea multiplă.

Actualizează-ți planul de securitate IT.

Un plan bun și concis te va ajuta să fii sigur că nu ratezi nimic și că ai o abordare consecventă asupra securității afacerii. Actualizează-l cu regularitate.

Fă backup de date.

Un backup bun reprezintă o ultimă linie de apărare importantă. Nu trebuie să plătești un infractor pentru a-ți decripta fișierele dacă ai copii de backup care nu au fost infectate cu ransomware. Asigură-te că faci backup tuturor datelor și că testezi backup-urile cu regularitate, pentru a fi sigur că funcționează.

Monitorizează aplicațiile bazate pe cloud și activitățile IT neconforme.

Politicile cu privire la aplicațiile cloud, SaaS și BYOD creează provocarea imensă pentru orice companie de a defini standarde de securitate foarte ridicate care nu permit compromisuri. Pentru a veni în întâmpinarea acestei provocări, evaluează utilizarea actuală a aplicațiilor SaaS permise și nepermise, oferind totodată flexibilitatea diferitelor tipuri de dispozitive. Analizează accesul și implementează controale și măsuri de securitate pentru a ajuta utilizatorii să fie productivi pe platformele preferate, protejați totodată de o soluție de încredere pentru companii și administratori.

Filtrează-ți e-mailul și conexiunea la internet.

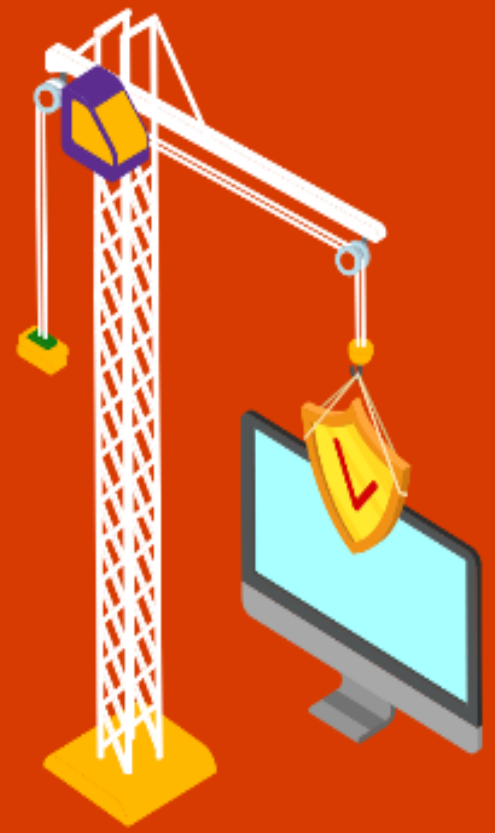
Este un sfat vechi și cunoscut, însă în continuare esențial: utilizează un firewall, software de scanare a emailului și a site-urilor web în cloud sau gateway-ul dintre rețeaua internă și internet, pentru a bloca malware-ul înainte să ajungă la angajați. De asemenea, este important să te asiguri că toți utilizatorii și toate sistemele tale sunt protejate, inclusiv utilizatorii de la distanță, serverele, sistemele nesupravegheate și dispozitivele mobile.

Riscul de **expunere la malware** este de **33%**, atunci când instalezi un program piratat sau cumperi un dispozitiv cu programe piratate deja instalate.

Studiu IDC "Legătura dintre software-ul piratat și brețele de securitate informatică", martie 2014.

În anul 2015 a fost identificat un număr de **430 de milioane** de noi coduri malware.

2016 Symantec Internet Security Threat Report, Volume 21, p. 5



Legea se aplică în cazul **oricărui** tip de produs, inclusiv software.

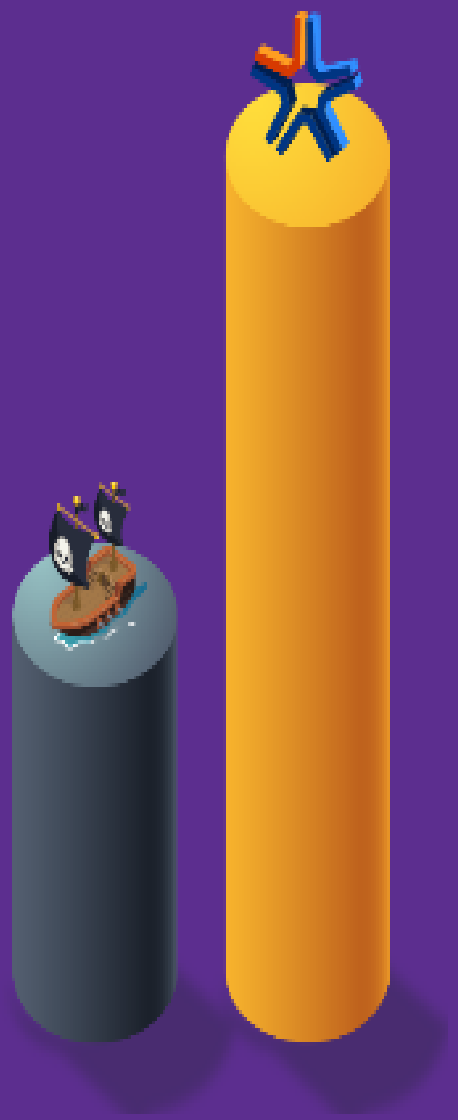
Așa cum nu ai ieși din magazin cu o haină, fără să plătești, nu este indicat nici să folosești un software fără licență originală. Și la fel cum eviți hainele de proveniență îndoielnică, **evită și softurile nelicențiate.**

Legea se aplică în cazul **oricărui** tip de produs, inclusiv software.

Așa cum nu ai ieși din magazin cu o haină, fără să o plătești, nu este indicat nici să folosești un software fără licență originală. Și la fel cum eviți hainele de proveniență îndoielnică, **evită și softurile nelicențiate**.

Asistența tehnică este **garantată** doar de o licență originală Microsoft.

E ca și cum ai avea **access direct la experții noștri**, la orice oră din zi și din noapte, pentru orice probleme legate de software-ul deviceului tău.



Un software cu licență e **mereu updatat** și prin urmare, are o durată de viață mai lungă decât unul piratat.

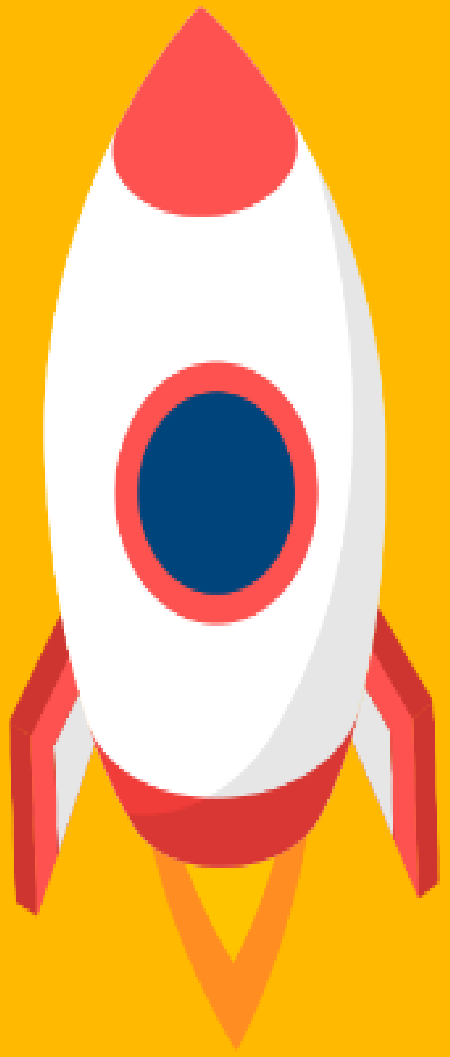
Protejează documentele importante!

Protejează documentele importante, folosind programe originale. Nu vrei ca intimitatea ta, sau munca ta de o viață, sa fie vreodată în pericol. Programele piratate prezintă un risc sporit de erori de funcționare, care pot deteriora documentele importante. În plus, cresc și șansele ca persoane rău-intenționate să aibă acces la documentele și fotografiile personale.

Doar în 2015 au existat **peste jumătate de miliard** de situații în care s-au furat sau s-au pierdut informații personale.

Asta înseamnă **de peste 27 de ori** echivalentul populației actuale a României.

(2016 Symantec internet Security Threat Report, Volume 21, p. 54.)



Cele mai bune performanțe

Cele mai bune performanțe sunt garantate doar cu programele originale. Cele piratate au suferit modificări, de cele mai multe ori, funcționalitatea lor poate fi afectată.

Adică exact diferența de calitate dintre o haină originală și un produs contrafăcut, care se poate descoase oricând.

Siguranța informațiilor **vitale**

Siguranța informațiilor tale vitale e pusă în pericol de programele cu proveniență incertă. o licență originală îți oferă **un nivel ridicat de încredere** că persoanele rău-voitoare nu vor avea acces la datele tale importante - de la conturile tale bancare, până la parolele de mail, pinuri, conturi de cloud...

SURSA

https://www.microsoft.com/ro-ro/romania/antipiraterie/

- https://www.microsoft.com/en-us/security/intelligence?3e5a1f28-58ad-4e5d-8e4b-1cf6c498b66f=1

- https://www.microsoft.com/security/intelligent-security-story/#

https://www.microsoft.com/ro-ro/rethink-IT-security/malware.aspx

- https://www.microsoft.com/en-us/security/intelligence?3e5a1f28-58ad-4e5d-8e4b-1cf6c498b66f=1

- https://www.microsoft.com/security/intelligent-security-story/#