HAMOR Soft
2017.05.13

Despre virusul WannaCry (WannaCrypt)

A apărut un nou virus de tip ransomware (de răscumpărare), care afectează şi România. Este cel mai periculos atac ransomware și cel mai mare atac cibernetic înregistrat până în prezent, după părerea specialiştilor.

Se răspândeşte pe calculatoarele cu sistemul de operare Windows.

Nu sunt afectate serverele Linux pe care rulează programele HAMOR Soft.

Ce trebuie făcut pentru a minimaliza efectele virusului:

1. Actualizaţi Windows-ul!
   - Windows update pe sistemele mai noi (Win 7, Win 8.1, Win 10)
   - Pe sistemele mai vechi (XP, Vista, 2003,…) trebuie actualizat manual

   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks

   Lista patchurilor descarcabile este:

   http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

   De exemplu pentru XP SP3 se alege:

   Security Update for Windows XP SP3 (KB4012598) **Descărcare**

   Iar din meniul care apare, de exemplu pentru XP în limba engleză, se alege:

   windowsxp-kb4012598-x86-custom-enu_eceb7d5023bbb23c0dc633e46b9c2f14fa6ee9dd.exe

2. Verificaţi şi actualizaţi programul antivirus folosit!
   Nu lucraţi cu calculatoare fără program antivirus sau cu antivirus expirat

3. Salvaţi datele pe un suport extern, care nu este conectat tot timpul la calculator!
   Salvările le puteţi face cu hUTIL – Salvare pe suport ales
   Verificaţi dacă se fac backupuri zilnice (distincte) ale bazelor de date ale programelor HAMOR Soft.

4. Nu deschideţi ataşamente sau linkuri dubioase, de la persoane necunoscute!

5. În meniul hSTART de conectare la serverul Linux **nu** folosiţi modul Admin cu **D** (DA) numai în cazuri neapărat necesare!

Pentru informaţii suplimentare luaţi legătura cu distribuitorul dumneavoastră, mai ales în eventualitatea infectării cu virus.

În cazul infectării vă recomandăm să:
- deconectaţi imediat de la rețea staţiile afectate
- luaţi legătura cu specialişti (distribuitori)
- dezinfectați staţiile
- restaurați copiile de siguranță (backup)

Pe lângă multele ştiri de pe internet şi televiziune, inclusiv Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică (CERT-RO) a publicat un comunicat despre virus (cum funcţionează şi recomandări pentru prevenirea infectării):

https://cert.ro/citeste/wannacry-ransomware-alerta

Documentul oferă o descriere detaliată a modului în care funcţionează noua variantă de virus precum şi a măsurilor minime pe care utilizatorii trebuie să le respecte pentru prevenirea infectării sau pentru diminuarea daunelor produse în eventualitatea infectării.

CERT-RO vă recomandă implementarea măsurilor cuprinse în „Ghidul privind combaterea ameninţărilor informatice de tip ransomware", disponibil la adresa:

https://cert.ro/vezi/document/ghid-protectie-ransomware