WannaCry Ransomware – šta činiti, kako sprečiti?

Za kućne korisnike i male firme

1. Ažurirajte, update-ujte (patch-ujte) Windows. Ključno je da instalirate MS17-010 patch. Više informacija: https://support.microsoft.com/en-us/help/4013389

2. Ažurirajte vaš antivirus i pobrinite se da radi. Ako nemate antivirus instaliran, krajnje je vreme da ga instalirate – možete da upotrebite čak i besplatni Microsoft Defender: https://www.microsoft.com/en-us/windows/windows-defender ako ne želite da kupite druga, komercijalna rešenja (na primer, Norton Security: https://ie.norton.com/norton-security-for-one-device).

3. Obavezno napravite rezervnu kopiju podataka (backup) sa računara i servera, sačuvajte sve što vam je važno – bilo ručno, kopiranjem na eksterni disk ili na neki "cloud" disk kao što je Google Drive, Box ili Microsoft OneDrive – nakon toga, ako ste koristili eksterni disk ne ostavljajte ga priključenog na računar, već ga sklonite do sledećeg pravljenja rezervne kopije. Backup možete da uradite i sa komercijalnim rešenjima na bolji, sigurniji i brži način (na primer, Norton Security Premium ima i ugrađen backup: https://ie.norton.com/norton-security-with-backup, ili Backup Exec ako imate servere u firmi: http://www.backupexec.com).

4. Upozorite sve koji rade sa računarima da ne klikću na linkove u email porukama od nepoznatih pošiljaoca, niti da otvaraju priloge (attachements) u email porukama od nepoznatih pošiljaoca, posebno ako su u pitanju arhive (.zip, .rar), Word, Excel ili PDF dokumenti, izvršni fajlovi (.com, .exe) ili fajlovi sa .js.

Za srednja i velika preduzeća

1. Ažurirajte sve Windows sisteme, posebno obratite pažnju na **MS17-010** patch. Proverite da li svi računari i serveri, uključujući i one kod kojih je prestala podrška Microsoft-a kao što su Windows XP i Server 2003 imaju instaliran MS17-010 patch. Microsoft je objavio i za ove sisteme zakrpe (patch). Više informacija: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx. Proveru možete da uradite preko sistema za upravljanje ažuriranjem, kao što je Microsoft WSUS ili System Centar (ako ih koristite), pomoći komercijalnih rešenja kao što je **Shavlik** (Patch Management, povoljno, a vrlo efikasno rešenje koje se jednostavno koristi: https://www.ivanti.com/products/patch-management).

   Proveru možete da izvršite i ručno kroz Command Prompt pomoću komande:

   `wmic qfe` – ispisuje sve instalirane patch-eve sa datumom primene
   `wmic qfe get hotfixid` – ispisuje samo KB broj instaliranih patch-eva
   `wmic /node:<ime servera> qfe` – proverava patcheve na udaljenom serveru

   Primer:
   `wmic qfe | find "KB4012213"` – proverava patch za Windows 2012 R2
   `wmic qfe | find "KB4012216"` – provera kumulativnnog patch-a za Win 2012 R2

Net++ technology d.o.o.
Bul. vojvode Mišića 39a, 11040 Beograd, Srbija
Tel. (011) 36-999-67, 4053-516, 4053-519 | Fax. (011) 4053-447
PIB: 100219596 | Mat.br.: 17413341
www.netpp.rs | office@netpp.rs

2. Tamo gde nemate vremena ili ne možete da instalirate update, onemogućite **SMBv1**. Više informacija: https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012.

   Za radne stanice:
   Otvorite **Control Panel**, kliknite na **Programs**, i zatim na **Turn Windows features on or off**.
   U Windows Features prozoru, odštiklirajte **SMB1.0/CIFS File Sharing Support** checkbox i zatim kliknite na **OK** da zatvorite prozor.
   Restartujte sistem.

   Za servere:
   Otvorite **Server Manager** i zatim kliknite na **Manage** meni i izaberite **Remove Roles and Features**.
   U Features prozoru, odštiklirajte **SMB1.0/CIFS File Sharing Support** check box, i zatim kliknite na **OK** da zatvorite prozor.
   Restartujte sistem.

3. Ažurirajte vaš **antivirus** (pobrinite se da svi računar i serveri imaju ažuran antivirus) ili **endpoint protection** rešenje. Instalirajte antivirus/endpoint protection na servere i ostale sisteme (bankomate na primer), ako ih do sada već niste instalirali. Pratite u centralnoj konzoli za upravljanje šta se dešava i da li su svi sistemi zaštite aktivni i ažurni, pratite upozorenja i detekcije. Ako još uvek koristite standardni, klasični antivirus pređite na napredna rešenja kao što je **Symantec Endpoint Protection** (https://www.symantec.com/products/endpoint-hybrid-cloud-security/endpoint/endpoint-protection) ili **Palo Alto Network Traps** (https://www.paloaltonetworks.com/products/secure-the-endpoint/traps).

4. Ako već nemate sistem za zaštitu email saobraćaja – hitno ga nabavite – na primer, **Symantec Email Security.cloud** može da se implementira u roku od nekoliko sati (https://www.symantec.com/products/messaging-security/email-security-cloud). Proverite vaša pravila (polise) na sistemima za email zaštitu i zaustavite (ili smestite u karantin) sve poruke koje sadrže potencijalno opasne fajlove (sa makroima, izvršnim kodom, skriptovima) i linkove. Uključite restriktivnije polise tokom ovog perioda kako bi povećali nivo zaštite (na primer one koje uklanjaju mogućnost da se klikne na link u porukama).

5. Proverite zaštitu i polise na vašem web proxy sistemu i/ili firewall-u. Kontrolišite sve izvršne fajlove koji prolaze kroz proxy i/ili firewall. Aktivirajte restriktivnije polise za zaštitu web saobraćaja (uključujući i aktiviranje dekripcije SSL saobraćaja) tokom ovog perioda povećane opasnosti. Rešenja koja nude veći stepen zaštite od standardnih su firewall uređaji nove generacije, kao što je **Palo Alto Networks** (https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall) i/ili web proxy kao što je **Symantec/Blue Coat ProxySG i ASG** (https://www.symantec.com/products/web-and-cloud-security/secure-web-gateway-proxy-sg-and-asg).

Net++ technology d.o.o.
Bul. vojvode Mišića 39a, 11040 Beograd, Srbija
Tel. (011) 36-999-67, 4053-516, 4053-519 | Fax. (011) 4053-447
PIB: 100219596 | Mat.br.: 17413341
www.netpp.rs | office@netpp.rs

6. **Proverite laptop računare koji su bili van mreže od petka, 12. 05. 2017.g. – nemojte ih priključivati na vašu lokalnu mrežu pre provere/skeniranja!**

7. Proverite stanje backup-a i ako je potrebno uradite ručni, hitni backup ključnih resursa. Ako već niste implementirali, sada je kranje vreme da uvedete backup rešenje u firmu: **Veritas Backup Exec** (http://www.backupexec.com) ili **Veritas NetBackup** (http://www.netbackup.com) su vodeća rešenja za backup podataka i sistema u preduzećima, kako virtuelnih, tako i fizičkih.

8. **Obavestite zaposlene o povećanom nivou opasnosti od ransomware-a** i upozorite ih da obrate više pažnje na email poruke od nepoznatih pošiljaoca, kao i da ne otvaraju priloge (attachements) u email porukama od nepoznatih pošiljaoca, posebno ako su u pitanju arhive (.zip, .rar), Word, Excel ili PDF dokumenti, izvršni fajlovi (.com, .exe) ili fajlovi sa .js. Dobro bi bilo da ih o ovome obavestite pre nego što uključe računare.

9. Informišite se o trenutnom stanju – **portal IT klinika** je odličan izvor informacija (http://www.it-klinika.rs), kao i naše
LinkedIn (https://www.linkedin.com/company/netpp i https://www.linkedin.com/company/it-klinika),
Facebook (https://www.facebook.com/itklinika.rs i https://www.facebook.com/netpptechnology) i
Twitter (https://twitter.com/IT_klinika **i** https://twitter.com/netpptechnology) - **@IT_klinika** i **@NetPPtechnology.**

Net++ technology d.o.o.
Bul. vojvode Mišića 39a, 11040 Beograd, Srbija
Tel. (011) 36-999-67, 4053-516, 4053-519 | Fax. (011) 4053-447
PIB: 100219596 | Mat.br.: 17413341
www.netpp.rs | office@netpp.rs