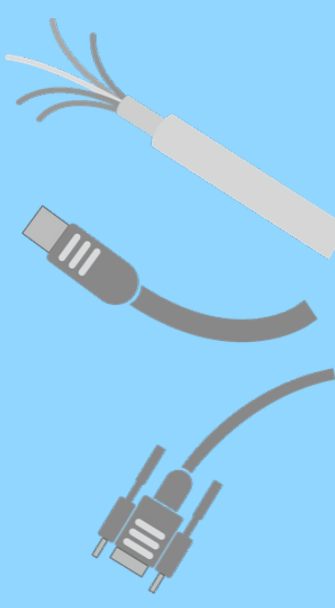
# CHECKLISTA U SLUČAJU RANSOMWARE NAPADA

Ransomware je vrsta malvera koja preuzima kontrolu nad mašinom ili fajlovima žrtve, a zatim traži otkupninu za njih . Ova checklista treba da vam pomogne u slučaju da ste žrtva ransomwarea.



## 1 KORAK 1: *Diskonektujte sve*

- [ ] Diskonektujte sve
- [ ] Isključite sve wireless funkcije: Wi-Fi, Bluetooth, NFC.

## 2 KORAK 2: *Utvrdite razmere infekcije; proverite da li je došlo do enkripcije na sledećim mestima:*

- [ ] Mapirani i zajednički diskovi.
- [ ] Mapirani i zajednički folderi sa drugih računara.
- [ ] Svi uređaji koji služe kao mrežno skladište.
- [ ] Eksterni hard diskovi.
- [ ] Svi USB uređaji (USB flash, memorijske kartice, povezani telefoni/kamere).
- [ ] Cloud skladišta: DropBox, Google Drive, OneDrive itd.

## 3 KORAK 3: *Odredite vrstu ransomwarea*

- [ ] Koja vrsta/tip ransomwarea je u pitanju? Na primer: CryptoLocker, TeslaCrypt itd

**Savet:** Posetite sajt https://www.nomoreransom.org - ovde na osnovu krptovanih fajlova možete da odredite koji konkretno ransomeware je u pitanju i da li za isti postoji dekriptor.

## 4 KORAK 4: *Izaberite odgovor/reakciju na ransomware infekciju*

Sada kada ste saznali razmere infekcije (količinu zaraženih/zaključanih fajlova) i kada znate sa kojom vrstom ransomwarea imate posla, možete doneti kvalitetniju odluku o vašem sledećem potezu.

### *Reakcija 1: Vratite fajlove iz backupa*

- [ ] 1. Uklonite ransomware iz zaraženog sistema.
- [ ] 2. Locirajte backup:
  - a. Proverite da li su tu svi fajlovi koji su vam potrebni.
  - b. Verifikujte integritet backupa (npr. da li ima fajlova koji se ne učitavaju ili su oštećeni).
  - c. Proverite Shadow kopije ako ste u mogućnosti (moguće je da neće pomoći kod novijih vrsta ransomwarea).
  - d. Proverite da li ima ranijih verzija fajlova koje su sačuvane u cloudu (DropBox, Google Drive, OneDrive itd.).
- [ ] 3. Vratite (restore) fajlove iz backupa.

KLINIKA

KLINIKA

## Reakcija 2: Pokušavate da dekriptujete fajlove

- [ ] 1. Odredite vrstu i verziju ransomwarea ako je to moguće (pogledajte Korak 3.)
- [ ] 2. Pronađite dekriptor (možda ne postoji za novije vrste).

Ako ste uspeli da ga pronađete, napravite sledeće korake:

- [ ] 3. Povežite sva skladišta koja imaju kriptovane fajlove (hard diskove, USB memorije itd.).
- [ ] 4. Dekriptujte fajlove.

## Reakcija 3: Odlučili ste da ne reagujete (gubite fajlove)

- [ ] 1. Uklonite ransomware.
- [ ] 2. Napravite backup kriptovanih fajlova ukoliko se pojavi dekriptor u budućnosti (opciono).

## Reakcija 4: Odlučili ste da pregovarate i/ili platite otkupninu napadačima

Plaćanje otkupnine NE PREPORUČUJEMO! Na taj način finansirate sajber kriminal i pomažete razvoj još naprednijih ransomwarea i drugih malvera.

- [ ] 1. Ukoliko je moguće, probajte da dogovorite manju cenu otkupnine i/ili duži period isplate.
- [ ] 2. Utvrdite prihvatljivi način plaćanja za konkretnu vrstu ransomwarea (Bitcoin itd.).
- [ ] 3. Pripremite se za plaćanje (najverovatnije će vam trebati Bitcoini):
  - a. Pronađite menjačnicu preko koje želite da kupite Bitcoine (vreme je ključno).
  - b. Napravite nalog/wallet i kupite Bitcoine.
- [ ] 4. Konektujte zaraženi računar na internet.
- [ ] 5. Instalirajte TOR browser (opciono).
- [ ] 6. Pronađite adresu za Bitcoin plaćanje. Ona se nalazi ili u ransomware poruci na ekranu ili na TOR sajtu koji je napravljen u ove svrhe.
- [ ] 7. Platite otkupninu: Prebacite Bitcoine u ransom wallet.
- [ ] 8. Povežite sve uređaje koji sadrže kriptovane fajlove sa vašim računarom.
- [ ] 9. Dekripcija fajlova bi trebalo da počne u periodu od 24h nakon plaćanja, a češći je slučaj da se to obavi u prvih nekoliko sati nakon plaćanja.

## Korak 5: Koraci za zaštitu u budućnosti

- [ ] Implementirajte Checklistu za prevenciju ransomwarea kako biste sprečili buduće napade. (Ovu listu pronaći ćete u nastavku)

# CHECKLISTA ZA PREVENCIJU RANSOMWAREA


Ako ne želite da postanete žrtva ransomwarea, ili ne želite da se ponovo nađete u situaciji da su vaši podaci taoci sajber kriminalaca, savetujemo vam da primenjujete sledeće preventivne korake:

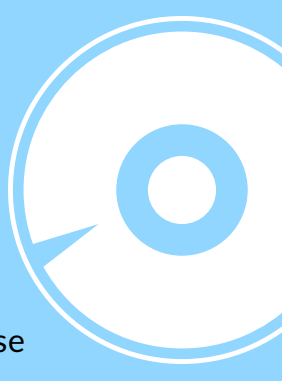
## 1 PRVA LINIJA ODBRANE: *Korisnici*

- [ ] 1. Implementirajte odgovarajući edukativni trening o bezbednosnim opasnostima kako bi korisnici znali kako da spreče preuzimanje i/ili izvršavanje opasnih aplikacija.
- [ ] 2. Sprovedite simulaciju phishing napada kako biste upoznali korisnike sa aktuelnim pretnjama.

## 2 DRUGA LINIJA ODBRANE: *Softver*

- [ ] 1. Proverite da li imate firewall (i da li je u funkciji).
- [ ] 2. Implementirajte antispam i/ili antiphishing. Ovo možete uraditi ili pomoću softvera ili preko hardvera namenjenog isključivo za te svrhe, poput Barracuda uređaja ili preko cloud servisa, kao što je Symantec Email Security.cloud.
- [ ] 3. Proverite da li svi zaposleni u organizaciji koriste neki od vrhunskih antivirus softvera (i da li se redovno ažuriraju), odnosno antivirusa sledeće generacije, kao što je Symantec Endpoint Protection.
- [ ] 4. Implementirajte polise za restrikciju softvera u vašoj mreži kako biste sprečili pokretanje neautorizovanih aplikacija (opciono).
- [ ] 5. Implementirajte rigoroznu proceduru zakrpa kojom se ažuriraju pojedine ili sve aplikacije koje imaju ranjivosti.

## 3 TREĆA LINIJA ODBRANE: *Backup*



- [ ] 1. Implementirajte backup rešenje – softversko, hardversko ili oba.
- [ ] 2. Proverite da li su backupovani svi fajlovi koji su vam potrebni , uključujući i fajlove iz mobilnih uređaja i sa USB-a.
- [ ] 3. Proverite da li su fajlovi na sigurnom, da li su redundantni i da li im se može jednostavno pristupiti.
- [ ] 4. Redovno testirajte funkcionalnost vraćanja (recovery) fajlova pomoću backup/restore procedura. Testirajte integritet fajlova u fizičkom backupu i jednostavnost vraćanja fajlova (ease-of-recovery) iz online i/ili softverskih backupa.

Borba protiv ransomwarea je neprekidan proces i sve provere moraju da se vrše redovno. Redovno ažuriranje softvera i znanja korisnika, kroz edukaciju o pretnjama, od ključne su važnosti za uspešnost borbe protiv ove, ali i mnogih drugih sajber pretnji.

KLINIKA

**www.it-klinika.rs**


NetPP TECHNOLOGY

www.netpp.rs office@netpp.rs +381 11 3699 967