

AKCIONI PLAN za zaštitu od ransomwara

KORAK 1:

- Napravite inventar kritičnih podataka
- Proverite postojeće backup procedure
- Inicirajte razgovor o sajber bezbednosti sa upravom

KORAK 2

- Organizujte osnovnu obuku o prepoznavanju phishinga
- Proverite podešavanja firewalla
- Ažurirajte sve sisteme i aplikacije

KORAK 3

- Implementirajte višefaktorsku autentifikaciju
- Razvijte osnovni plan reagovanja na incidente
- Testirajte procedure za oporavak podataka

KORAK 4

- Sprovedite prvu simulaciju phishing napada
- Dokumentujte sve procedure
- Uspostavite redovan ritam provera i ažuriranja