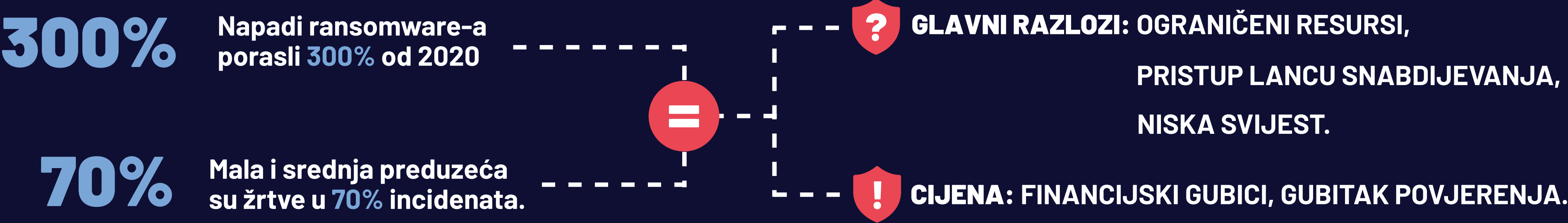


POLITIKE I PRAKSE
CYBER SIGURNOSTI
ZA MALA I SREDNJA
PREDUZEĆA U BIH



10 HITNIH KORAKA



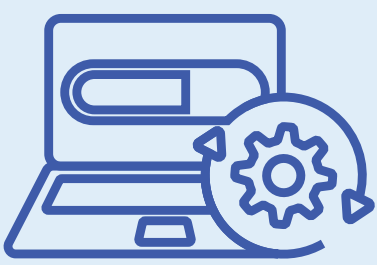
DANI OD 1. DO 30. – SIGURNOSNE MJERE



Omogućite višefaktorsku autentifikaciju (MFA) na kritičnim računima (e-mail, cloud).



Implementirajte automatizirane sigurnosne kopije (dnevne, van lokacije).



Nadogradite i instalirajte zakrpe za sve sisteme.



Implementirajte zaštitu krajnjih tačaka (antivirus poslovnog nivoa).



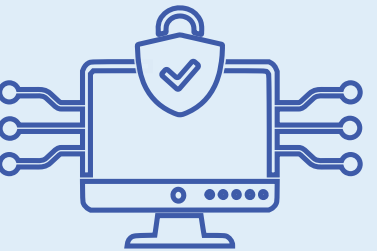
DANI OD 31. DO 60. – KONTROLA PRISTUPA I NADZOR



Implementirajte upravljanje lozinkama (upravitelj lozinke, jake lozinke).



Konfigurirajte osnovnu mrežnu sigurnost (firewall, segmentacija).



Uspostavite osnovni sigurnosni nadzor (logovi, upozorenja).



Kreirajte sigurnosne politike i procedure (prihvatljiva upotreba, incidente).



DANI OD 61. DO 90. OBUKA I PRIPRAVNOST ZA INCIDENTE



Provesti obuku o sigurnosti (phishing simulacije).



Razviti procedure za odgovor na incidente (koga kontaktirati).



CILJ: IZGRADNJA OTPORNE ODBRANE.

POČNITE SADA – SAVRŠENA SIGURNOST NIJE MOGUĆA, ALI OVO VAS ČINI MANJE ATRAKTIVNOM METOM!