Udruženje
e-Transformacija

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

300% Napadi ransomware-a porasli 300% od 2020

70% Mala i srednja preduzeća su žrtve u 70% incidenata.

GLAVNI RAZLOZI: OGRANIČENI RESURSI, PRISTUP LANCU SNABDIJEVANJA, NISKA SVIJEST.

CIJENA: FINANCIJSKI GUBICI, GUBITAK POVJERENJA.

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 lozinki, jake lozinke).
- Konfigurišite 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!

Ova infografika je izrađena u okviru SEDEP programa, koji sufinansiraju Njemacko savezno ministarstvo za ekonomsku saradnju i razvoj (BMZ), Evropska unija i Švicarska vlada. Sadržaj ove infografike isključiva je odgovornost Udruženja e-Transformacija i ne odražava nužno stavove njemačke vlade, švicarske vlade ili Evropske unije.

Sufinansira Europska unija
Switzerland.
german cooperation
DEUTSCHE ZUSAMMENARBEIT
Implemented by
giz