VODIČ ZA CYBER SIGURNOST ZA MALA I SREDNJA PREDUZEĆA

Odabir partnera za cyber sigurnost je strateški izbor koji može značajno uticati na otpornost organizacije prema cyber napadima i njen dugoročni uspjeh.

British Embassy Sarajevo

CHEVENING

Cranfield University

WOMEN 4CYBER BOSNIA AND HERZEGOVINA

13 MJERA CYBER OTPORNOSTI

UPRAVLJANJE IMOVINOM

Napravite listu svih uređaja, aplikacija i usluga koje koristite. Obezbijedite da je popis imovine u svakom trenutku ažuran.

SIGURNOST LANCA SNADBDIJEVANJA

Kreirajte listu svih dobavljača i partnera, te identificirajte one koji predstavljaju najveći rizik. Jasno definirajte odgovornosti u slučaju incidenta.

KLASIFIKACIJA PODATAKA

Klasifikacirajte podatake na osnovu njihove osjetljivosti i važnosti. Jasno definišite odgovornost nad podacima.

OBUKA I PODIZANJE SVIJESTI

Kreirajte ažuran i kreativan plan obuke i kontinuirano ga sprovodite za sve zaposlenike. Redovno provodite simulacije i praktične vježbe. Uključite analizu stvarnih i simuliranih incidenata.

UPRAVLJANJE RIZICIMA

Implementirajte adekvatnu metodu upravljanja rizicima. Identificirajte rizike i implementirajte kontrole minimizacije rizika. Kontinuirno radite revizije rizika.

UPRAVLJANJE INCIDENTIMA

Pripremite sveobuhvatan plan odgovora na incidente. Formirajte tim, uključite relevantne osobe, te uspostavite kriterije za eskalaciju. Redovno provodite vježbe odgovora na incidente.

UPRAVLJANJE IDENTITETOM I PRISTUPOM

Uspostavite kontrolu pristupa podacima ovlaštenim osobama. Implementirajte višefaktorsku autentikaciju. Kontinuirano nadzirite pokušaje pristupa.

LOGIRANJE I MONITORING

Omogućite logiranje u svim kritičnim sistemima i aplikacijama Obezbijedite da su svi logovi sigurno pohranjeni na centraliziranoj lokaciji. Zaštitite logove od izmjena i neovlaštenog brisanja.

UPRAVLJANJE UREĐAJIMA I RANJIVOSTIMA

Održavajte standardizirane sigurnosne konfiguracije na svim uređajima kako biste minimizirali rizike od ranjivosti. Redovno sprovodite automatsko otkrivanje ranjivosti.

REZERVNE KOPIJE

Redovno kopirajte poslovne i konfiguracijske podatke. Implementirajte 3-2-1 strategiju pohrane kopija podataka. Redovno testirajte rezervne kopije.

KONTINUIRANA NADOGRADNJA

Omogućite automatska ažuriranja za sve uređaje i aplikacije. Uspostavite redovan raspored za ručno ažuriranje.

RAD NA DALJINU

Implementirajte sigurnosne protokole za pristup resursima sa udaljenih lokacija. Uspostavite višefaktorsku autentikaciju.

SIGURNOST PODATAKA

Osigurajte da su svi podaci, u prenosu i mirovanju, zaštićeni implementacijom enkripcije podataka. Implementirajte fizičke i logičke kontrole pristupa

https://smesecurity.ba