Sufinansira Europska unija

Switzerland.

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

# PREPORUČENE PRAKSE, ALATI I RESURSI

## ZA UNAPRJEĐENJE CYBER SIGURNOSTI ČLANICA BIZNIS UDRUŽENJA I ORGANIZACIJA

Udruženje
e-Transformacija

Sarajevo, 2025.

## Sadržaj

## Uvod

U današnjem poslovnom okruženju, digitalna transformacija nije samo prednost, ili luksuz, već i nužnost, odnosno osnovni preduslov za opstanak i rast. Mala i srednja preduzeća sve češće se oslanjaju na tehnologiju, odnosno na digitalne alate za gotovo svaki aspekt poslovanja: od interne i eksterne komunikacije, preko prodaje i marketinga, pa sve do upravljanja dokumentima, bazama podataka i korisničkim informacijama. Međutim, kako se povećava stepen digitalizacije, proporcionalno raste i izloženost raznovrsnim cyber prijetnjama. Ransomware napadi, krađa podataka, lažni e-mailovi (phishing), i kompromitovane lozinke – to su realne opasnosti koje svakodnevno pogađaju i male i srednje velike firme, a ne samo velike korporacije. Upravo zato, **cyber sigurnost više nije tehničko pitanje rezervisano za IT odjel – ona postaje sastavni dio šire poslovne strategije svake organizacije.**

Udruženja poput biznis udruženja i organizacija koja okupljaju mala i srednja preduzeća, imaju jedinstvenu i odgovornu poziciju u ovom procesu. One mogu (i treba da) djeluju kao:

- **Edukatori** – pružajući članicama pristup znanju, obukama i smjernicama o digitalnoj sigurnosti;
- **Posrednici** – povezujući firme s provjerenim pružaocima sigurnosnih rješenja i savjetnicima;
- **Lideri** – aktivno promovišući kulturu sigurnosti kroz vlastite politike, kampanje i projekte.

Kao takvi, oni imaju moć da podignu svijest, smanje ranjivost sektora i ojačaju ukupnu digitalnu otpornost ekonomije.

### Ovaj vodič – u službi praktičnih rješenja

Ovaj dokument razvijen je kao **praktični alat** koji biznis udruženjima i organizacijama i njihovim članicama nudi:

- Jasne preporuke za svakodnevnu zaštitu podataka i sistema;
- Konkretne alate i resurse prilagođene malim i srednjim firmama;
- Smjernice kako prepoznati, reagovati i spriječiti najčešće digitalne prijetnje.

**Cilj: Osnovno razumijevanje i pametna praksa, ne tehnička ekspertiza**

Nije cilj da svaka firma postane ekspert za IT sigurnost. Cilj je mnogo jednostavniji – a istovremeno dalekosežan: **izgraditi osnovno razumijevanje cyber rizika i usvojiti jednostavne, ali učinkovite sigurnosne navike.** Baš te svakodnevne prakse – poput upotrebe jakih lozinki, redovnog ažuriranja softvera, ili opreznog rukovanja e-mailovima – mogu biti presudne u sprečavanju potencijalno skupih i štetnih incidenata.

**Konačno**, digitalna sigurnost je zajednička odgovornost svih – pojedinaca, firmi i organizacija. Biznis udruženja i organizacije imaju priliku da budu pokretač te promjene.

# Zašto biznis udruženja i organizacije moraju brinuti o cyber sigurnosti?

## Cyber sigurnost – zajednička odgovornost u digitalnom dobu

U savremenom poslovnom okruženju, gdje je digitalna tehnologija postala osnova gotovo svih operacija, pitanje cyber sigurnosti ne može više biti ograničeno samo na IT odjeljenja. Sve veći broj incidenata pokazuje da sigurnost nije tehnički izazov rezervisan za stručnjake, već **zajednička odgovornost svih aktera u poslovnom ekosistemu** – od rukovodilaca i zaposlenih, do partnera, dobavljača i sektorskih udruženja.

Biznis udruženja i organizacije, koje okupljaju desetine, pa i stotine malih i srednjih preduzeća (MSP-ova), imaju posebno značajnu ulogu u ovom kontekstu. Mnoge firme koje su članice ovakvih udruženja **nemaju sopstveni IT sektor**, niti pristup specijalizovanim znanjima ili alatima za prevenciju i odgovor na sigurnosne prijetnje. U tom smislu, biznis udruženja i organizacija nisu samo platforme za povezivanje, već i potencijalni **stubovi digitalne otpornosti** svojih članova.

Prema **ENISA Threat Landscape Reportu za 2024. godinu**, više od **40% svih zabilježenih cyber napada u 2023. bilo je usmjereno na MSP-ove**. Ovi napadi nisu više ručno usmjereni ni tehnički kompleksni – često su **automatizovani**, sistematski skeniraju internet u potrazi za ranjivim sistemima, i napadaju gdje god naiđu na **loše lozinke, nezaštićene servere, zastarjele softvere ili neobučen kadar**. Male firme, koje su često slabije zaštićene, postaju **lak plijen** za kriminalne grupe, koje ih vide kao "nisko obješeno voće" – jednostavnu metu s potencijalom za brzu finansijsku dobit.

Ovo alarmantno stanje ne mora biti trajno. Upravo su sektorska udruženja u poziciji da budu **prvi posrednici između MSP-ova i svijeta digitalne sigurnosti**. Kroz strateške aktivnosti, udruženje može:

- **Postaviti osnovne standarde i preporuke ponašanja**, prilagođene potrebama malih firmi;
- **Obezbijediti edukativne resurse i treninge** – webinari, brošure, vodiči;
- **Omogućiti pristup relevantnim stručnjacima i partnerima** iz oblasti cyber sigurnosti;
- **Uspostaviti razmjenu iskustava i dobre prakse** među članicama.

Ovakvim pristupom, biznis udruženja i organizacije ne samo da doprinose unaprjeđenju bezbjednosne prakse među članicama, već i **grade svoju reputaciju kao odgovornog, proaktivnog i pouzdanog partnera** u digitalnom dobu. U vremenu kada povjerenje po-

staje valuta, sposobnost da zaštitimo svoje podatke, sisteme i korisnike – postaje ključna za konkurentnost i dugoročnu održivost.

Zato cyber sigurnost više nije „tehnička tema“. Ona je pitanje **liderstva, zajedništva i spremnosti da djelujemo preventivno – svi zajedno.**

## Osnovne prijetnje s kojima se susreću članice:

### Cyber prijetnje za male firme: Isti napadi, manje resursa

Iako se često pretpostavlja da su meta cyber napada uglavnom velike korporacije, stvarnost je sasvim drugačija. **Male i srednje firme suočavaju se sa gotovo identičnim prijetnjama**, ali za razliku od velikih sistema, one često **nemaju stručne timove, napredne zaštitne alate, ni razvijene protokole za krizne situacije**. To ih čini izuzetno ranjivim – a upravo zato su često i ciljane.

Prema brojnim izvještajima, uključujući podatke IBM-a i ENISA-e, broj napada na MSP-ove u konstantnom je porastu. Napadi su često automatizovani i neselektivni – **traže najlakšu metu**, što male firme često, nažalost, jesu. Evo ključnih prijetnji s kojima se suočavaju:

### 1. Phishing napadi

Phishing je najraširenija vrsta cyber prevare. Napadači šalju e-mailove koji izgledaju kao da dolaze od poznatih izvora – banaka, dobavljača, pa čak i kolega iz firme. Cilj je da primatelj klikne na link koji vodi do lažne web stranice ili da otkrije povjerljive podatke (npr. lozinku ili broj platne kartice).

**• Primjer iz prakse:**

Zaposleni prima e-mail koji izgleda kao hitan zahtjev za uplatu od „direktora“ firme. U žurbi, bez provjere, prenosi sredstva na račun napadača.

**• Prevencija:**

Obuka zaposlenih da prepoznaju sumnjive poruke;

Implementacija filtera i alata za detekciju lažnih e-mailova;

Dvofaktorska autentifikacija kao dodatna zaštita u slučaju krađe lozinke.

### 2. Ransomware

Ransomware je zlonamjerni softver koji, nakon infiltracije, šifrira sve podatke na računaru korisnika, ili serveru, a zatim traži otkup (najčešće u kriptovalutama) za dešifrovanje podataka. Male firme često plaćaju otkup – jer **nemaju backup**, niti kapacitet da se same oporave.

• **Način širenja:**

Prilozi u e-mailovima (npr. .zip, .pdf, .doc);

Posjete zaraženim web sajtovima;

USB uređaji bez kontrole.

• **Prevencija:**

Redovan backup podataka (lokalno i u cloud-u);

Antivirusni softver sa aktivnim praćenjem ponašanja fajlova;

Edukacija o prepoznavanju rizičnih priloga.

## 3. Nepouzdane Wi-Fi mreže

Korišćenje nezaštićenih ili javnih Wi-Fi mreža (npr. u kafićima, hotelima, co-working prostorima) predstavlja veliki rizik. Napadači mogu kreirati **lažne mreže** sličnog imena ili nadgledati promet na postojećoj mreži (tzv. „man-in-the-middle" napad).

• **Šta napadač može vidjeti?**

Korisnička imena, lozinke, e-mail poruke, čak i bankarske informacije, odnosno podatke o bankovnim transakcijama – ako iste nisu kriptovane.

• **Prevencija:**

Izbjegavati spajanje na mreže bez lozinke;

Korištenje VPN-a (Virtual Private Network);

Onemogućiti automatsko povezivanje uređaja na mreže;

## 4. Zastarjeli softver i sistemi

Softver koji se ne ažurira redovno (operativni sistemi, web pretraživači, aplikacije) često sadrži poznate sigurnosne ranjivosti. Hakeri ih lako pronalaze i iskorištavaju putem automatizovanih alata.

• **Rizik za male firme:**

Neke male firme i dalje koriste Windows 7 ili druge nepodržane sisteme jer „rade bez problema". Nažalost, ti sistemi **više ne dobijaju sigurnosne zakrpe**.

• **Prevencija:**

Ažurirati softver čim su dostupna sigurnosna poboljšanja/zakrpe;

Koristiti softver koji je i dalje podržan od strane proizvođača;

Automatizovati update-e gdje je moguće.

## 5. Slabe lozinke i nedostatak višefaktorske autentifikacije

Lozinke poput „123456“ ili „firma2024“ i dalje su česte. Pored toga, korištenje iste lozinke za više servisa (e-mail, CRM, bankarstvo) znači da **kompromitacija jedne platforme otvara pristup svima**.

**• Statistika:**

Prema istraživanju IBM-a, više od 90% cyber incidenata rezultat je **ljudske pogreške** – a lozinke su često prvo mjesto gdje ta greška započinje.

**• Prevencija:**

Koristiti jake lozinke (min. 12 karaktera, kombinacija slova, brojeva i simbola);

Aktivirati **dvofaktorsku autentifikaciju (2FA)** na svim servisima;

Koristiti menadžere lozinki za sigurno čuvanje pristupnih podataka;

## Zaključak: Ljudi su prva linija odbrane

Iako su tehnološka rješenja važna, nijedan sistem nije potpuno siguran bez **osviješćenih i obučenih ljudi**. Ljudska greška – klik na pogrešan link, unošenje lozinke na lažnu stranicu ili ignorisanje upozorenja – najčešći je uzrok cyber incidenata. Upravo zato je **edukacija zaposlenih** ključna komponenta svakog sigurnosnog pristupa.

Za male firme, posebno one koje nemaju vlastiti IT sektor, osvještavanje o ovim prijetnjama i usvajanje osnovnih sigurnosnih mjera mogu **značiti razliku između jednog klika – i gubitka čitavog poslovanja.**

## Preporučene prakse za internu otpornost udruženja – Sažetak

Kako bi bila kredibilna u očima članica, biznis udruženja i organizacije moraju i same primjenjivati osnovne sigurnosne mjere. To uključuje:

- **Dvofaktorska autentifikacija (MFA)**: Svi nalozi koji se koriste za internu komunikaciju, pristup fajlovima i nalozima moraju imati dodatni sloj zaštite.
- **Redovno ažuriranje softvera**: Zastarjeli softver otvara sigurnosne rupe. Preporučuje se automatsko ažuriranje sistema i aplikacija.
- **Sigurnosne kopije (backup)**: Redovno pravljenje kopija važnih dokumenata omogućava oporavak u slučaju incidenta, kao što je ransomware.
- **Politike sigurnog ponašanja**: Dokumentovane smjernice o tome kako koristiti službene uređaje, kako se ponašati s e-mailom i kako prijaviti sumnjive aktivnosti.
- **Edukacija osoblja**: Čak i osnovne interne radionice na temu prepoznavanja lažnih poruka mogu prevenirati ozbiljne incidente.

Postavljanje ovih praksi ne zahtijeva veliki budžet, ali značajno podiže ukupnu sigurnost udruženja.

# Uloga udruženja u edukaciji i podršci članicama

Udruženja imaju priliku da oblikuju ponašanje članica kroz kontinuiranu edukaciju. Evo nekoliko načina kako to mogu uraditi:

- **Mjesečne edukacije**: Tematski dani o sigurnosti (npr. "Dan sigurnog e-maila") kroz Zoom sesije od 30 minuta.
- **Infografike i vodiči**: Jednostavni dokumenti koji se mogu dijeliti članicama i kačiti na oglasne ploče ili portale.
- **Saradnja sa stručnjacima**: Pozivanje IT stručnjaka da održe besplatne sesije za članice.
- **Newsletter sekcija o sigurnosti**: Dodavanje kratkih savjeta u postojeće biltene.
- **Simulacije incidenata**: Jednostavne vježbe kako bi članice znale prepoznati phishing e-mail.

Edukacija ne mora biti formalna – najvažnija je dosljednost i prilagođenost kontekstu lokalne poslovne zajednice.

## Preporučeni alati – besplatni i pouzdani

Mnoge organizacije misle da je cyber sigurnost skupa, ali postoji veliki broj besplatnih i pouzdanih alata koji mogu znatno unaprijediti sigurnost:

- **Microsoft Defender**: Ugrađen u Windows 10/11 i nudi osnovnu zaštitu od zlonamjernih softvera.
- **Duplicati**: Open-source alat za pravljenje sigurnosnih kopija, jednostavan za korištenje.
- **CyberReady Toolkit**: EU inicijativa za edukaciju MSP-a – uključuje vodiče, alate i trening materijale.
- **HaveIBeenPwned**: Provjera da li je e-mail adresa kompromitovana u prethodnim napadima.
- **Google sigurnosni alati**: Notifikacije i autentifikacija kroz Google Workspace.

Svi ovi alati su preporučeni od strane priznatih organizacija kao što su NIST i ENISA i mogu se koristiti bez dodatnog budžeta.

# Osnovni krizni plan: predložak i smjernice

## Osnovni krizni plan:

## Predložak i smjernice za postupanje u slučaju cyber incidenta

U digitalnom svijetu, pitanje nije *da li* će se dogoditi sigurnosni incident, već *kada*. Bilo da se radi o curenju podataka, ransomware napadu, krađi identiteta ili neautorizovanom pristupu sistemima – brzina i jasnoća reakcije može napraviti razliku između manjeg zastoja i dugotrajne poslovne štete.

Zato je **krizni plan** nezamjenjiv alat za svaku organizaciju, bez obzira na veličinu ili sektor. On predstavlja skup **unaprijed definisanih koraka i procedura koje osiguravaju smirenu, organizovanu i učinkovitu reakciju u trenutku incidenta.** Krizni plan ne treba biti opširan i složen – naprotiv, njegova snaga je u jasnoći, jednostavnosti i pristupačnosti.

### Evo osnovnih elemenata koje svaki krizni plan treba da sadrži:

### 1. Obavještavanje: Ko, kome i kada prijavljuje incident

Prvi i najvažniji korak je **trenutno prepoznavanje i prijavljivanje sumnjivog događaja**. Plan treba da precizira:

- Ko je zadužen za **primanje prijava** (npr. IT kontakt osoba, menadžer sigurnosti, eksterni partner);
- Kako prijaviti incident (telefonom, e-mailom, formularom);
- Koja je procedura za **eskalaciju** ako je incident većih razmjera;
- Da li postoji backup kontakt u slučaju odsustva primarnog lica.

*Preporuka: Na vidljivom mjestu (i digitalno i fizički) objavite kontakt osobu za sigurnost s jasnim uputama za prijavu.*

### 2. Izolacija incidenta: Sprečavanje širenja

Nakon prijave, prioritet je **izolovati incident** kako bi se spriječilo dalje oštećenje sistema ili curenje podataka. To uključuje:

- Odspajanje pogođenog uređaja sa mreže (Wi-Fi, LAN);
- Onemogućavanje pristupa kompromitovanom nalogu;

- Privremeno isključivanje sumnjive aplikacije ili servisa;
- Promjena lozinki ako se sumnja na kompromitaciju pristupa.

*Napomena: Ne pokušavajte sami „brisati" sumnjive datoteke ili reinstalirati softver bez prethodnog savjetovanja sa stručnjacima – možete nehotice uništiti dokaze koji su važni za forenziku.*

## 3. Komunikacija s članicama i partnerima: Transparentno i odgovorno

U kriznim situacijama je **kvalitet komunikacije jednako važan kao i tehnički odgovor**. Dezinformacije, panika ili ćutanje mogu pogoršati situaciju.

Zbog toga plan treba da sadrži:

- Spisak internih i eksternih grupa koje trebaju biti obaviještene (npr. članice, upravni odbor, IT partneri);
- **Unaprijed pripremljene šablone poruka** – za e-mail, SMS ili objavu;
- Osobu zaduženu za eksternu komunikaciju;
- Smjernice o tome šta se smije, a šta ne smije dijeliti u javnosti (posebno ako je u toku istraga).

*Transparentnost gradi povjerenje – ali svaka poruka mora biti promišljena, tačna i vremenski usklađena.*

## 4. Angažman stručnjaka: Niko ne mora biti sam u kriznoj situaciji

Većina malih firmi nema interni IT tim, što znači da je ključno imati **unaprijed dogovorenu saradnju sa vanjskim stručnjacima**. To uključuje:

- IT servisere ili MSP (Managed Service Provider);
- Stručnjake za **digitalnu forenziku i analizu štete;**
- Pravno savjetovanje (posebno u vezi s obavezama prema zakonima o zaštiti podataka, npr. GDPR);
- Osiguranje (ako postoji polisa cyber osiguranja).

*Unaprijed dogovoreni partneri mogu reagovati brže i efikasnije nego ako ih tek tražite usred krize.*

## 5. Dokumentovanje i izvještavanje: Lekcije koje spašavaju budućnost

Svaki korak koji se preduzme tokom i nakon incidenta mora biti zabilježen – ne samo zbog pravnih razloga, već i kao osnova za učenje i unapređenje procesa. Plan treba uključiti:

- Predložak izvještaja o incidentu;
- Mjesto gdje se dokumentacija čuva (digitalno + fizički);
- Spisak osoba koje su učestvovale u odgovoru;
- Procjenu štete i preporuke za prevenciju sličnih incidenata.

*Sistematsko dokumentovanje pomaže i u razgovoru s regulatorima, osiguravajućim kućama i partnerima.*

## Kako krizni plan treba izgledati?

Idealni krizni plan za MSP firme treba da bude:

- **Kratak i jasan** – 1–3 stranice, bez tehničkog žargona;
- **Dostupan svima** – u digitalnom formatu (cloud, intranet) i štampano u kancelariji;
- **Redovno ažuriran** – makar jednom godišnje ili nakon svakog incidenta;
- **Testiran** – kroz simulacije i scenarije (“šta ako”).

*Plan koji postoji samo na papiru – i nikad nije pregledan ni testiran – ne donosi vrijednost kada je najpotrebnije.*

## Završna poruka

**Krizni plan nije znak paranoje – to je znak odgovornosti.** On ne garantuje da se incident neće dogoditi, ali značajno povećava šanse da firma prebrodi krizu s minimalnim gubicima.

Za članice biznis udruženja i organizacija, posjedovanje ovakvog plana ne samo da štiti poslovanje, već i podiže povjerenje kupaca, partnera i cijele zajednice. **Sigurnost počinje sa planom – i sa spremnošću da reagujemo kada je najvažnije.**

# Krizni plan – Sažetak

## Priprema kratkih edukacija za članice

Jedna od najefikasnijih aktivnosti koje biznis udruženja i organizacije mogu sprovoditi jesu kratke, redovne edukacije. One ne moraju biti skupe ni komplikovane. Cilj je da članice dobiju korisne informacije u formatu koji im je razumljiv i pristupačan.

## Koraci za pripremu edukacije:

1. **Odabir teme**: Fokusirati se na jednu konkretnu prijetnju – npr. kako prepoznati lažni e-mail.
2. **Format**: Online sesija do 30 minuta, po mogućnosti s pauzom za pitanja.
3. **Priprema**: 5-6 slajdova s praktičnim primjerima. Idealno uključiti kviz ili anketu.
4. **Komunikacija**: Obavijestiti članice putem e-maila i društvenih mreža.
5. **Evaluacija**: Kratka anketa nakon sesije – šta im je bilo korisno, šta nije.

Ove edukacije postaju prostor za dijalog, razmjenu iskustava i jačanje zajednice.

## Saradnja s lokalnim IT i sigurnosnim stručnjacima

Biznis udruženja i organizacije ne moraju imati svoj IT tim – ali mogu i trebaju graditi mrežu saradnika koji će stajati na raspolaganju članicama.

**Mogući partneri uključuju:**

- IT firme koje mogu pružiti početne revizije sigurnosti (audit);
- Freelancere – etičke hakere, edukatore, developere;
- Fakultete i tehničke škole – uključiti studente kao podršku i istraživače.

Može se kreirati mreža “cyber mentora” – stručnjaka koji volontiraju određeni broj sati mjesečno u podršci MSP-ovima. Takođe, moguće je organizovati tematske “otvorene dane” gdje članice mogu doći sa konkretnim pitanjima.

## Resursi za dalju edukaciju

Dobra edukacija zahtijeva dobre izvore. U nastavku su preporučeni besplatni resursi koji mogu služiti i udruženju i članicama:

- ENISA edukativni paketi – obuhvataju teme od osnova do naprednih koncepata
- OWASP Top 10 – pregled najčešćih sigurnosnih grešaka s primjerima i preporukama.

- NIST Cybersecurity Corner za MSP – alatke, vodiči i kontrolne liste.
- EU CyberNet akademija – besplatna platforma sa kursevima.
- YouTube kanali: “Cyber Security for Beginners”, “InfosecTrain”, “SimplyCyber”.

Korištenjem provjerenih izvora podiže se kvalitet edukacije i izbjegava se širenje netačnih ili zastarjelih informacija.

## Primjeri dobre prakse iz regije i EU

Dobre ideje treba prepoznati i prilagoditi lokalnom kontekstu. U nastavku su prikazani primjeri koji se mogu replicirati:

- **Austrija**: Privredna komora je razvila alat za samoprocjenu rizika u obliku online upitnika.
- **Estonija**: Udruženja objavljuju mjesečne biltene s praktičnim savjetima.
- **BiH**: Jedno udruženje organizovalo je “Cyber mjesec” s tematskim radionicama (sigurna e-trgovina, zaštita podataka).

Ovi primjeri pokazuju da i bez velikih budžeta, uz volju i organizaciju, udruženja mogu djelovati strateški i edukativno.

## Preporučeni interni checklist (mjesečni i kvartalni)

Jedan od najpraktičnijih alata za organizaciju i provjeru stanja jeste kontrolna lista. U nastavku je prijedlog checklista koje biznis udruženja i organizacija mogu koristiti:

## Mjesečna lista:

- Ažurirani svi operativni sistemi i aplikacije;
- Backup podataka urađen i testiran;
- Poslan edukativni e-mail članicama;
- Provjereni svi korisnički nalozi i pristupi;
- Analiziran potencijalni incident (ako postoji).

## Kvartalna lista:

- Održan barem jedan webinar;
- Ažuriran krizni plan i kontakti;
- Provjereni ugovori s IT partnerima;
- Odraditi anonimnu anketu sigurnosne kulture među članicama.

Checklist omogućava sistematičan pristup i osigurava da važni koraci ne budu zaboravljeni.

## Mitovi i istine o cyber sigurnosti u malim firmama

**U nastavku su najčešći mitovi koje je važno razbiti:**

**MIT**: "Mali biznisi nisu zanimljivi hakerima."
**ISTINA**: MSP su najčešće mete jer imaju slabiju zaštitu.

**MIT**: "Ako imam antivirus, ne moram brinuti."
**ISTINA**: Antivirus je samo jedan sloj. Potrebna je šira strategija.

**MIT**: "Naši ljudi znaju kako prepoznati lažni e-mail."
**ISTINA**: Ljudska greška je uzrok 9 od 10 napada. Potrebna je stalna edukacija.

**MIT**: "Cyber sigurnost košta previše."
**ISTINA**: Mnoge mjere zaštite su besplatne i zahtijevaju samo dobru organizaciju.

Borba protiv mitova je prvi korak u izgradnji otpornosti.

## Kako mjeriti napredak u otpornosti

Napredak se mora mjeriti – u suprotnom ne znamo da li idemo u pravom smjeru. Preporučene metrike za biznis udruženja i organizacije:

- **Učešće**: Broj članica koje prisustvuju edukacijama
- **Doseg**: Broj distribuisanih materijala (vodiča, infografika)
- **Povratne informacije**: Rezultati anketa, zadovoljstvo, prijedlozi
- **Interni kapacitet**: Postoji li krizni plan? Da li su napravljeni backupi?
- **Reakcija na incidente**: Da li su incidenti prijavljeni? Kako je proces tekao?

Jednostavan kvartalni izvještaj (1 strana) može se koristiti za internu evaluaciju i strategijsko planiranje.

# Zaključak i poziv na akciju

### Vrijeme je za proaktivnu sigurnost

Da ponovimo, u digitalnom dobu, **cyber sigurnost nije luksuz, već temelj opstanka i povjerenja**. Bez obzira na veličinu, sektor ili nivo digitalizacije, svaka organizacija – uključujući i male firme – izložena je sve sofisticiranijim cyber prijetnjama. Napadači ne biraju mete prema imenu ili broju zaposlenih, već prema stepenu ranjivosti. Upravo zato, **reaktivni pristup više nije dovoljan. Vrijeme je za promjenu paradigme – od reakcije ka prevenciji**.

Organizacije kao što su **biznis udruženja i organizacije imaju moć da budu katalizatori te promjene.** Kroz znanje, umrežavanje i koordinaciju, mogu pomoći članicama da:

- **Prepoznaju rizike prije nego što postanu incidenti;**
- **Primijene jednostavne, ali učinkovite sigurnosne mjere;**
- **Podignu svijest unutar svojih timova;**
- **Povežu se s pouzdanim stručnjacima i relevantnim resursima.**

Male firme često nemaju kapacitete za izgradnju sopstvenih sigurnosnih sistema – ali zato imaju **biznis udruženja i organizacije**. Umjesto da čekaju da se desi šteta, udruženja mogu postati **lideri digitalne otpornosti**, pružajući podršku tamo gdje je najpotrebnija. Informisanje, edukacija i zajedničko djelovanje – to su alati budućnosti.

Ovaj vodič nije samo zbirka preporuka – to je **poziv na promjenu pristupa.** Cyber sigurnost nije posao jedne osobe, jednog sektora ili samo jedne firme. To je zajednički izazov i zajednička odgovornost.

## Šta možete uraditi već danas?

- **Organizujte osnovnu obuku o cyber sigurnosti za članice;**
- **Postavite minimalne sigurnosne standarde unutar udruženja;**
- **Iskoristite dostupne resurse iz ovog vodiča: ček liste, alati, predlošci politika;**
- **Podijelite ovaj vodič sa svim članicama kao obaveznu lektiru;**
- **Uključite sigurnost u sve komunikacije, događaje i inicijative biznis udruženja i organizacija.**

## Zajedno gradimo otpornu zajednicu

Cyber sigurnost nije samo tehničko pitanje – ona je pitanje kulture, povjerenja i odgovornosti. Udruženja koja prepoznaju tu ulogu danas, postaće **lideri sigurnog poslovnog okruženja sutra**.

**Budite ti koji uvode promjenu.**

**Budite nosioci sigurnosti u svojoj zajednici.**

Ova publikacija je objavljena u sklopu implementacije projekta Cyber Security education program a u okviru SEDEP programa, koji sufinansiraju Njemačko savezno ministarstvo za ekonomsku saradnju i razvoj (BMZ), Evropska unija i Švicarska vlada. Sadržaj ove publikacije isključiva je odgovornost Udruženja e-Transformacija i ne odražava nužno stavove njemačke vlade, švicarske vlade ili Evropske unije.