KOR
2026.



Osnove kibernetičke sigurnosti za MSP-ove

Prezentira:

Zoran Kežman,
konzultant za edukaciju iz područja kibernetičke sigurnosti,
Span d.d.

Kibernetički napadi se i MSP-ovima događaju svakodnevno



Obično su laka meta jer u pravilu nemaju odgovarajuće sigurnosne mjere



Koristi ih se kao „ulazna vrata” u veće lance dobavljača u svrhu napada na veće organizacije

Učestale zablude

„Nama se to neće dogoditi…”

„Naše poslovanje je premalo da bi bilo meta napada…”

Nije stvar u tome koliko je netko „zanimljiv”, nego koliko je ranjiv!

HR PSOR

Ključne značajke edukacije iz kibernetičke sigurnosti za MSP-ove

- ☑ Namijenjena je i prilagođena rukovodstvu u mikro, malim i srednje velikim poduzećima.
- ☑ Pruža temeljna znanja potrebna za učinkovito upravljanje kibernetičkim rizicima na organizacijskom nivou.
- ☑ Omogućuje upoznavanje s važnim konceptima kibernetičke sigurnosti bez napora i složenog tehničkog žargona.
- ☑ Daje strukturirani pregled i praktične preporuke za izgradnju kibernetičke otpornosti na način koji najbolje odgovara poslovanju pojedinog MSP-a, njegovim resursima i upravljanju.

HR PSOR

Ključne značajke edukacije iz kibernetičke sigurnosti za MSP-ove

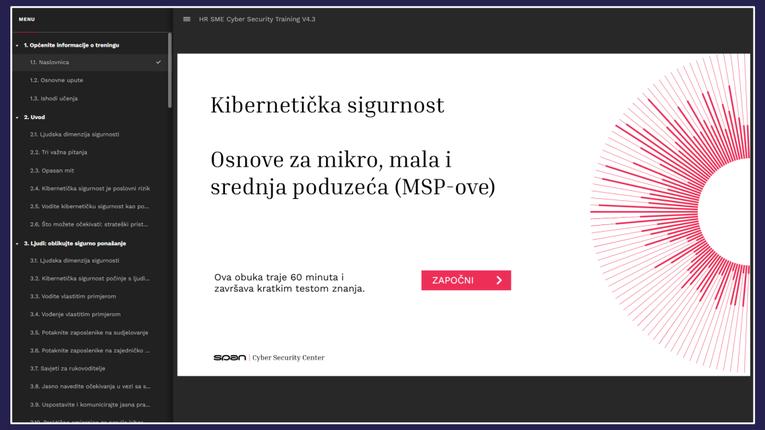
- ☑ **Interaktivni edukacijski sadržaj koji potiče aktivno sudjelovanje.**

- ☑ **Omogućeno je preuzimanje dodatnog vodiča namijenjenog svim zaposlenicima. Vodič „Osnove kibernetičke sigurnosti" sadrži temeljne sigurnosne prakse kojih bi se svatko u organizaciji trebao pridržavati, i privatno i poslovno.**

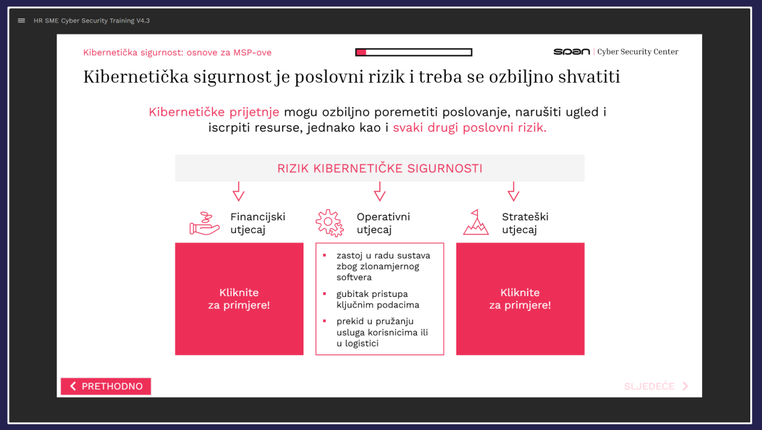
- ☑ **Edukacija je raspoloživa on-line, moguće ju je koristiti prema vlastitom tempu i potrebama i u cijelosti je besplatna.**

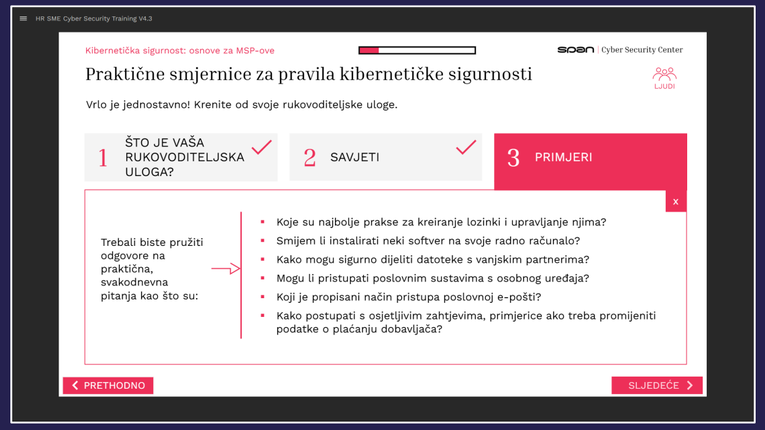
HR PSOR

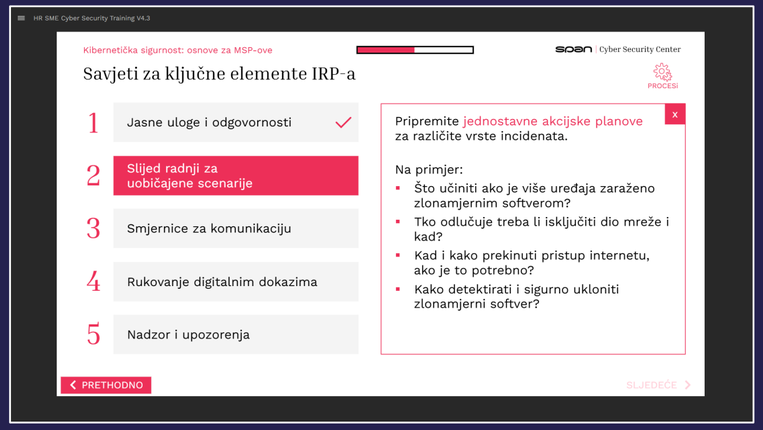
Isječci iz on-line edukacijskog sadržaja

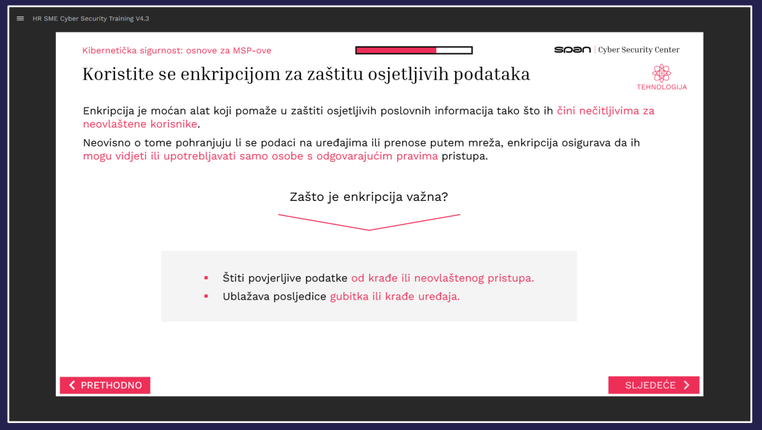






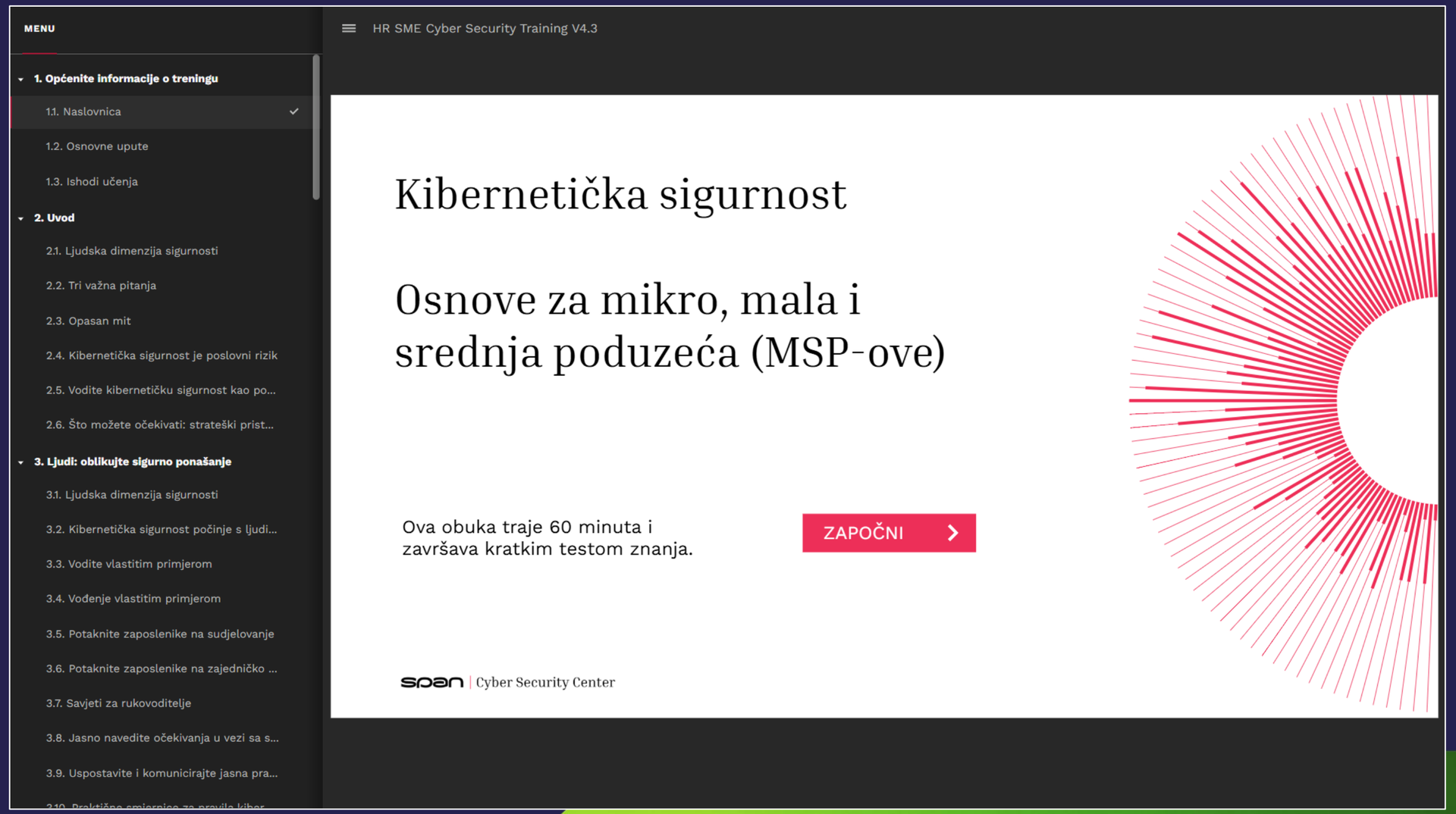






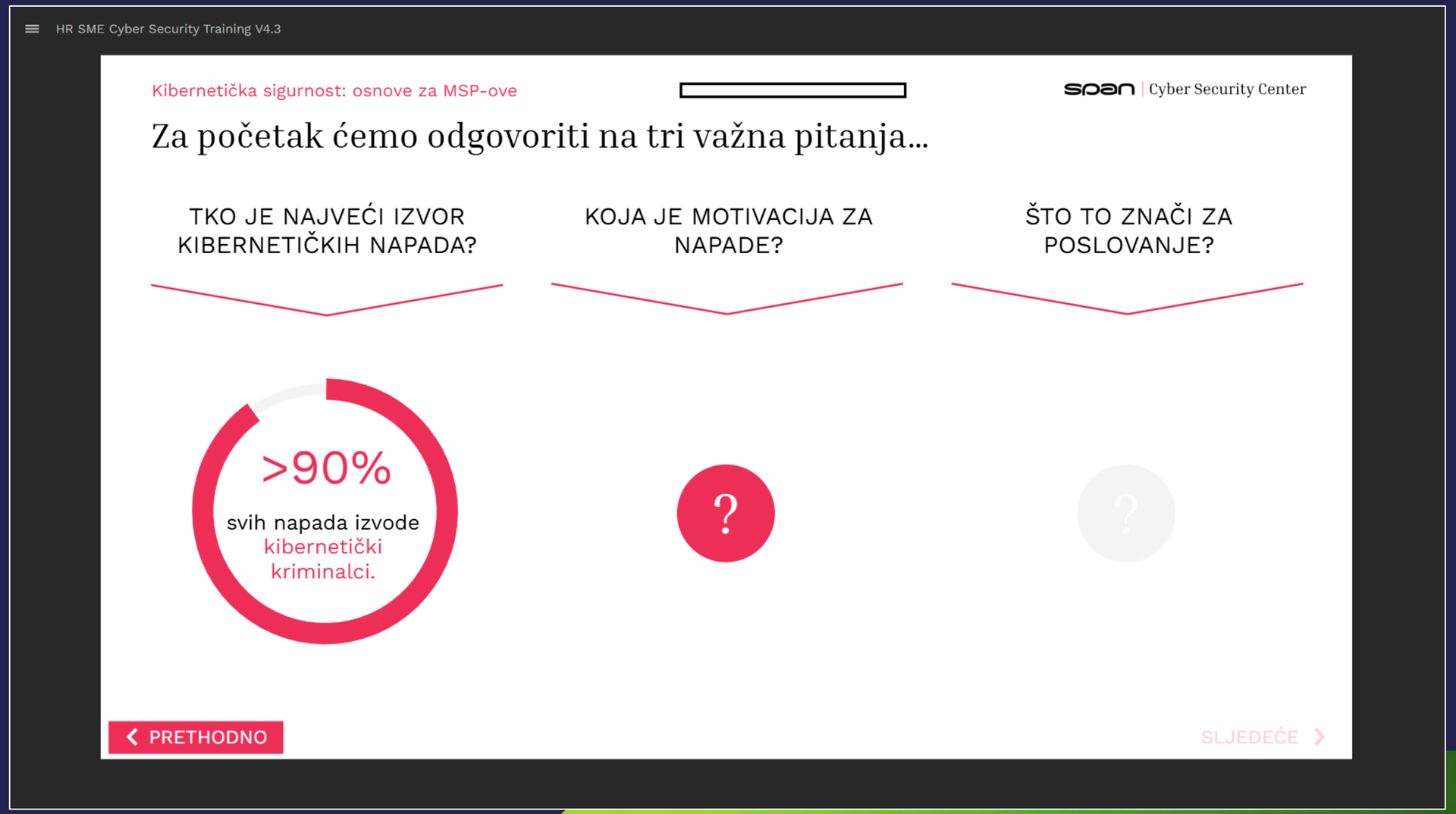
HR PSOR

Isječci iz on-line edukacijskog sadržaja



HR PSOR

Isječci iz on-line edukacijskog sadržaja



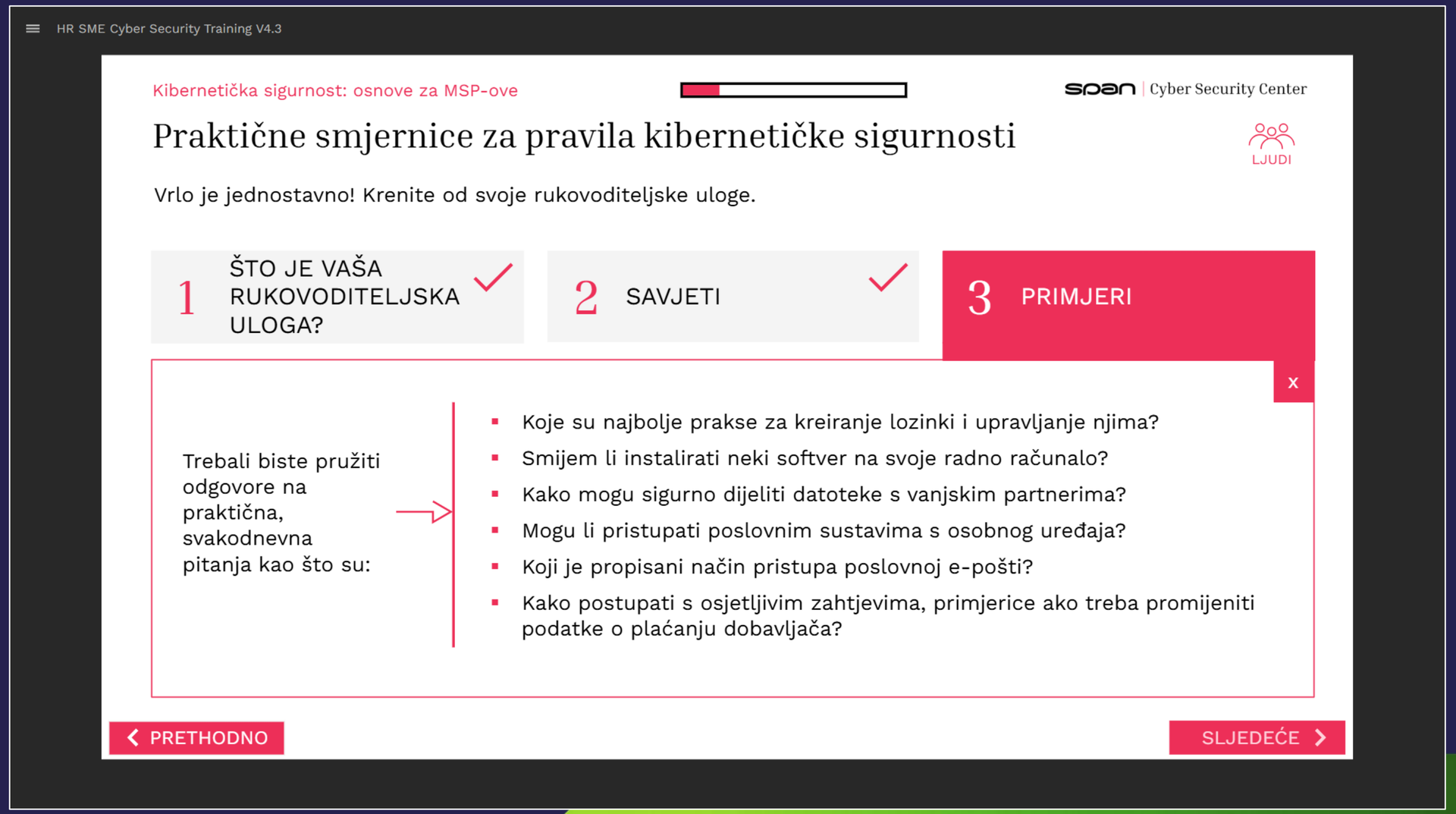
HR PSOR

Isječci iz on-line edukacijskog sadržaja



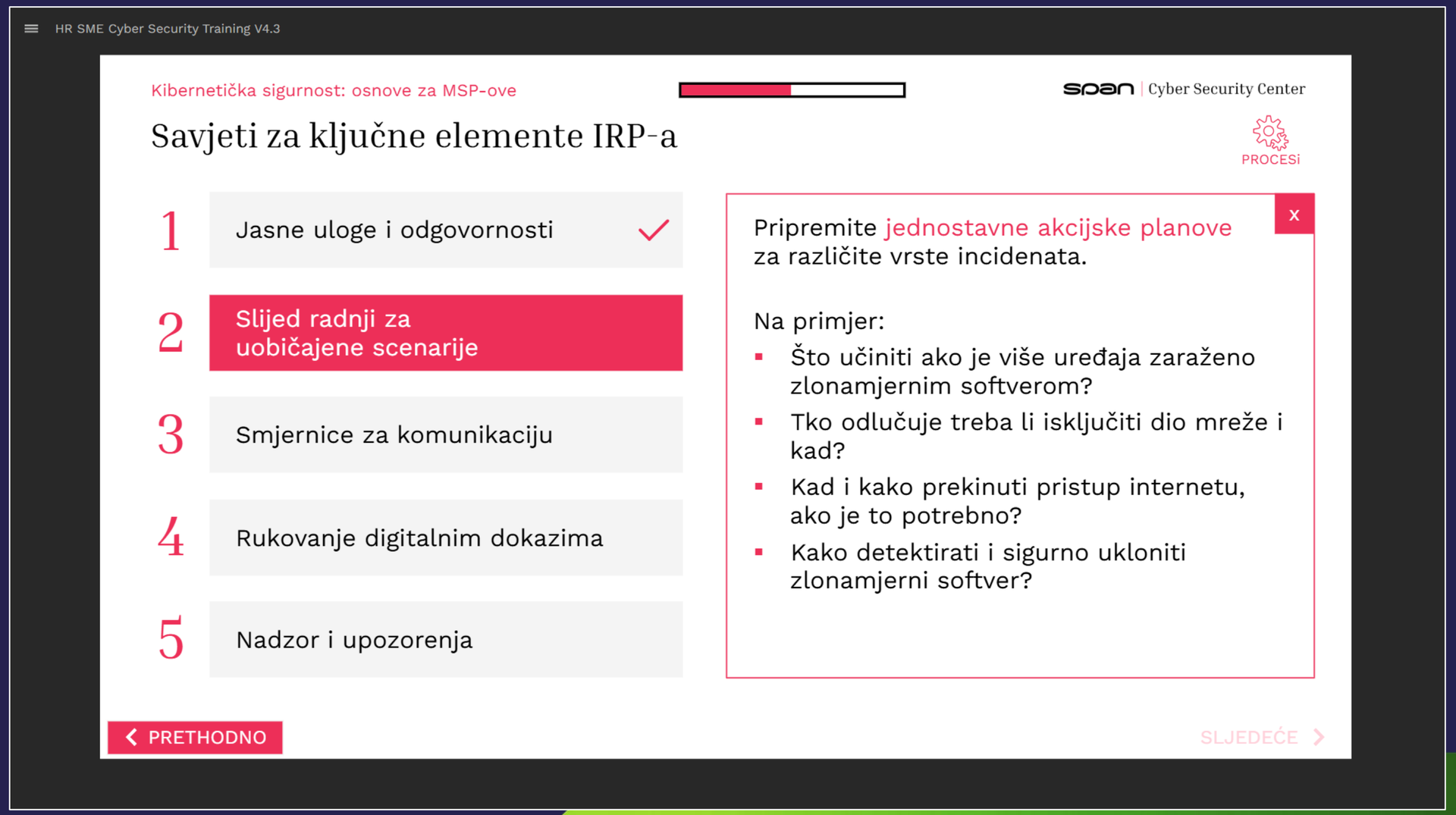
HR PSOR

Isječci iz on-line edukacijskog sadržaja



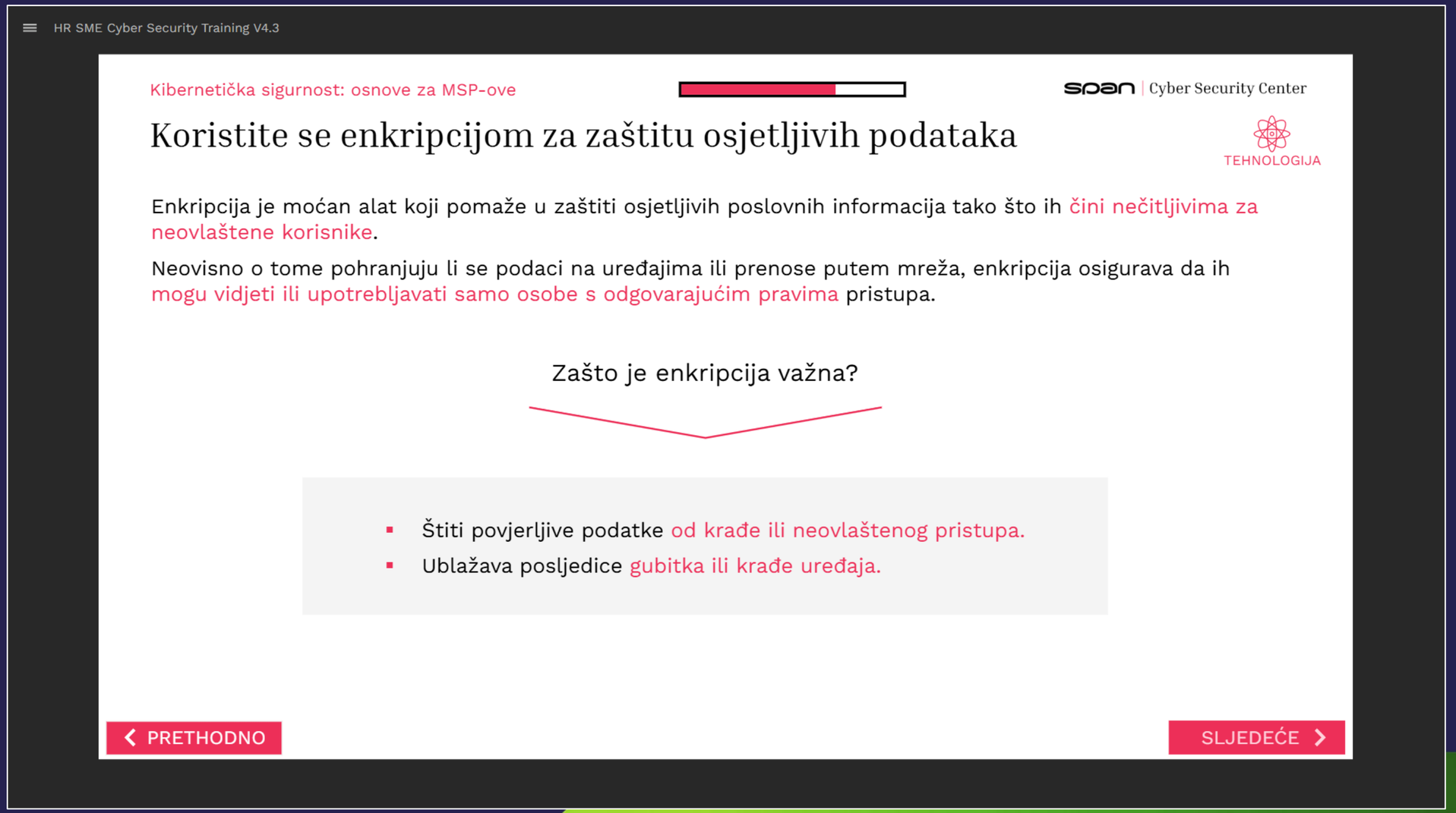
HR PSOR

Isječci iz on-line edukacijskog sadržaja



HR PSOR

Isječci iz on-line edukacijskog sadržaja



HR PSOR

Osnove kibernetičke sigurnosti za MSP-ove

Ova interaktivna on-line edukacija dostupna je na našoj internetskoj stranici:

https://spansecuritycenter.eu/hr/edukacije/besplatna-edukacija-za-mala-i-srednja-poduzeca/

HR PSOR

KOR
2026.



Radionica 1

Uloga kibernetičke sigurnosti u održivom poslovanju

Presented by:

Marina Dimić Vugec,

Cyber Security Education and
Project Senior Specialist,
Span Cyber Security Center

HR PSOR HRI HRVATSKI INDEKS ODRŽIVOSTI

ured@hrpsor.hr www.hrpsor.hr

Agenda

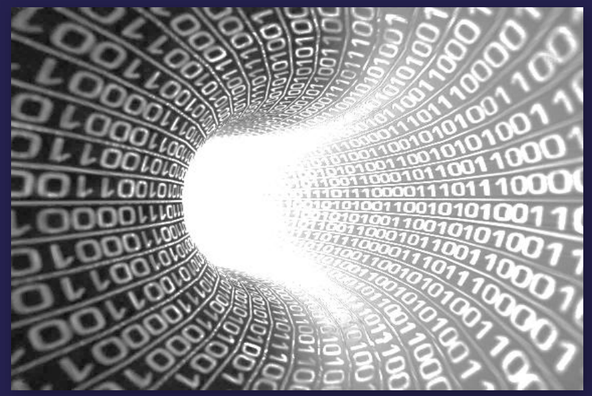
- Kibernetički kriminal i utjecaj kibernetičkih napada
- Značaj ljudskog faktora i kako dolazi do incidenata
- 4 temeljne prakse / ponašanja
- Kibernetička sigurnost u ESG strategiji

HR PSOR

Kibernetički kriminal i utjecaj kibernetičkih napada

Digitalna transformacija i povezani svijet

PODACI



Eksplozija podataka

Kritična imovina

KRIMINAL



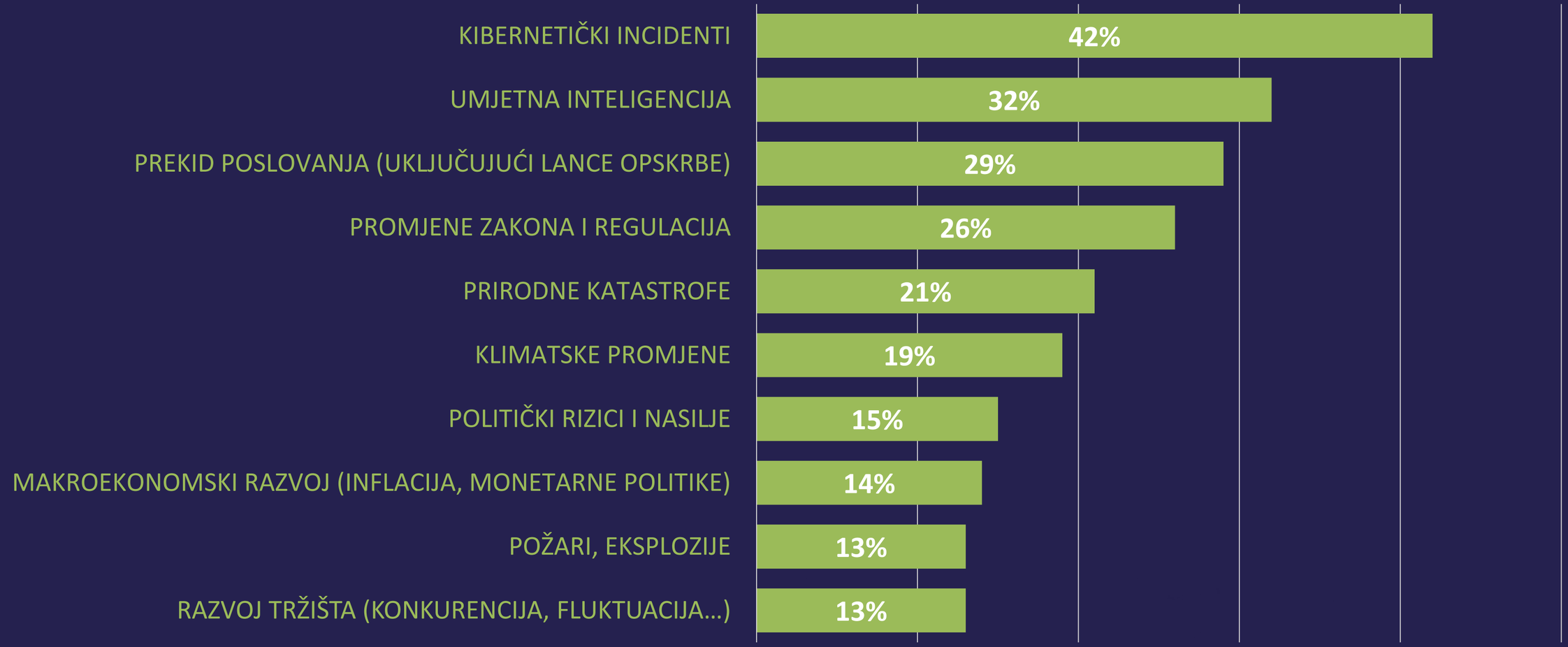
Postaje digitalan

Kibernetički kriminal u porastu

HR PSOR

Najvažniji poslovni rizici u 2026., Globalno

Allianz Risk Barometer 2026 (2026 Allianz Global Corporate & Specialty (N=3.338, izbor do 3 rizika po industriji)



HR PSOR

Implikacije za organizacije i njihovo poslovanje

Štetni događaji

- Krađa i razotkrivanje vrijednih poslovnih podataka
- Oštećenje ili uništenje podataka
- Prekid poslovanja, tijekom i nakon napada (oporavak)
- Iznuda
- Prijevara / Zloupotreba podataka
- Zloupotreba računalnih resursa

Utjecaj na poslovanje

DIREKTNA ŠTETA	Izgubljeni prihodi, pad produktivnosti, gubitak korisnika, izgubljena proizvodnja i druge štete
TROŠKOVI OPORAVKA	Koliko košta otkrivanje, istraživanje, obuzdavanje i iskorjenjivanje napadača
PRAVNI TROŠKOVI	Regulatorne novčane kazne i tužbe dioničara ili korisnika
REPUTACIJSKA ŠTETA	Gubitak povjerenja klijenata i poslovnih partnera, izgubljena konkurentska prednost

Povezano s ESG pokazateljima

Štetni događaji

- Krađa i razotkrivanje vrijednih poslovnih podataka
- Oštećenje ili uništenje podataka
- Prekid poslovanja, tijekom i nakon napada (oporavak)
- Iznuda
- Prijevara / Zloupotreba podataka
- Zloupotreba računalnih resursa

Utjecaj na poslovanje

E - okolišni

prekid rada sustava za nadzor emisija i onečišćenja
izlijevanje opasnih tvari ili incidentna onečišćenja
povećana potrošnja energije tijekom oporavka sustava

S - društveni

ugrožavanje osobnih podataka zaposlenika i korisnika
narušeno povjerenje kupaca i poslovnih partnera
nedostupnost ključnih usluga građanima i gospodarstvu

G - upravljački

loše upravljanje i nedovoljan nadzor nad rizicima
nedostatne interne kontrole
neusklađenost sa zakonima i regulativom

Povezano s ESG pokazateljima

Kibernetički napad je rizik održivosti jer može ugroziti šire gospodarske, okolišne i društvene ciljeve

Utjecaj na poslovanje

- Kontinuitet poslovanja
- Lanac opskrbe
- Povjerenje korisnika
- Financijski rezultati
- Reputacija organizacije
- ESG pokazatelji i izvještavanje

HR PSOR

Američki primjer

Colonial Pipeline (svibanj, 2021.) Ransomware

Posljedice

- **Kontinuitet poslovanja:** preventivna obustava rada kako bi se ograničilo širenje; prekid distribucije oko 45% goriva za istočnu obalu SAD-a
- **Lanac opskrbe:** poremećena opskrba gorivom, logistika i transport dodatni troškovi, nestabilna opskrba energentima – čitav ekosustav dobavljača, kupaca i partnera
- **Povjerenje korisnika:** nedostupnost usluge za građane i poslovne subjekte, zabrinutost javnosti, propitkivanje kibernetičke otpornosti, dugoročno narušeno povjerenje
- **Financijski rezultati:** plaćanje otkupnine, troškovi istrage i oporavka, vanjski stručnjaci, gubitak prihoda, dodatna ulaganja, osiguranje
- **Reputacija organizacije:** interes medija, regulatora, investitora, loša percepcija otpornosti i spremnosti na upravljanje kriznim situacijama
- **ESG pokazatelji i izvještavanje:** dodatne logističke aktivnosti i manje učinkovite alternativne rute prijevoza, povećana potrošnja energija i veća emisija stakleničkih plinova, utjecaj na društvo, smanjeno povjerenje i povećana zabrinutost, upravljanje kibernetičkim rizicima i kriznim situacijama

Hrvatski primjer

KBC Zagreb
Rebro, lipanj, 2024.
Ransomware

Posljedice

Kontinuitet poslovanja: nedostupnost informacijskog sustava utjecalo je na redovno poslovanje, prebačeno na ručno, povećano opterećenje

Lanac opskrbe: nedostupnost informacija, usporena administracija i koordinacija, utjecaj na ekosustav pacijent, zdravstveni djelatnici, vanjski suradnici i druge ustanove

Povjerenje korisnika: narušeno povjerenje u otpornost zdravstvene infrastrukture, zaštita osjetljivih zdravstvenih i osobnih podataka

Financijski rezultati: troškovi istrage i oporavka, dodatni radni angažman zaposlenika, ulaganje u ojačanje poslovanja, troškovi upravljanja rizicima

Reputacija organizacije: interes medija i javnosti, predmet javne rasprave otpornost zdravstvenog sustava, otpornost digitalnih usluga i zaštite podataka

ESG pokazatelji i izvještavanje: oporavak sustava dodatni resursi, otežana dostupnost usluga, smanjena učinkovitost pružanja usluga, narušeno povjerenje i povećana zabrinutost, upravljanje kibernetičkim rizicima u zdravstvenom sustavu

Što je zajedničko?

PRIJETNJA	RANJIVOST	UTJECAJ
▪ Napadač s određenom motivacijom ▪ Korištene su specifične metode i tehnike napada	▪ Ljudski faktor ▪ Politike / procedure / procesi ▪ Tehnološki nedostaci	▪ Financijski ▪ Reputacijski ▪ Operativni ▪ Na krajnje korisnike / kupce

Što je zajedničko?

- Nešto što bi moglo nanijeti štetu

PRIJETNJA

- Slabost koja prijetnji omogućuje nanošenje štete

RANJIVOST

- Neka specifična šteta

UTJECAJ

RIZIK

MJERE KIBERNETIČKE SIGURNOSTI

HR PSOR

Tretman rizika

PRIHVAĆANJE

Priznavanje da rizik postoji, ali bez primjene zaštitnih mjera

IZBJEGAVANJE

Donošenje informirane odluke da se ne uključite u rizičnu radnju, prekid aktivnosti prije nego što dođe do rizika



TRANSFER

Prebacivanje odgovornosti za rizik na treću stranu (osiguranje)

MITIGACIJA

Ograničavanje rizika provedbom mjera koje smanjuju ranjivosti i minimiziraju štetni utjecaj (prevencijske, detekcijske i korekcijske)

HR PSOR

Što je kibernetička sigurnost?

Kako ih zaštititi?

Koji su to sustavi?

Koje su to informacije?

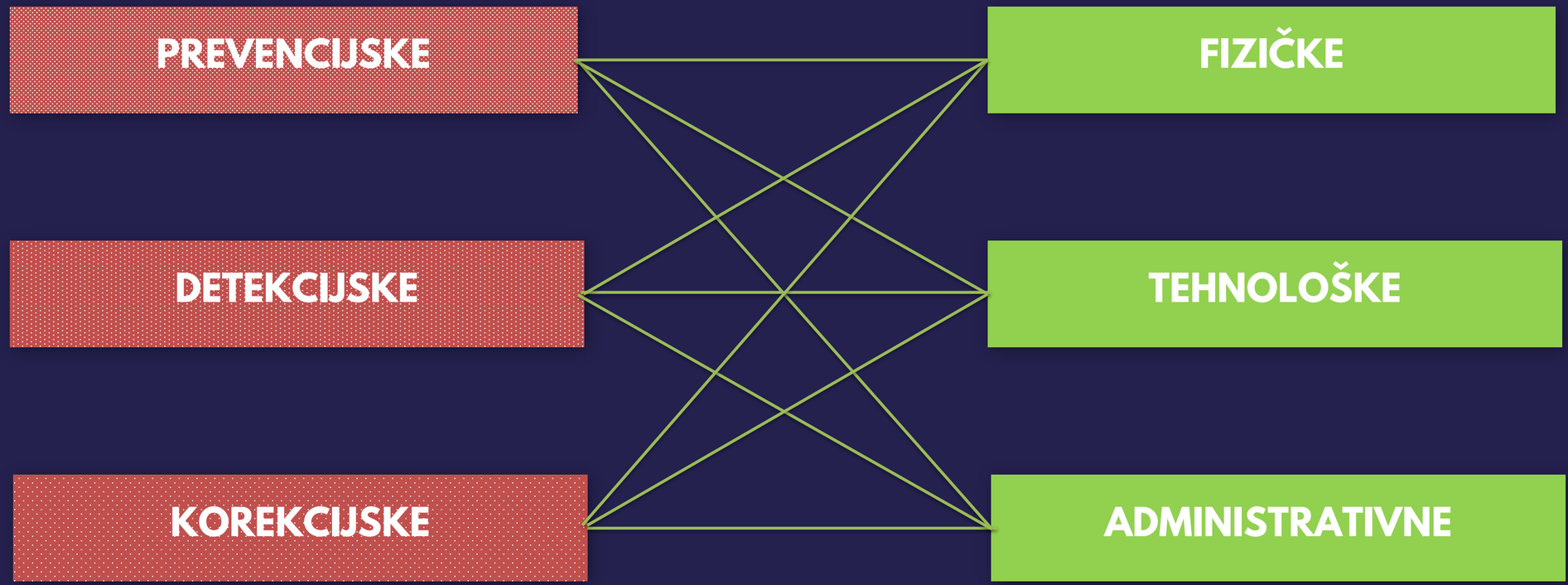
Zaštita kritičnih sustava i osjetljivih informacija od kibernetičkih napada.

Od čega ih treba zaštititi?

HR PSOR

Mjere kibernetičke sigurnosti

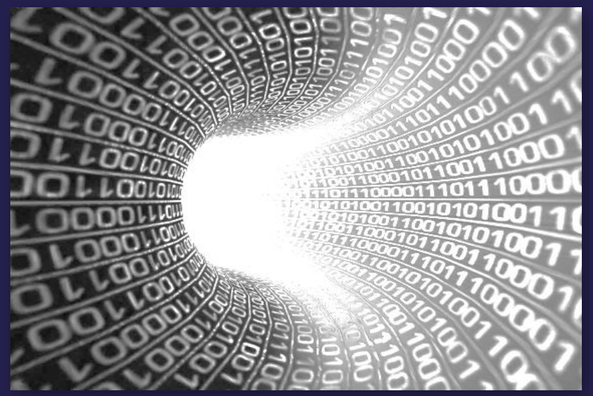
Skup praksi, tehnologija i politika posebno dizajniranih za zaštitu računalnih i mrežnih sustava od kibernetičkih napada



Ljudski faktor kao sigurnosna ranjivost

Kritična komponenta svakog sustava obrane

PODACI



LJUDSKI FAKTOR



KRIMINAL



HR PSOR



Rezultat ljudskog faktora

Verizon, Data Breach Investigations Report, 2025



Uključuje ljudski element

Verizon, Data Breach Investigations Report, 2024



Rezultat nemara zaposlenika ili izvođača

IBM, Voice of the CISO Report, 2024



Priznaje pogrešku koja je ugrozila sigurnost

Tessian, Psychology of Human Error Report, 2022

Kako dolazi do sigurnosnog incidenta?

IZABRANI STE KAO CILJ

Napredni napadi

Dobro organizirani, ciljani (jasan cilj, iskorištavanje ranjivosti), hakerski napadi u više faza

„POKUPITE” NEŠTO

Primjeri zlonamjernog softvera

Ransomware

Keyloggeri koji bilježe sve što se unese na tastaturi

NAPRAVITE POGREŠKU

Primjeri ljudskih pogreški

Osjetljivi podaci poslani pogrešnoj osobi

Krivo postupanje s podacima

Izgubljeni uređaj

„NAVEDENI STE” DA NAPRAVITE POGREŠKU

Primjeri socijalnog inženjeringa

Zlonamjerne poruke e-pošte koje izgledaju legitimno

Lažno predstavljanje

DALI STE PRILIKU

Primjeri neadekvatnih politika i procesa

Prevelike ovlasti, loša higijena lozinki

Neažuriran softver, loš „backup”

NISTE NI SVJESNI TOGA

Ograničene mogućnosti reakcije

Nedovoljna evidencija sigurnosnih događaja

Neadekvatan nadzor i otkrivanje

HR PSOR

Kako se zaštititi?

Koristite snažne lozinke

- Koristite duge, složene i jedinstvene lozinke za svaki pojedini korisnički račun
- Koristite "Password manager" – namjenski program za kreiranje i pohranu lozinki
- Koristite fraze kao lozinke

Uključite 2FA/MFA

- Kad god je moguće koristite MFA za zaštitu računa
- Nešto što znamo
- Nešto što imamo / posjedujemo
- Nešto što jesmo

Ažurirajte sav softver

- Redovito ažurirajte sav softver na svim uređajima
- Opcija automatskog ažuriranja
- Izbrišite sve što ne koristite – aplikacije / softver

Oprezno na internetu

- Uvijek provjerite jeste li na pravom mjestu
- Ima li stranica https
- Oprez sa skidanjem datoteka jer mogu sadržavati malware
- Onemogućite skočne prozore i automatsko preuzimanje datoteka
- Omogućite provjeru reputacije stranica

HR PSOR

Provjeri svoj račun!



0

Data Breaches

Good news — no pwnage found! This email address wasn't found in any of the data breaches loaded into Have I Been Pwned. That's great news!

1

Data Breach

Oh no — pwned! This email address has been found in a data breach. Review the details below to see where your data was exposed.

2

Data Breaches

Oh no — pwned! This email address has been found in multiple data breaches. Review the details below to see where your data was exposed.

HR PSOR

Kibernetička sigurnost u ESG strategiji

- **KIBERNETIČKA SIGURNOST više nije isključivo tehničko pitanje, već PREDUVJET ODRŽIVOG POSLOVANJA i ključna je komponenta ESG strategije**

- **Organizacije koje ne ulažu u kibernetičku otpornost izlažu riziku:**
  - **svoje ESG ciljeve,**
  - **poslovni kontinuitet i**
  - **dugoročnu konkurentnost.**

HR PSOR

KOR
2026.



Hvala!

THANK YOU FOR YOUR ATTENTION!

https://spansecuritycenter.eu/hr/

marina.dimicvugec@span.security, zoran.kezman@span.eu

HR PSOR HRIO HRVATSKI INDEKS ODRŽIVOSTI