Vaučeri za digitalizaciju

Ministarstvo gospodarstva i održivog razvoja kroz Nacionalni plan oporavka i otpornosti 2021. – 2026. objavio je Poziv za dostavu projektnih prijedloga „Vaučeri za digitalizaciju“

Cilj Poziva je doprinos povećanju razine digitalne zrelosti MSP-ova kroz razvoj digitalnih poslovnih modela, jačanje kapaciteta za provedbu digitalizacije i digitalne transformacije ili unaprjeđenje kibernetičke sigurnosti, što će u konačnici povećati konkurentnost i otpornost poduzeća korištenjem digitalnih tehnologija.

Prijavitelj jednim projektnim prijedlogom može zatražiti samo jedan vaučer. U postupku dodjele prijavitelj može istovremeno imati samo jedan projektni prijedlog kojim traži dodjelu vaučera za usluge koje pruža isključivo jedan pružatelj usluga, a koje obuhvaćaju jednu ili više aktivnosti prihvatljivih za traženu vrstu vaučera. Jedan prijavitelj može iskoristiti najviše dva vaučera različite vrste, uz napomenu da se oba ne mogu zatražiti na istom roku prijave.

Span d.d. jedan je od pružatelja usluga u Katalogu pružatelja usluga u okviru Poziva “Vaučeri za digitalizaciju”

Poziv obuhvaća:

Vaučer za poboljšanje digitalnih vještina	**9.990,00***
Vaučer za digitalni marketing	**9.990,00***
Vaučer za izradu strategije digitalne transformacije	**9.990,00***
Vaučer za dijagnostiku kibernetičke otpornosti	**14.500,00***
Vaučer za složena digitalna rješenja	**19.900,00***

Intenzitet potpore:

60% prihvatljivih troškova

**maksimalni iznos potpore*

Prihvatljivost prijavitelja:

Prijavitelj mora biti pravna ili fizička osoba koja je **mikro, malo ili srednje poduzeće** sukladno definiciji malih i srednjih poduzeća na način utvrđen u Prilogu I. „Definicija MSP-ova“ Uredbe Komisije br. 651/2014.

Rok za prijavu:

1. rok od 01.06. do 07.07.2023.
2. rok od 01.11. do 01.12.2023.
3. rok od 01.03. do 01.04.2024.

Projektni prijedlozi podnose se isključivo putem sustava **eNPOO**

Predviđeno trajanje projekta nije dulje od 30. lipnja 2026. godine; dokazuje se: Prijavnim obrascem, Izjavom prijavitelja (**Obrazac 2.**)

Predviđeno trajanje projekta nije dulje od 12 mjeseci od dana izdavanja vaučera; dokazuje se: Prijavnim obrascem, Izjavom prijavitelja (**Obrazac 2.**)

 | www.span.eu

VAUČER ZA DIJAGNOSTIKU KIBERNETIČKE OTPORNOSTI (CYBERSECURITY)

Aktivnosti vaučera uključuju **provjeru kibernetičke sigurnosti poduzeća** kroz provedbu sigurnosnih provjera sustava/provjera propusnosti podataka, provedbu penetracijskih ispitivanja uz izradu pripadajućih izvješća, kroz provedbu sigurnosnog testiranja i detekcije kibernetičkih prijetnji informacijskom sustavu poduzeća. Također uključuju **analizu prikupljenih podataka i definiranje dodatnih poboljšanja sustava** te generiranje izvještaja za potrebe regulatora, certifikacijskih kuća i sl. te **edukaciju zaposlenika** od strane pružatelja usluga radi povećanja osposobljenosti, za postizanje kibernetičke sigurnosti poduzeća u minimalnom trajanju od 3 sata.

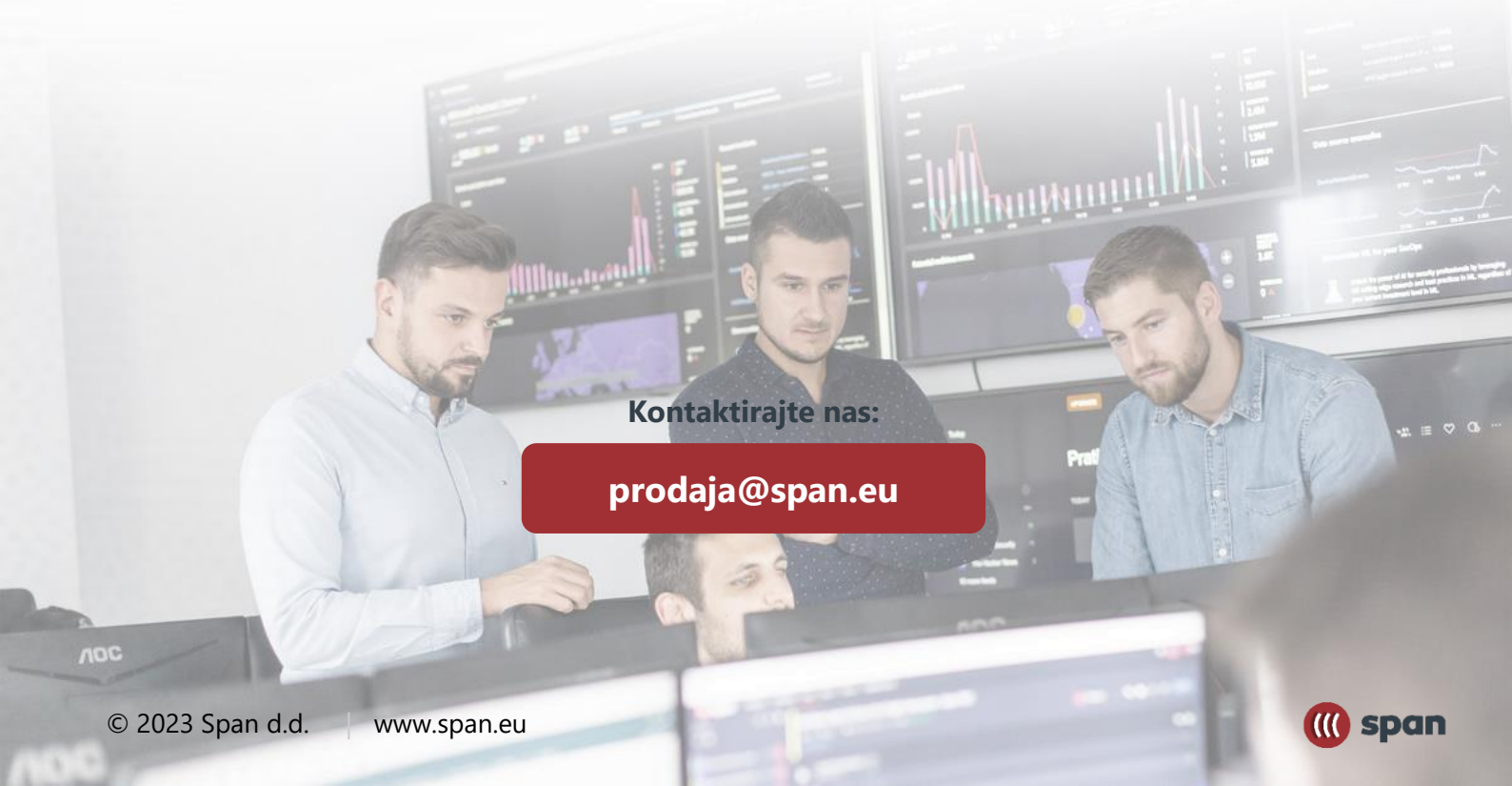
Napomena: prilikom pružanje usluge iz područja dijagnostike kibernetičke sigurnosti pružatelj usluge mora isporučiti sve navedene usluge.

Vrste aktivnosti koje nisu prihvatljive za financiranje u okviru ovog Poziva:

- sve aktivnosti koje izlaze van okvira traženog vaučera, i/ili koje se odnose na usluge drugog/drugih pružatelja usluga
- dorada internetskih stranica prijavitelja, e-trgovine, m-trgovine i mobilnih aplikacija koje ne uključuju nadogradnju novih funkcionalnosti
- promotivne aktivnosti poduzeća i oglašavanje na društvenim mrežama (Google, Facebook i dr.)
- prihvatljive aktivnosti financirane u okviru poziva „Bespovratne potpore za digitalizaciju"(referentni broj Poziva: NPOO.C1.1.2. R3-I3.01)
- sve druge aktivnosti koje nisu navedene u poglavlju 2.8 Prihvatljive aktivnosti projekta i prihvatljivi troškovi ovih Uputa

Uvjet:

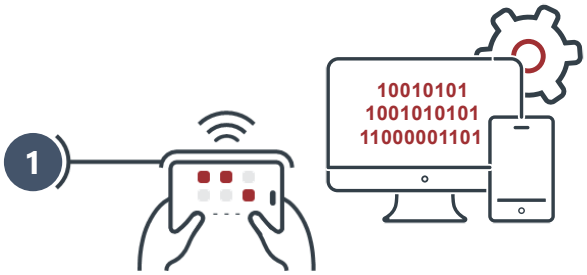
- Prijavitelj mora imati **min. 1 zaposlenika**



Kontaktirajte nas:

prodaja@span.eu

SIGURNOSNE USLUGE KOJE NUDIMO KORISNICIMA VAUČERA ZA KIBERNETIČKU OTPORNOST



SIGURNOSNA PROVJERA SUSTAVA

Sigurnosna provjera sustava uključuje analizu trenutačnog stanja sigurnosti organizacije, u sklopu koje ćemo procijeniti stanje ključnih poslovnih procesa te implementiranih tehničkih i organizacijskih mjera sigurnosti kroz navedene aktivnosti:

- **provjera zrelosti poslovnih procesa** – procijenit ćemo zrelost ključnih procesa koji su ujedno i preduvjeti za uspostavljanje sigurnosnih mjera (npr. proces klasifikacije informacija, proces upravljanja rizicima, proces upravljanja pravima pristupa, proces upravljanja sigurnosnim incidentima…)
- **provjera trenutačno uspostavljenih mjera sigurnosti** – analizirat ćemo i procijeniti stanje trenutačno implementiranih sigurnosnih mjera u organizaciji (npr. segmentacija mreže, implementirana rješenja za dodjelu/ukidanje prava pristupa, upravljanje fizičkom sigurnošću, segmentacija razvojnog/testnog/produkcijskog okruženja, definirane politike backupa…)

Rezultat sigurnosne provjere sustava je isporuka izvješća s ocjenom zrelosti informacijske sigurnosti organizacije sa strateškim i operativnim smjernicama za poboljšanje.

PENETRACIJSKA TESTIRANJA I TESTIRANJA RANJIVOSTI

Testiranja ranjivosti provode se specijaliziranim alatima, u cilju identifikacije ranjivosti IT sustava i aplikacija te detekcije kibernetičkih prijetnji. U sklopu penetracijskog testa, sigurnosni stručnjak/tester glumi stvarnog cyber napadača te pokušava uočiti i iskoristiti pronađene ranjivosti, odnosno preuzeti kontrolu nad sustavom i pristupiti osjetljivim informacijama organizacije. Organizacija na kraju dobiva izvještaj s uočenim nedostatcima i preporukama za popravak/neutralizaciju.

U okviru usluge penetracijskog testiranja i testiranja ranjivosti Spanovi stručnjaci izvršit će sljedeće aktivnosti:

- uz pomoć specijaliziranih alata pronaći će ranjivosti i propuste IT sustava i aplikacija organizacije
- pronađene ranjivosti pokušat će iskoristiti za preuzimanje kontrole nad IT sustavom organizacije
- dati smjernice za uklanjanje uočenih propusta

Nakon provedenih aktivnosti isporučuje se izvješće o provedenom penetracijskom testiranju i testiranju ranjivosti, s preporukama za uklanjanje propusta i prijedlozima za poboljšanje.

EDUKACIJA OSNOVE KIBERNETIČKE SIGURNOSTI

Trosatni tečaj o prijetnjama u on-line svijetu s praktičnim savjetima koji adresiraju različite aspekte cyber prijetnji, s ciljem podizanja znanja o kibernetičkoj sigurnosti i stjecanja osnovnih znanja o načelima kojih se pojedinci trebaju pridržavati kako bi zaštitili i sebe i svoju organizaciju. Sadržaj tečaja se fokusira na kibernetičke prijetnje oko nas i praktične koncepte kibernetičke sigurnosti.

span