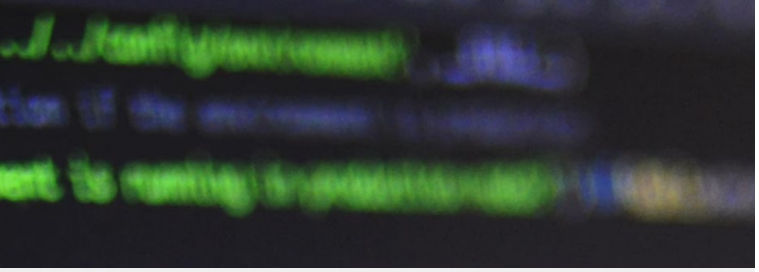

CRATIS

Vaučeri za dijagnostiku kibernetičke otpornosti (cybersecurity)

Ministarstvo gospodarstva i održivog razvoja objavilo je Poziv na dostavu projektnih prijedloga "Vaučeri za digitalizaciju" kroz Nacionalni plan oporavka i otpornosti za razdoblje od 2021. do 2026.

Cilj ovog Poziva je pomoći MSP-ovima u poboljšanju njihove digitalne zrelosti kroz razvoj digitalnih poslovnih modela, jačanje kapaciteta za provedbu digitalizacije i digitalne transformacije te unaprjeđenje kibernetičke sigurnosti. Korištenje digitalnih tehnologija na taj način će povećati konkurentnost i otpornost poduzeća.

CRATIS d.o.o. **jedan je od pružatelja usluga i nalazi se u Katalogu pružatelja usluga u okviru Vaučera za dijagnostiku kibernetičke otpornosti (cybersecurity).**

Društvo CRATIS osnovano je 2014. godine kao rezultat potrebe tržišta za beskompromisno pouzdanim Managed Cloud operaterom koji pruža cjelovite ICT usluge sa fokusom na kompleksne sustave koji traže najvišu razinu dostupnosti i pouzdanosti.

U svijetu ICT usluga CRATIS je prepoznat po svojoj stručnosti, fleksibilnosti, susretljivosti i vrhunskoj tehničkoj podršci za korisnike te je jedan od regionalnih lidera u pružanju Managed Cloud usluga.
Naši stručnjaci će na temelju provedene analize postojećeg stanja kibernetičke sigurnosti u Vašoj organizaciji izraditi sve potrebne izvještaje i ponuditi Vam adekvatna rješenja.

Ovisno o opsegu, cijena usluga može varirati između 5.000,00 i 30.000,00 eura.

O nama

Intenzitet potpore:

70% prihvatljivih troškova

Maksimalni iznos potpore:
14.500,00 eura

Rok za prijavu:

3. rok od 01.03. do 08.04.2024.

Projektni prijedlozi podnose se isključivo putem sustava eNPOO.

Prihvatljivost prijavitelja:
Prijavitelj mora biti pravna ili fizička osoba koja je mikro, malo ili srednje poduzeće sukladno definiciji malih i srednjih poduzeća.
Prijavitelj mora imati minimalno jednu zaposlenu osobu.

Predviđeno trajanje projekta nije dulje od 12 mjeseci od dana izdavanja vaučera.

sales@cratis.hr

Sigurnosne usluge koje nudimo korisnicima vaučera za dijagnostiku kibernetičke otpornosti (cybersecurity)

Provedba sigurnosnih provjera sustava

Provedba sigurnosnih provjera sustava je postupak kojim se testira sigurnost računalnih sustava, mreža ili aplikacija kako bi se identificirale ranjivosti i slabosti u njihovoj sigurnosti. Ovaj proces uključuje razne tehnike, alate i metode koje stručnjaci za sigurnost primjenjuju kako bi proaktivno otkrili sigurnosne propuste i izazove.

Redovito testiranje sustava pomaže održavati visoku razinu sigurnosti i identificirati nove ranjivosti koje se mogu pojaviti tijekom vremena.

Analiza prikupljenih podataka

Analizom prikupljenih podataka o trenutnom stanju kibernetičke sigurnosti u organizaciji se identificiraju, procjenjuju i prioritiziraju potencijalni rizici koji mogu utjecati na sigurnost informacijskog sustava ili organizacije.

Cilj analize je identificirati i razumjeti prijetnje, ranjivosti i posljedice sigurnosnih incidenata kako bi se poduzeli odgovarajući koraci za njihovo upravljanje i smanjenje.

Implementacija mrežnih i sigurnosnih rješenja

Implementacija mrežnih i sigurnosnih sustava se odnosi na prilagođavanje i implementaciju specifičnih mrežnih i sigurnosnih rješenja za potrebe određene organizacije ili sustava.

Individualiziran pristup osigurava da se mrežni i sigurnosni sustavi prilagode specifičnim zahtjevima, ciljevima i okruženju organizacije kako bi se osigurala najviša razina sigurnosti i funkcionalnosti.

sales@cratis.hr

Provedba penetracijskih testiranja

Penetracijsko testiranje je postupak kojim se provjerava sigurnost računalnih sustava, mreža ili aplikacija. Cilj penetracijskog testiranja je identificirati ranjivosti i slabosti u sustavu kako bi se procijenio njegov potencijalni rizik od neovlaštenog pristupa, zloupotrebe ili napada.

Proces penetracijskog testiranja uključuje simulaciju stvarnih napada na sustav kako bi se provjerila njegova otpornost na različite sigurnosne prijetnje.

CRATIS

Kontaktirajte nas:

sales@cratis.hr