A1 Cyber Security Paketi

Odaberite paket koji najbolje odgovara potrebama Vaše organizacije – od osnovne edukacije do napredne zaštite mrežnih sustava i korisnika.

PLATINUM
Najpotpuniji paket namijenjen organizacijama koje žele ostvariti potpunu kontrolu nad svojim sigurnosnim stanjem.
Obuhvaća procjenu postojećih procesa i tehničkih kontrola, detaljna testiranja interne i eksterne mreže, provjeru ranjivosti te simulaciju phishing napada.
Rezultati se nadopunjuju edukacijom zaposlenika kako bi se sigurnost unaprijedila i na tehničkoj i na ljudskoj razini.

- Samoprocjenu stanja kibernetičke sigurnosti (skupina 1)
- Testiranje internog i vanjskog perimetra mreže (skupina 2)
- Provjeru ranjivosti sustava (skupina 2)
- Phishing testiranje i edukaciju zaposlenika kroz platformu (skupina 2 + edukativni element)
- Opću edukaciju zaposlenika o sigurnosnim prijetnjama (skupina 3)
- vCISO

ADVANCED
Paket koji kombinira ključne tehničke provjere i edukaciju zaposlenika.
Kroz GAP analizu, testiranja perimetra i phishing kampanju, korisnik dobiva cjelovitu sliku o rizicima i preporuke za njihovo smanjenje.
Idealno rješenje za tvrtke koje žele podići sigurnosne standarde i osigurati otpornost poslovanja.

- Samoprocjenu stanja kibernetičke sigurnosti
- Interno i vanjsko penetracijsko testiranje
- Phishing testiranje s edukacijom putem platforme

STANDARD PLUS
Kompaktan sigurnosni paket koji pokriva najvažnije aspekte zaštite – procjenu postojećeg stanja, testiranje mreže i edukaciju zaposlenika.
Omogućuje brzo prepoznavanje sigurnosnih nedostataka i provedbu preventivnih mjera u skladu s najboljim praksama.

- Samoprocjenu stanja kibernetičke sigurnosti

- Testiranje internog perimetra mreže
- Opću edukaciju zaposlenika

STANDARD
Usmjeren na identifikaciju osnovnih sigurnosnih propusta i osvještavanje zaposlenika o prijetnjama.
Kombinira analizu postojećeg stanja, testiranje interne mreže i phishing simulaciju, čime tvrtka dobiva konkretne preporuke za poboljšanje zaštite.

- Samoprocjenu stanja kibernetičke sigurnosti
- Testiranje internog perimetra mreže
- Phishing testiranje

BASIC
Namijenjen organizacijama koje žele započeti put prema sustavnom pristupu sigurnosti.
Kroz GAP analizu i edukaciju zaposlenika stvara se temelj za razvoj sigurnosne kulture i implementaciju daljnjih mjera zaštite.

- Samoprocjenu stanja kibernetičke sigurnosti
- Opću edukaciju zaposlenika

Pojedinačne usluge kibernetičke sigurnosti

Sve usluge moguće je kombinirati unutar jednog projekta kako bi se ostvarila maksimalna vrijednost i sufinanciranje.

GAP ANALIZA
Analiza trenutnog stanja kibernetičke sigurnosti organizacije kroz pregled politika, procedura, infrastrukture i tehničkih kontrola.
Rezultat je izvještaj koji jasno pokazuje zrelost sustava te daje konkretne preporuke za unapređenje sigurnosnih mjera i procesa.

INTERNI PENTEST
Sigurnosno testiranje provedeno unutar mrežnog okruženja organizacije s ciljem identifikacije propusta koji bi mogli omogućiti neovlašten pristup sustavima ili podacima.
Test se provodi simulacijom napada unutar interne mreže, a rezultat je tehnički i menadžerski izvještaj s prioritetnim preporukama.

VANJSKI PENTEST
Procjena sigurnosti javno dostupnih servisa i aplikacija kako bi se identificirale ranjivosti koje bi mogle biti iskorištene izvana.

Test se izvodi iz perspektive vanjskog napadača, a cilj je pomoći organizaciji u jačanju zaštite prema internetu i smanjenju rizika kompromitacije.
VULNERABILITY ASSESSMENT Sustavna provjera sigurnosnih ranjivosti kroz automatizirano skeniranje i analizu sustava. Izvještaj prikazuje postojeće ranjivosti, njihove razine rizika i preporuke za njihovo otklanjanje, čime se stvara jasan plan za daljnje poboljšanje sigurnosti.
PHISHING TESTIRANJE Simulirana phishing kampanja kojom se provjerava otpornost zaposlenika na pokušaje socijalnog inženjeringa. Rezultat testiranja pokazuje razinu svijesti unutar organizacije i pomaže u oblikovanju budućih edukacija i internih sigurnosnih politika.
OPĆA EDUKACIJA Praktična edukacija zaposlenika i menadžmenta o najčešćim prijetnjama i sigurnosnim praksama. Kroz interaktivna predavanja i radionice sudionici uče prepoznati phishing napade, sigurno upravljati lozinkama i štititi poslovne podatke.
vCISO Cilj aktivnosti je omogućiti prijavitelju da uspostavi trajnu funkciju upravljanja kibernetičkom sigurnošću kroz vanjskog stručnjaka (vCISO) koji nadzire provedbu i održavanje tehničkih i organizacijskih mjera definiranih zakonskim i normativnim okvirom.

Napomena:

Minimalna vrijednost projekta prijavljenog na poziv **NKS-DEP-0001** iznosi **15.000 €**.

Pojedinačne usluge prikazane iznad mogu se **kombinirati** unutar jednog projekta kako bi se zadovoljili uvjeti i ostvarilo sufinanciranje do 50%.