

EVROPSKÝ DIGITÁLNÍ INOVAČNÍ HUB NORTH EAST BOHEMIA (NEB)



Zpracování kyberbezpečnostní analýzy



Partneři projektu:



ARICOMA

CXI TUL



Služby EDIH NEB:



Test before invest



Digitální akademie, networking



Finanční management

KYBERBEZPEČNOST

Zpracování kyberbezpečnostní analýzy



Nabízíme zpracování kyberbezpečnostní analýzy/auditů v různých úrovních podrobnosti, od řešení základních analýz reflektujících sledování parametrů, které předepisuje Nová směrnice EU o kybernetické bezpečnosti, resp. nový návrh ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI až po komplexnější analýzy stavu kyberbezpečnosti ve firmě či organizaci.

KYBERBEZPEČNOST

Zpracování kyberbezpečnostní analýzy

Realizace služby se uskutečňuje provedením analýzy shody kybernetické bezpečnosti /kyberbezpečnostního auditu = prvotní identifikace stavu, rizik, primární zranitelnosti a systémových doporučení v postupech i technologickém zabezpečení ICT ve firmě či organizaci veřejné správy.

Hodnocení stavu kybernetické bezpečnosti bude provedeno ve struktuře dle relevantních požadavků zákona č. 104/2017 Sb., novely zákona č. 181/2014 Sb., tzv. zákona o kybernetické bezpečnosti, a jeho doprovodné vyhlášky. Zohledněna budou též doporučení pro systém řízení bezpečnosti informací dle dlouhodobě uznávané normy ČSN ISO 27001 a na ní navazující normy ČSN ISO 27002, která je souborem doporučených opatření pro zajištění bezpečnosti informací, z této normy vychází také nová směrnice NIS2.

Základní verze analýzy bude obsahovat minimálně řešení následujících oblastí:

- a) politika analýzy rizik a politika bezpečnosti informačních systémů;
- b) řešení incidentů;
- c) řízení kontinuity provozu, jako je například správa zálohování a obnova provozu po havárii, a krizové řízení;
- d) bezpečnost dodavatelského řetězce včetně bezpečnostních aspektů týkajících se vztahů mezi každým subjektem a jeho přímými dodavateli nebo poskytovateli služeb;
- e) zabezpečení pořizování, vývoje a údržby sítí a informačních systémů, včetně zveřejňování zranitelností a jejich řešení;
- f) politiky a postupy za účelem posouzení účinnosti opatření k řízení kybernetických bezpečnostních rizik;
- g) základní postupy kybernetické hygieny a školení v oblasti kybernetické bezpečnosti;
- h) politiky a postupy týkající se používání kryptografie a případně šifrování;
- i) bezpečnost lidských zdrojů, postupy kontroly přístupu a správa aktiv;
- j) v příslušných případech používání vícefaktorových autentizačních řešení nebo trvalých autentizačních řešení zabezpečené hlasové, obrazové a textové komunikace a zabezpečených systémů nouzové komunikace v rámci subjektu.

Realizace analýzy a její výstupy

Analýza shody kybernetické bezpečnosti bude řízena expertní osobou se specializací v oboru kybernetické bezpečnosti. V rámci plnění dle této nabídky budou poskytnuty služby, jejichž cílem je zjistit a posoudit aktuální stav bezpečnosti IT infrastruktury klienta a procesů spojených s provozem této infrastruktury, zejména pak stav technických i organizačních bezpečnostních kontrol, které jsou v provozním prostředí IT infrastruktury aplikovány. Realizátor spolu s klientem vybere hloubku a šíři provedení analýzy, kyberbezpečnostního auditu od nejzákladnějšího po komplexnější dle potřeb a požadavků zákazníka. Výstupem budou též doporučená opatření vedoucí ke zlepšení stavu.

Výstupem plnění Analýzy stavu kyberbezpečnosti budou:

- **Dokument „Analýza stavu kybernetické bezpečnosti“ s návrhem doporučených opatření**
- **Přehledy dotazníkových šetření „Hodnocení kybernetické bezpečnosti“** (tabulkové podklady studie)

V případě hlubšího auditu požadovaného zákazníkem, může být sjednaným výstupem také analýza aktiv - Katalog IT služeb a jejich požadovaných parametrů (tzv. primárních aktiv).

Cena a podmínky

Podmínkou je provedení **Úvodního digitálního auditu**: základní hodnocení digitální zralosti dle metodiky Evropské komise „Digital Maturity Assessment“. Výstupem bude identifikace stavu Příjemce a definování vhodných oblastí pro implementaci dostupných digitálních technologií.

Délka trvání služby je 8 hodin. Cena služby je 505,92 EUR. Dotace 505,92 EUR. Klient hradí 0 EUR.

Kyberbezpečnostní analýza

Předpokládaná náročnost realizace analýzy je 120 hodin (bude záležet na rozsahu).

Cena služby je 110 EUR/hod, zvýhodněná cena je 15 EUR/hod (dotace 95 EUR/hod).

Při náročnosti 120 hodin je cena služby 1 800 EUR bez DPH. Bude fakturována po předání analýzy.

Dotaci na cenu služby lze poskytnout pouze malým a středním firmám (do 499 zaměstnanců). Polovina hodnoty poskytnuté dotace bude firmě zapsána do evidence podpor malého rozsahu „de minimis“.

Kontakt

Národní klastrová asociace

**budova PIANO
3. patro, číslo kanceláře 308/C
Technologická 372/2
708 00 Ostrava – Pustkovec**

PhDr. Mgr. Ivo Říha, riha@nca.cz, 775 282 431

Ing. Jiří Herinek, herinek@nca.cz, 724 315 041