Vážené dámy a páni

Obraciame sa na Vás s informáciou o možnosti získať finančné zdroje z plánu obnovy a odolnosti SR na vybudovanie či zlepšenie kybernetickej bezpečnosti vo Vašej spoločnosti.

O čo ide?

16.01.2023 nadobudla účinnosť smernica EU 2022/2555 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 tzv. Smernica NIS 2.

Členské štáty majú povinnosť uplatňovať novú smernicu najneskôr od 18.10.2024. V SR pôjde o rozsiahlu novelu zákona o kybernetickej bezpečnosti. Podľa novej smernice tak bude musieť podstatne viac subjektov a odvetví povinne prijať opatrenia na svoju kybernetickú ochranu. Po novelizácii sa bude okruh povinných subjektov v SR blížiť až k hranici 10 000 právnických a fyzických osôb.

Nové bezpečnostné ustanovenia sa budú vzťahovať na základné odvetvia kam patrí najmä energetika, doprava, bankovníctvo, zdravotníctvo, digitálna infraštruktúra a verejná správa. Smernica sa bude okrem nich vzťahovať a chrániť aj takzvané dôležité odvetvia, kam patria poštové služby, odpadové hospodárstvo, chemické látky, potraviny, výroba zdravotníckych pomôcok, elektronika, strojárstvo, motorové vozidlá či poskytovatelia digitálnych služieb. Povinnosť uplatňovať bezpečnostné opatrenia sa má vzťahovať na všetky stredné a veľké spoločnosti v týchto vybraných odvetviach. Regulácii tak bude podliehať každý podnik ktorý má viac ako 50 zamestnancov alebo ročný obrat od 10 miliónov eur.

Zavedenie smernice NIS 2 resp. uplatňovanie nových pravidiel kybernetickej bezpečnosti si od podnikateľských subjektov vyžiada investície do bezpečnosti. Aby Vaše investície boli primerané a zároveň aby ste dosiahli požadovanú kvalitu ochrany vašich informačných systémov a sietí je potrebné aby ste vedeli v akom bezpečnostnom stave sa Vaša spoločnosť nachádza a aké sú technické či ekonomické možnosti dosiahnutia požadovaných cieľov. V praxi sa tieto aktivity realizujú vypracovaním GAP analýzy a štúdie realizovateľnosti

Na financovanie týchto aktivít je možné až do výšky 15.000,- EUR využiť prostriedky z tzv. digitálnej výzvy – z prostriedkov plánu obnovy a odolnosti SR. https://vaia.gov.sk/sk/2023/07/14/vyzva-digitalne-vouchery/

Sme Cluster Kybernetickej Bezpečnosti a združujeme právnické osoby podnikajúce v oblasti kybernetickej bezpečnosti, ktoré sa zaoberajú právnymi, procesnými a technickými otázkami komplexnej ochrany informačnej bezpečnosti dátových aktív. Disponujeme členskou základňou, ktorá vie vyriešiť všetky otázky a problémy vo Vašej spoločnosti týkajúce sa kybernetickej bezpečnosti. Viac informácií o nás nájdete tu: https://clusterkb.sk

Žiadosti o poskytnutie „digitálneho voucheru" je možné predkladať od 14.8.2023. Vzhľadom na obmedzený rozsah alokovaných zdrojov predpokladáme ich vyčerpanie v priebehu niekoľkých dní. Sme pripravení pre Vás zabezpečiť komplexný servis služieb, tak aby bola Vaša žiadosť o digitálny voucher podaná včas a v súlade s požiadavkami výzvy.

Cluster kybernetickej bezpečnosti
so sídlom/seat: Školská 10/119, 031 01 Liptovský Mikuláš, Slovenská republika
bankové spojenie // bank account details: ČSOB, a.s., IBAN: SK SK58 7500 0000 0040 2603 7061,
e - mail: office@clusterkb.sk; gsm: + 421 907 136 800, IČO // ID number: 51 749 416

V prípade Vášho záujmu o bližšie informácie či vypracovanie cenovej ponuky nás čo najskôr kontaktujte telefonicky na:

+421903417862 - Mgr. Milan Brach
+421903848397 - Mgr. Martin Holič
+421907136800 - Ing. Ján Lichvár

alebo emailom na: office@clusterkb.sk

S úctou

Ing. Ján Lichvár
predseda
Cluster Kybernetickej Bezpečnosti