DOTAZNÍK

1. Čo rozumiete pod pojmom „kybernetická bezpečnosť“?

☐ Stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov.
☐ Postup ochrany digitálnych informácií, zariadení a aktív, ku ktorým patria vaše osobné informácie, kontá, súbory, fotografie a dokonca aj peniaze.
☐ Činnosti potrebné na ochranu sietí a informačných systémov, užívateľov takýchto systémov a iných osôb dotknutých kybernetickými hrozbami (*napr. zneužitie za účelom získania finančných prostriedkov formou vydierania*).
☐ Ochrana štátu a štátnych orgánov pred napadnutím treťou mocou v kyber priestore.

2. Koho sa týka kybernetická bezpečnosť?

☐ Verejných a súkromných subjektov, ktoré reguluje zákon.
☐ Subjektov kritickej infraštruktúry.
☐ Subjektov zasiahnutých kybernetickým incidentom, ktoré nie sú regulované zákonom.
☐ Nás všetkých.

3. Aké sú hlavné povinnosti Vášho subjektu vo vzťahu ku kybernetickej bezpečnosti?

☐ Plníme opatrenia, ktoré sa viažu na prevádzkovateľa základnej služby alebo poskytovateľa digitálnej služby podľa zákona č. 69/2018 Z. z.[1]
☐ Realizujeme aktivity, ktoré prispievajú k zvyšovaniu úrovne kybernetickej bezpečnosti ako informovanosť a vzdelávanie o dodržiavaní kybernetickej bezpečnosti, kybernetická hygiena, segmentácie siete, konfigurácia zariadení, penetračné testy a podobne.
☐ Využívame externé konzultačné služby a aktívne zapájame špecializované firmy pri nastavovaní bezpečnosti systémov a sietí za účelom zvýšenia úrovne kybernetickej bezpečnosti.
☐ Iné (prosím uviesť) .....

4. Čo je to kybernetický bezpečnostný incident?

☐ Akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je:

1. strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,
2. obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,
3. vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo
4. ohrozenie bezpečnosti informácií.

☐ Narušenie bezpečnosti informácií v informačných systémoch, alebo narušenie bezpečnosti služieb, alebo bezpečnosti a integrity sietí elektronických komunikácií v dôsledku kybernetickej bezpečnostnej udalosti.

[1] Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť.

☐ Narušenie informačných činností, ktoré slúžia na získavanie, zhromažďovanie, spracúvanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archiváciu a likvidáciu údajov takým spôsobom, že dôvernosť a integrita týchto informačných činností nemôže byť zaručená.
☐ Udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov.
☐ Iné (prosím uviesť) .....

5. Kde hlásim vznik, detekciu alebo riziko kybernetického bezpečnostného incidentu?

☐ Riadim sa povinnosťou hlásiť každý závažný kybernetický bezpečnostný incident, ktorý identifikujem na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov. Hlásenie kybernetických bezpečnostných incidentov vykonávam prostredníctvom jednotného informačného systému kybernetickej bezpečnosti príslušnému orgánu.
☐ Hlásim každý závažný kybernetický bezpečnostný incident, ktorý identifikujem na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov. Hlásenie kybernetických bezpečnostných incidentov vykonávam prostredníctvom manažéra kybernetickej bezpečnosti/štatutára.
☐ Hlásim každý závažný kybernetický bezpečnostný incident, ktorý identifikujem na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov. Hlásenie kybernetických bezpečnostných incidentov vykonávam prostredníctvom hlásenia medzinárodným orgánom na to určeným (ENISA).
☐ Hlásim každý závažný kybernetický bezpečnostný incident, ktorý identifikujem na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov. Hlásenie kybernetických bezpečnostných incidentov vykonávam prostredníctvom orgánov presadzovania práva (resp. orgánov činných v trestnom konaní).

5A V prípade, ak ste hlásili kybernetický bezpečnostný incident
☐ Uveďte počet incidentov, ktoré ste nahlásili ..... a komu ..... .

6. Čo znamená audit kybernetickej bezpečnosti?

☐ Splnenie si zákonných povinností, ktoré mi ukladá zákon č. 69/2018 Z. z.[1]
☐ Zvyšovanie úrovne kybernetickej bezpečnosti regulovaného subjektu, spoločnosti (firmy), orgánu verejnej moci, samosprávy alebo obce.
☐ Nástroj na zisťovanie nedostatkov úrovne kybernetickej bezpečnosti a zraniteľnosti regulovaného subjektu, spoločnosti (firma), orgánu verejnej moci, samosprávy alebo obce.
☐ Iné (prosím uviesť).....

7. Vykonali ste už audit kybernetickej bezpečnosti?

ÁNO
7A
☐ Áno a stretli sme sa s nasledujúcimi problémami:
- ☐ Žiadne problémy
- ☐ Časový rámec (*nepostačujúca doba na vykonanie auditu*)
- ☐ Personálne zdroje (*bolo to náročné na vykonanie zo strany zamestnanca/ov*)
- ☐ Finančné zdroje (*bolo to finančne nákladné*)
- ☐ Nejasná formulácia v zákone (*nie úplne sme rozumeli tejto povinnosti*)
- ☐ Iné (prosím uviesť).....

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť.

NIE

7B

☐ Nie, z dôvodu:

- ☐ Nedostatok personálnych zdrojov (chýba nám odborný pracovník)
- ☐ Nedostatok finančných prostriedkov (chýbajú nám peniaze na vykonanie auditu)
- ☐ Nedostatočná znalosť zákona (neoboznámili sme sa s danou povinnosťou)
- ☐ Nejasná formulácia v zákone (nerozumieme tejto povinnosti, keďže zákon to neupravuje jasne)
- ☐ Iné (prosím uviesť).....

8. Čo Vám chýba v zákone č. 69/2018 Z. z.[1] a čo by ste chceli upraviť (doplniť)?

.....
.....
.....

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť.