Smernica EURÓPSKEHO PARLAMENTU A RADY o odolnosti kritických subjektov (COM(2020) 829)

- https://data.consilium.europa.eu/doc/document/PE-51-2022-INIT/sk/pdf
- cieľom je znížiť zraniteľnosť a posilniť odolnosť kritických subjektov.
- kritické subjekty sú subjekty poskytujúce základné služby, ktoré sú kľúčové pre zachovanie nevyhnutných spoločenských funkcií, hospodárskych činností, verejného zdravia, bezpečnosti a ochranu životného prostredia. Musia byť schopné predchádzať hybridným útokom, prírodným katastrofám, teroristickým hrozbám a ohrozeniam verejného zdravia, chrániť sa pred nimi, reagovať na ne, zvládať ich a zotaviť sa z nich.

Smernica EURÓPSKEHO PARLAMENTU A RADY o odolnosti kritických subjektov (COM(2020) 829)

- Výroba spracovanie a distribúcia potravín – potravinárske podniky, ktoré sa zaoberajú logistikou a veľkoobchodnou distribúciou a veľkoobjemovou priemyselnou výrobou a spracovaním
- Pitná voda – dodávatelia a distribútori vody určenej na ľudskú spotrebu

Smernica EURÓPSKEHO PARLAMENTU A RADY o odolnosti kritických subjektov (COM(2020) 829)

Postup implementácie

- 2023 – príprava zákona (gestor Ministerstvo vnútra SR)
- 2024 – pripomienkovanie a predloženie zákona do NR SR
- 2026 – platnosť

- DISKUSIA ...

Zákon 497/2022 Z. z. o preverovaní zahraničných investícií a o zmene a doplnení niektorých zákonov

- preverovanie zahraničných investícií z dôvodu ochrany bezpečnosti a verejného poriadku Slovenskej republiky a Európskej únie
- gestor je Ministerstvo hospodárstva SR
- v prípade, že subjekt investície bude spadať do pôsobnosti rezortu pôdohospodárstva a rozvoja vidieka SR bude vykonané posudzovanie

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

- gestor kybernetickej bezpečnosti v SR Národný bezpečnostný úrad (zoznam digitálnych služieb, register poskytovateľov digitálnych služieb)
- poskytovateľom digitálnej služby právnická osoba alebo fyzická osoba – podnikateľ, ktorá poskytuje digitálnu službu a zároveň zamestnáva aspoň 50 zamestnancov a má ročný obrat alebo celkovú ročnú bilanciu viac ako 10 000 000 eur,
- Poskytovateľ digitálnej služby je povinný do 30 dní odo dňa začatia poskytovania digitálnej služby oznámiť úradu (názov a sídlo, kontaktné údaje, poskytovanú službu, názov, sídlo a kontaktné údaje zástupcu)
- Povinnosti poskytovateľa digitálnej služby
- (1) Poskytovateľ digitálnej služby je povinný do šiestich mesiacov odo dňa oznámenia o zaradení do registra poskytovateľov digitálnych služieb prijať a dodržiavať vhodné a primerané bezpečnostné opatrenia podľa osobitného predpisu24) na účely riadenia rizík súvisiacich s ohrozením kontinuity digitálnej služby a procesu riešenia kybernetických bezpečnostných incidentov. Na tento účel je poskytovateľ digitálnej služby povinný vyčleniť dostatočné personálne, materiálno-technické, časové a finančné zdroje s cieľom zabezpečenia kontinuity digitálnej služby.

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

- Poskytovateľ digitálnej služby
- a) bezpečnosť sietí a informačného systému a jeho schopnosť predchádzať a riešiť kybernetický bezpečnostný incident,
- b) spôsob zachovania kontinuity digitálnej služby v prípade kybernetického bezpečnostného incidentu,
- c) súlad sietí a informačného systému s bezpečnostnými štandardmi v oblasti kybernetickej bezpečnosti.

- Poskytovateľ digitálnej služby je povinný
- a) hlásiť každý kybernetický bezpečnostný incident, ak disponuje informáciami, na základe ktorých je spôsobilý identifikovať, či má tento kybernetický bezpečnostný incident podstatný vplyv podľa osobitného predpisu a to bezodkladne po jeho zistení,
- b) riešiť hlásený kybernetický bezpečnostný incident,
- c) spolupracovať s úradom pri riešení hláseného kybernetického bezpečnostného incidentu.

Kyberterorizmus a agroterorizmus

- Kyberterorizmus (počítačový terorizmus) použitie internetu na poškodenie alebo zničenie počítačových systémov za účelom plnenia politických alebo iných cieľov.
- Agroterorizmus – terorizmus v prostredí výroby poľnohospodárstva a potravinárstva. Napr. zámerné použitie patogénov, počítačové útoky a pod.
- Dôvody kybernetických útokov : snaha získať údaje o činnosti/finančné údaje, snaha o narušenie výroby/zásobovania, záškodníctvo, snaha o zničenie výrobných prostriedkov/produktov, vydieranie (finančný efekt)

- Možnosti narušenia:
- PLC – programovateľné logické senzory (teplomer, termostat),
- SCADA (Supervisory Control and Data Acquisition), IoT (Internet of Things),
- „Inteligentné“ zariadenia (mobilný telefón, traktor),

Kyberterorizmus a agroterorizmus

Možnosti ochrany/predchádzania

- pravidelne aktualizovať softvér, (sledovať informácie od výrobcu)
- dodržiavať politiku bezpečných hesiel,
- používať antivírus,
- firewall,
- monitoring činnosti v sieti,
- monitoring vonkajších pripojení,
- prehodnotenie prístupu tretích strán,
- pripravený plán obnovy činnosti
- vzdelávanie používateľov

Osobná odolnosť

- z Maslowovej pyramídy (hierarchie) potrieb patrí zabezpečenie dostatku potravín a vody medzi základné fyziologické potreby človeka
- spochybňovaním týchto základných potrieb sa narušuje psychologické pohodlie osoby

Osobná odolnosť

- v súčasnosti sa nachádzame v období klimatickej zmeny a výrazne zmenenej bezpečnostnej situácie, každý z týchto vplyvov môže ovplyvniť (ovplyvňuje) zásobovanie obyvateľstva potravinami na našom území
- Je nutné zvýšiť povedomie obyvateľstva o možnostiach predchádzaniu potravinovému nedostatku formou udržiavania vlastných zásob potravín a spôsobe ich optimálneho využitia v krízovej situácii

Ďakujem za pozornosť

Mgr. Ladislav Olekšák, oddelenie krízového riadenia MPRV SR

Tel.: 02 / 592 66 159, Mail: ladislav.oleksak@land.gov.sk