Kibernetička sigurnost – Usklađivanje s EU Uredbom 2016 / 1148 i Zakonom o kibernetičkoj sigurnosti (NN 68/20118)

Značaj

Informacije su danas osnovni resurs svakog društva i poslovnog sustava. Razvoj i primjena novih informacijsko komunikacijskih tehnologija (ICT), te globalizacija koje one omogućavaju, glavni su pokretači današnjih izrazito velikih i dramatičnih gospodarskih, tehnoloških, društvenih i drugih promjena u cijelom svijetu, pa tako i u RH. Nastao je kibernetički prostor kao virtualni prostor kojeg čine njegovi mrežni i informacijski sustavi. Oni su osnova učinkovitog i djelotvornog funkcioniranja svakog društva i poslovnog sustava. No, osim ogromnih prednosti koje donosi digitalno društvo, pojavljuju se i nove sigurnosne prijetnje. Ovaj novi pojam, nazvan kibernetički kriminal, su mnogobrojne zlouporabe koje se mogu desiti u ovom prostoru, a kibernetička sigurnost su aktivnosti i mjere kojima se postiže povjerljivost, cjelovitost i dostupnost podataka i sustava u ovom prostoru. Ukoliko **r**azina sigurnosti nije primjerena mogućim prijetnjama kojima može biti izložena informacijska imovina (podaci, aplikacije, mreže, digitalne usluge, reputacija itd.) u kibernetičkom prostoru, vodstva svake zemlje i uprave poslovnih, osobito vitalno značajnih sustava, izloženi su velikom riziku.

Zbog toga su mnoge zemlje donijele svoje strategije kibernetičke sigurnosti. No, da bi se postigla transparentnost, EU je 2016.g. usvojila direktivu pod nazivom *Directive 2016/1148 of the European Parliament and of the Councel concerning measures for a high common level of security of network and information systems across the Union*.

RH nastoji pratiti ovo područje, tako da je 2015.g. donijela svoju Strategiju kibernetičke sigurnosti i Zakon o kibernetičkoj sigurnosti (NN /2018) kojim je u naše zakonodavstvo implementirana navedena EU Uredba. Također, slijedom svojih obveza iz ovog područja, Vlada RH donijela je Uredbu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 68/2018).

Navedenim dokumentima određeno je područje od naročito 8 ključnih sektora (Energetika, Prijevoz, Bankarstvo, Infrastruktura financijskog tržišta, Zdravstvo, Opskrba vodom za piće, Digitalna infrastruktura i Poslovne usluge za državna tijela). Za ova područja definirane su 54 ključne usluge, te 84 potencijalna sigurnosna incidenta o kojima treba voditi računa.

Dionici ovih područja dužni su provoditi organizacijske i tehničke mjere kojima se postiže primjerena razina kibernetičke sigurnosti u cilju zaštite ključnih sustava. Ove mjere kategorizirane su u:

1. Upravljanje rizicima kibernetičke sigurnosti

2. Zaštitu ključnih sustava (fizičku sigurnost i sigurnost okruženja, sigurnost opskrbe, upravljanje ugovornim odnosima, upravljanje eksternalizacijom, kontrolu pristupa prostorima, fizičko i logičko razdvajanje ključnih sustava, kontrolu pristupa ključnim sustavima, vođenje dnevnika aktivnosti, zaštitu

podataka u ključnim sustavima, zaštitu od zlonamjernih programskih kodova, zaštitu od narušavanja raspoloživosti ključnih sustava, razvoj i održavanje ključnih sustava, upravljanje projektima, upravljanje sklopovskom imovinom, upravljanje promjenama programske imovine, preventivne procjene ranjivosti ključne imovine, upravljanje kontrolom poslovanja i pričuvnu pohranu) i

3. Obavješćivanje o incidentima.

Zakonski rok za implementaciju zahtjeva za osiguranje visoke razine kibernetičke sigurnosti temeljem Uredbe EU, Zakona RH i Uredbe Vlade RH je kraj 2019. godine.

Usluge ZIH-a

Konzultantske usluge

- Analiza postojećeg stanja zadovoljenja zahtjeva Zakona i Uredbe
- Izrada Politike upravljanja sigurnošću ključnih sustava
- Definiranje ciljeva, strateških smjernica očuvanja kontinuiteta poslovanja i kriterija za imenovanje osobe odgovorne za uspostavu i upravljanje sigurnošću ključnih sustava
- Definiranje ovlasti i odgovornosti vezano za sigurnost ključnih sustava
- Definiranje procesa upravljanja rizicima ključnih sustava
- Definiranje mjera upravljanja fizičkom sigurnosti i sigurnosti okruženja ključnih sustava
- Definiranje mjera osiguravanja sigurnosti opskrbe, dostupnosti opreme i drugih resursa nužnih za funkcioniranje i održavanje ključnih resursa
- Definiranje mjera upravljanja ugovornim odnosima vezanih za ključne resurse
- Definiranje načina upravljanja eksternalizacijom
- Definiranje mjera kontrole pristupa prostorima i ključnom sustavu
- Definiranje mjera potrebnih za fizičko i logičko razdvajanje ključnih sustava
- Definiranje mjera za zaštitu podataka koji se obrađuju, pohranjuju i prenose u ključnom sustavu
- Definiranje mjera zaštite programskog koda
- Definiranje mjera zaštite od narušavanja raspoloživosti ključnih sustava
- Definiranje mjera razvoja i održavanja ključnih sustava
- Definiranje mjera upravljanja projektima u vezi s ključnim sustavima
- Definiranje mjera upravljanja sklopovskom imovinom ključnih sustava
- Definiranje mjera upravljanja promjenama i konfiguracijom
- Definiranje procesa upravljanja kontinuitetom ključnih sustava
- Definiranje procesa upravljanja incidentima na ključnim sustavima

- Definiranje procesa upravljanja pričuvnom pohranom
- Definiranje procesa preventivne provjere ranjivosti ključnih sustava
- Definiranje procesa internih nadzora ključnih sustava
- Provedba edukacija s ciljem podizanja svijesti o kibernetičkoj sigurnosti

Seminari, prezentacije

- **Prezentacija poslovodstvu** o obvezama iz EU Uredbe, Zakona i Uredbe Vlade RH
- **Edukacije tima za realizaciju zahtjeva kibernetičke sigurnosti –** radionice na kojima bi se prolazili zahtjevi i način njihove realizacije
- **Edukacija za interne procjenitelje –** edukacija tima korisnika koji će provoditi interni nadzor provedbe mjera kibernetičke sigurnosti
- **Edukacija osobe korisnika koja će biti imenovana kao odgovorna osoba za uspostavu i upravljanje kibernetičkom sigurnošću -** međunarodno certificirani seminar *„Certified ISO 27032 Lead Cybersecurity manager".*

Način rada

Poduhvat Usklađivanje s EU Uredbom 2016 / 1148, Zakonom o kibernetičkoj sigurnosti (NN 68/20118) i Uredbom Vlade RH ZIH realizira zajedničkim radom svojih stručnjaka za ovo područje, predstavnika uprave poslovnog sustava zaduženog za sigurnost i tima korisnika određenog za ovu problematiku. U pripremnoj fazi ovog poduhvata radi se plan projekta s potrebnim aktivnostima i striktnim odgovornostima članova konzultantskog tima i tima korisnika. U kontrolnim točkama provodi se analiza ostvarenja plana projekta, sve do trenutka njegovog dovršetka.