Sarajevo, 15.09.2022. godine

Dana 15.09.2022. godine u Sarajevu je održan okrugli sto „Izazovi cyber sigurnosti u elektroenergetskim komapnijama“

Sposobnost nove generacije elektroenergetskih sistema (nazvanih Smart Grid) da proizvodi, prenosi i isporuči energiju je veoma zavisna od informacionih i komunikacionih sistema i njihove tehnologije. Osnova za realizaciju ove potrebe je internet tehnologija, koja obezbjeđuje automatsko razmjenjivanje podataka uz minimalnu ljudsku intervenciju. Međutim, uz navedena poboljšanja vezana za automatsku razmjenu podataka, suočavamo se sa velikim sigurnosnim problemima. Cyber napadi na automatsku kontrolu unutar razuđene kompjuterske mreže koja posjeduje izuzetno vrijedne i klasifikovane podatke mogu da se organizuju istovremeno sa hiljadama računara smještenih na neograničenim geografskim udaljenostima i u različitim državama. Ovi cyber napadi mogu prodrijeti u međusobno povezane računarske sisteme u milisekundama, ugrožavajući podatke i operacije vezane za proizvodnju, prenos i isporuku. Postavlja se pitanje, kako se može povećati povjerenje u električnu mrežu i mrežne usluge i osigurati da njihove mjere bezbjednosti zadovoljavaju potrebe nove generacije elektroenergetskih sistema, „smart grid“.

Nakon izvršenih prezentacija i diskusija, tokom rada okruglog stola „Izazovi cyber sigurnosti u elektroenergetskim komapnijama“, na kome je prisustvovalo oko 70 učesnika, predloženi su sljedeći:

ZAKLJUČCI:

1) **Aktivnosti vezane za osnivanje CERT:**

   - **Inicirati formiranje CERT tima na nivou BiH te preuzimanje obaveze upravljanja/koordinacije i akreditacije CERT timova u BiH,**
   - **Ostvariti saradnju u smislu podrške i razmjene informacija o cyber prijetnjama/incidentima između formiranih CERT timova u/izvan BiH,**
   - **Osnivanje CERT tima za EE kompanije kao podrške operatorima ključnih usluga i kao tima odgovornog za saradnju sa drugim CERT timovima.**

2) **Iako se mnogo vremenski izgubilo u radu na uspostavi procesa cyber sigurnosti na svim nivoima u BiH i dalje postoji mogućnost da se ovaj put skrati korištenjem:**

   - **Novih standarda koji omogućavaju povezanost sa cyber sigurnosnim alatima, čime se vrši automatsko upravljanje sigurnosnim kontrolama,**

- **Uvesti sistem odbrane od cyber napada korištenjem digitalnih platformi za razmjenu informacija čime bi se implementirali digitalni cyber sigurnosni ekosistemi.**

3) **Značaj problematike usporenih procesa javnih nabavki za cyber sigurnost. Ova problematika nalaže blagovremeno planiranje potrebnih sredstava kako bi se skratilo vrijeme izloženosti kompanija cyber napadima;**

4) **Ostvariti aktivnu saradnju i kontinuiranu komunikaciju među operatorima kritičnih usluga;**

5) **Podržati održavanje godišnje konferencije o cyber sigurnosti na nivou BiH;**

6) **Uposliti edukovan kadar koji ce omogućiti rad na cyber sigurnosti i koji će biti u mogućnosti obučiti i educirati nove saradnike iz ove oblasti. Na ovaj način bi stručni kadar bio u mogućnosti voditi računa o cyber sigurnosnoj higijeni u kompanijama;**

7) **Postoji potreba za otvaranjem odjela i postdiplomskih studija za cyber sigurnost na obrazovnim institucijama u BiH;**

8) **Zaključke treba dostaviti nadležnim ministarstvima i institucijama na nivou BiH i entiteta.**

Predsjednik
BH K/O CIGRÉ

Edhem Bičakčić