

Do zvyšování úrovně kybernetické bezpečnosti vynakládá desítky miliónů ročně

• ČEZ loni zachytil 6,5krát více podezřelých aktivit na sítích než před třemi lety.

• Nově spuštěné bezpečnostní dohledové centrum – iSOC (Integrated Security Operations Center) dohlíží na ochranu Skupiny ČEZ v oblastech fyzické, informační a kybernetické bezpečnosti.

• Ochrana kritické informační infrastruktury v České republice patří k prioritám nově vznikajícího Národního koordinačního centra výzkumu a vývoje v oblasti kybernetické bezpečnosti.

Energetická společnost ČEZ za účasti vedoucích představitelů Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), Vojenského zpravodajství (VZ) a Policie ČR (PČR) slavnostně otevřela nové integrované bezpečnostní dohledové centrum – iSOC, které dohlíží zejména na kybernetickou bezpečnost informačních systémů Skupiny ČEZ. Jeho úkolem je nejen detekovat bezpečnostní události a incidenty a co nejrychleji aktivovat nezbytná protiopatření, ale také dohlížet na jejich efektivní řešení a v budoucnu především bezpečnostním událostem předcházet.

Start iSOC centra završil jednu z etap komplexního zvyšování kybernetické bezpečnosti Skupiny ČEZ, které odstartovalo v roce 2016. Jde především o nastavování procesů kybernetické bezpečnosti, včetně certifikace ISMS (Information Security Management System), zvyšování bezpečnostního povědomí zaměstnanců, budování týmů specialistů

kyberbezpečnosti a realizaci mnoha technických opatření.

Jak to celé funguje? Do nového centra putují on-line data bezpečnostních logů z kancelářských, technologických i bezpečnostních systémů celé Skupiny ČEZ. Informace shromážděné moderními bezpečnostními technologiemi ihned vyhodnocují operátoři iSOC a specialisté útvaru ochrana Skupiny ČEZ. V případě potřeby konzultují výstupy i se specialisty NÚKIB, VZ nebo PČR. Synergie správně nastavených procesů, kompetentních a vysoce kvalifikovaných lidí a moderní techniky umožňují snižovat rizika hrozeb, rychle přijímat efektivní opatření k eliminaci útoků a předcházet ekonomickým ztrátám.

„Hrozby a rizika v oblasti kybernetické bezpečnosti bereme velice vážně, chceme být v této oblasti lídrem, a proto průběžně posilujeme zajištění našich systémů před kyberútoky. Doposud jsme vždy obstáli, ale v této disciplíně nemůže nikdy nastat stoprocentní uspokojení. Bezpečnostní opatření musíme neustále aktualizovat tak, aby byla adekvátní vyvíjejícím se hrozbám. Spolupracujeme s širším okruhem partnerů v čele s NÚKIB, Vojenským zpravodajstvím a Národní centrálou proti organizovanému zločinu PČR. V následujících letech předpokládáme v této oblasti výdaje v řádu stovek milionů korun,“ říká **předseda představenstva a generální ředitel ČEZ**
Daniel Beneš
.

„Opakovaně zdůrazňujeme dvě věci: kybernetickou bezpečnost je třeba řešit na úrovni nejvyššího managementu a dále že kybernetická bezpečnost stojí na spolupráci všech zainteresovaných subjektů. ČEZ se dle našich zkušeností úspěšně snaží o naplňování jednoho i druhého a nově otevírané integrované bezpečnostní dohledové centrum, které navíc umožní komplexnější přístup ke kybernetické bezpečnosti díky propojení různých oblastí bezpečnosti, je toho důkazem,“ říká **náměstek sekce Národní centrum kybernetické bezpečnosti NÚKIB**
Lukáš Kintr .

V ČR zastřešuje kybernetickou bezpečnost NÚKIB. Obrannou linii zajišťuje Vojenské zpravodajství spadající pod Ministerstvo obrany. Národní koordinační centrum výzkumu a vývoje v oblasti kybernetické bezpečnosti by mělo spadat pod Evropské průmyslové, technologické a výzkumné centrum koordinující síť národních koordinačních center v rámci EU.

Martin Schreier