20. 10. 2021

ID: 113711

ČEZ se chystá na hackery. Do zvyšování úrovně kybernetické bezpečnosti investuje desítky miliónů ročně

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.

- 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.

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**.

Za poslední roky se dramaticky zvýšil počet alertů, varování identifikovaných a vyhodnocených bezpečnostním dohledem ČEZ jako potenciální kyberhrozba. Loňských 19 971 případů je 6,5krát více než v roce 2017. Skupina ČEZ proto neustále posiluje svou kybernetickou obranu. Její zajištění se také stalo nedílnou součástí všech investičních akcí poslední doby, např. obměny technického systému fyzické ochrany jaderné elektrárny Dukovany, výstavby moderního datového centra v Tušimicích nebo nového technologického dispečinku vodních elektráren ve Štěchovicích.

- V roce 2017 činily globální ztráty z kybernetické kriminality 1,5 mld. USD, loni už 4,2 mld USD.
- Počet trestných činů v této kategorii v rámci ČR činil loni 8417, o 3073 více než o tři roky dříve.
- Přibylo útoků na nemocnice, sítě orgánů státní správy a samosprávy i větší průmyslové podniky.

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.

Věděli jste, že…

- … jen 33 procent českých firem má ucelenou bezpečnostní strategii? *(zdroj: IDC)*
- … firemní školení kyberbezpečnosti v ČR absolvovalo jen 25 % zaměstnanců *(zdroj: Kaspersky)*
- … loni napadli hackeři každou pátou nemocnici v ČR *(zdroj: Policie ČR, BDO)* a počet útoků na zdravotnická zařízení ve střední Evropě se loni zvýšil o 135 %? *(zdroj: Check Point)*
- …hitparádě světové kyberkriminality vévodí krádeže citlivých dat, vyděračský ransomware šifrující údaje nebo DDoS zahlcující webové stránky firem? *(zdroj: Comsec Global)*

Martin Schreier

mluvčí Skupiny ČEZ

Více informací naleznete na: www.cez.cz

Další články:

- Význam specializovaného vzdělávání v oblasti obchodního práva v době rostoucí regulatorní náročnosti podnikání
- Prémiový rezidenční komplex Bakers Court přináší na realitní trh komfortní bydlení s 5* službami
- ESG Simple jako praktická opora pro ESG reporting malých a středních podniků
- Digitální důkazy z webu v soudním řízení: jak doložit, co bylo online zveřejněno?
- V lednu přišel šok. Ze seznamu zmizely tisíce soudních překladatelů
- Koupě nemovitosti v Rakousku: vedlejší náklady v praxi
- Legal Innovation Day 2026: Praktické využití umělé inteligence v právní praxi
- Prémiový rezidenční komplex Bakers Court přináší na realitní trh komfortní bydlení s 5*