Operátor trhu a kybernetická bezpečnost při přeshraničním obchodování

Kateřina Novotná
OTE, a.s.

Martina Gabriel
OTE, a.s.

Igor Chemišinec
OTE, a.s.

Uplynulý čas s pandemií v zádech nám ukázal, že digitální prostor sahá mnohem dál, než jsme si dokázali představit. Digitální svět se pro mnohé z nás stal tím jediným, ve kterém bylo možné relativně bez omezení pracovat, jednat, nakupovat, bavit se nebo se setkávat s rodinou. Nároky na spolehlivé plnění povinností operátora trhu vyplývajících z energetického zákona [1] však nejen zůstaly, ale v těchto nových podmínkách i narostly. Bezvýpadkový provoz i v době pandemie prokázal, že dlouhodobé investice do odbornosti zaměstnanců a robustního systému operátora trhu a vysoké nároky na provozní a kybernetickou bezpečnost nesou své ovoce. Jak se v čase měnil právní rámec a spolupráce v oblasti kybernetické bezpečnosti na evropské úrovni a co nás do budoucna čeká z pohledu operátora trhu v oblasti jednotného trhu s elektřinou, přeshraničního obchodování a kybernetické bezpečnosti?

Quo Vadis?

Jedním ze specifik kybernetické bezpečnosti je, že je vždy o krok pozadu za pachatelem. Ačkoli se týmy po celém světě snaží předvídat kroky hackerů a permanentně aktualizovat databáze virů, nikdy je nedokážou stoprocentně předběhnout, jak vidíme na statistikách kybernetických útoků. I přes to, že jsme ušli dlouhou cestu, stále žijeme ve světě, kde jsou kybernetické hrozby realitou – ať už přichází ze strany individuálních hackerů, nebo třeba státních celků. A pokud se k tomu útoky nedají předvídat, je na místě prevence. Prevenci, a tedy ochranu před útoky, je nutno stavět na třech základních pilířích: ***resilience*** (odolnost, tj. schopnost rychle se přizpůsobovat měnícímu se prostředí při neporušení činnosti), ***cyber hygiene*** (soubor opatření, kterými by se měl řídit každý uživatel informačních technologií – počínaje informovaností, včasnou aktualizací softwaru atd.) a ***security by design*** (zahrnout tedy hledisko kybernetické bezpečnosti již do fáze technologického výzkumu a návrhů). A protože každý řetěz, i ten kybernetický, je jen tak silný, jak silný je jeho nejslabší článek, hraje významnou roli v rámci kybernetické bezpečnosti jednoznačně fungující spolupráce.

Právě tato myšlenka stála u zrodu první evropské legislativy pro kybernetickou bezpečnost. Tou byla Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (tzv. směrnice NIS) [3]. Hlavním cílem směrnice NIS bylo stanovit základní požadavky kybernetické bezpečnosti jednotlivých členských států EU, např. nutnost mít národní tým pro řešení počítačových bezpečnostních událostí (Computer Security Incident Response Team, tzv. CSIRT) nebo provádět kybernetická cvičení. Na úrovni EU byly nastaveny základní principy spolupráce, např. operační síť EU CSIRT nebo strategická skupina pro spolupráci. Směrnice NIS zároveň stanovila pravidla pro vnitrostátní dohled nad kritickými sektory, mezi které patří i energetický sektor. Směrnice NIS je nyní revidována a její nová verze, tzv. NIS 2 je očekávána v průběhu tohoto roku.

Druhým zásadním legislativním aktem na evropské úrovni je nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA (ENISA, Agentura Evropské unie pro kybernetickou bezpečnost) [4], o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií (tzv. Zákon o kybernetické bezpečnosti). Tento legislativní akt přinesl celoevropský certifikační rámec kybernetické bezpečnosti pro produkty, služby a ICT procesy. Zároveň změnil mandát evropské agentury ENISA z dočasného na trvalý a přidal agentuře nové pravomoci, úkoly i zdroje.

Příběh agentury ENISA [5] mimochodem dobře ilustruje i změnu vnímání problematiky kybernetické bezpečnosti. Každý členský stát EU má právo na to, aby na jeho území měla sídlo některá z evropských agentur. ENISA tak byla založena již v roce 2004 se sídlem v Heraklionu, hlavním městě Kréty, a byla tak jednoznačně nejvzdálenější a zároveň nejhůře dostupnou evropskou agenturou. S narůstající důležitostí kybernetické bezpečnosti a větší nutností spolupráce se její poloha i dočasný mandát ukázaly jako problém. Dnes má ENISA sice

stále oficiální sídlo na Krétě, ale kromě toho také budovu v Aténách a kancelář v Bruselu.

Česká republika v kybernetické bezpečnosti předběhla dobu. Zákon o kybernetické bezpečnosti č. 181/2014 Sb., [6] (novelizován v roce 2017) byl účinný už 4 roky před implementací evropské směrnice, a Česká republika se tak stala premiantem implementace evropské kybernetické legislativy. Ostatně i Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) [7], který je českým centrálním správním orgánem pro kybernetickou bezpečnost, vznikl po novele zákona o kybernetické bezpečnosti již v roce 2017.

Operátor trhu a kybernetická bezpečnost

V celé ekonomice, a speciálně v tak propojeném odvětví, jakým je energetika, je nutné nacházet uspokojivé odpovědi na otázky typu: Jsou systémy adekvátně chráněné a je naše spolupráce pro řešení kybernetických hrozeb dostatečná? Operátor trhu (společnost OTE, a.s., dále jen OTE) věnuje bezpečnosti svého informačního systému a kybernetické bezpečnosti při zajištění svého provozu významnou pozornost již od svého založení. OTE v rámci své činnosti zejména organizuje krátkodobý trh s elektřinou a plynem, provádí zúčtování a finanční vypořádání odchylek v elektroenergetice a plynu, zajišťuje výplatu provozní podpory výrobcům elektřiny z podporovaných zdrojů a vykonává činnosti spojené se správou rejstříku obchodování s povolenkami na emise skleníkových plynů. Zároveň jako nominovaný organizátor trhu (anglický akronym NEMO) přispívá k rozvoji přeshraničního obchodování a mezinárodní spolupráce v rámci integračních projektů na trhu s elektřinou, a podílí se tak na vytvoření jednotného evropského trhu s elektřinou. Přestože na provozu OTE není přímo závislá fyzická dodávka elektřiny a plynu, jsme si vědomi toho, že operátor trhu svou rolí poskytuje významnou podporu jednotlivým obchodním procesům na trhu s elektřinou a plynem.


ITC

Certifikační orgán systémů managementu
Institut pro testování a certifikaci, a.s.
třída Tomáše Bati 299, Louky, 763 02 Zlín, Česká republika

CERTIFIKÁT
č. 21 0001 ISMS

OTE, a. s.
Sokolovská 192/79, Karlín, 186 00 Praha 8, Česká republika
IČ: 26463318

má zavedený, dokumentovaný a funkční systém managementu bezpečnosti informací v souladu s požadavky normy

ČSN EN ISO/IEC 27001:2014

v souladu s „Prohlášením o aplikovatelnosti", verze č. 4 ze dne 23. 04. 2021 pro činnosti (služby):

- Činnosti operátora trhu podle §20a zákona č. 458/2000 Sb. na základě licence č. 150504700
- Správa veřejně přístupného rejstříku obchodování s povolenkami na emise skleníkových plynů

Datum vydání 10. 06. 2021
Platnost do: 09. 06. 2024

Obr. 1: ***Certifikát OTE podle ČSN EN ISO/IEC 27001:2014***

V této souvislosti nelze nezmínit personální i systémovou podporu účastníkům trhu v době pandemie covid-19 nebo při bezprecedentní situaci na trhu s elektřinou a trhu s plynem na konci roku 2021. Ta byla charakterizována významným nárůstem cen komodit, souvisejícím ukončováním obchodních aktivit některých dodavatelů elektřiny a plynu a následnými převody statisíců odběrných míst zákazníků těchto dodavatelů v co nejkratším čase do režimu poslední instance a později zpět ke standardním dodávkám.

Rozvoj informačního systému operátora trhu následuje rozšiřování činností OTE, tak jak mu je energetická legislativa v ČR a Evropské unii přiděluje. IT architektura operátora trhu je průběžně rozvíjena tak, aby jejím prostřednictvím bylo možné transparentně a bezpečně zajistit stabilní nárůst objemu uskutečněných obchodů, přenášených a zpracovávaných dat, včetně jejich primární validace, agregace do skupin a zajištění jejich přístupnosti pro relevantní příjemce. Operátor trhu úspěšně implementoval řadu doporučení požadovaných českou i evropskou legislativou v oblasti kybernetické bezpečnosti, tématu kybernetické bezpečnosti se věnuje zkušený tým odborníků. OTE se tak v této oblasti může, nejen z pohledu zajištění kybernetické bezpečnosti, porovnávat s organizacemi spadajícími svým charakterem pod definici kritické infrastruktury.

Zkušenosti ukazují, že z pohledu kybernetické bezpečnosti je potřeba věnovat pozornost nejen ochraně centrálních systémů, ale vždy je nutné začít nastavením systémových pravidel a jednotného přístupu k ochraně informací již na straně uživatelů a přístupu do jednotlivých systémů a k informacím. Jedním z takovýchto opatření je dodržování bezpečnostní politiky u všech zaměstnanců OTE bez rozdílu funkce či zařazení. Pravidelná kontrola přidělování přístupových práv a jejich revize, stejně jako školení zaměstnanců v oblasti kybernetické bezpečnosti, je na straně operátora trhu standardním úkonem pro omezení případných útoků proti jednotlivým zaměstnancům.

Operátor trhu úspěšně implementoval opatření vycházející z ČSN EN ISO/IEC 27001:2014 (Systém managementu bezpečnosti informací), a je tak již několik let držitelem příslušného certifikátu (viz **obr. 1**). Velký význam v oblasti bezpečnosti informačního systému a spravovaných dat má implementovaný bezpečnostní monitoring aplikací a systémů OTE (*SIEM – Security Information and Event Management*) a analýza přijímaných dat. Bezpečnostní a auditní log a zajištění integrity uložených dat není výjimkou. Aplikace SIEM řešení v CS OTE tak přináší výhody týkající se komplexnosti dohledu nad dílčími oblastmi informační bezpečnosti a jejich propojení s informacemi o aktuálních hrozbách, automatizace procesu vyhodnocování událostí, zajištění integrity uložení a archivace analyzovaných událostí za účelem forenzních aktivit nebo prokazování, připravenost na integraci událostí z dalších nástrojů informační bezpečnosti, jako například integritní management, identity management, data-leak protection, behaviorální analýza sítě a uživatelů. S ohledem na nařízení GDPR věnuje OTE pozornost i ochraně osobních dat a opatřením proti jejich úniku.

Neméně důležitá je samozřejmě i oblast fyzické

bezpečnosti provozovaných systémů. Ty jsou provozovány v oddělených systémech mimo standardní prostory sídla společnosti operátora trhu, včetně zajištění tzv. disaster recovery plánu, provozu záložního systému a pravidelně prováděných disaster recovery testů. S cílem ještě více podpořit bezpečnost provozu jsou pravidelně prováděny tzv. testy zranitelnosti (vulnerability scan) a penetrační testy. V případě nálezů jsou s ohledem na míru rizika bezodkladně přijímána vhodná opatření.

Výše uvedený výčet je jen příkladem pečlivého přístupu operátora trhu k problematice kybernetické bezpečnosti. Správnost přístupu je ověřována pravidelnými dozorovými audity (vč. auditu části systému v rámci statutárního auditu) ať už na úrovni samotného IT systému a přístupu k němu, tak i přístupu k bezpečnosti spravovaných informací. Dokladem jsou i opětovně úspěšně obhajované certifikáty splnění požadavků normy ISO/IEC 27001:2014.

Jak bylo uvedeno výše, operátor trhu v rámci svých činností je aktivní i v rámci evropského prostoru. Při jejich výkonu se řídí evropským Nařízením Komise (EU) 2015/1222 ze dne 24. července 2015, kterým se stanoví rámcový pokyn pro přidělování kapacity a řízení přetížení (CACM) [8]. Toto nařízení přispívá k zachování bezpečnosti dodávek energie, zvýšení konkurenceschopnosti a dostupnosti energie spotřebitelům, a to zavedením jednotného propojení denních a vnitrodenních trhů s elektřinou. Operátor trhu v roli Nominovaného organizátora trhu s elektřinou naplňuje požadavky tohoto nařízení ve vztahu k provozovaným informačním a komunikačním systémům.

OTE spolupracuje při naplňování nařízení CACM s ostatními evropskými provozovateli přenosových soustav a nominovanými organizátory trhu s elektřinou, a to tak, aby denní a vnitrodenní trhy, které organizuje, mimo jiné přispívaly k posílení přeshraničního obchodování a provozní bezpečnosti a umožňovaly maximální využití přenosové kapacity. Jak už ze samotné definice vyplývá, odpovědnost a role jsou rozděleny tak, že nominovaní organizátoři trhů umožňují účastníkům trhu obchodovat s energií prostřednictvím tzv. implicitních aukcí, zatímco provozovatelé přenosových soustav jsou zodpovědní za stanovování a výpočet přeshraničních kapacit a následně i v reálném čase zajištění příslušné přeshraniční výměny v rámci provozu elektrizačních soustav.

S posilováním významu přeshraničního obchodování s elektřinou a přeshraniční výměny elektřiny roste i význam kybernetické bezpečnosti v tomto segmentu. Z toho plyne nutnost analýzy rizik kybernetické bezpečnosti z pohledu aspektů přeshraničních toků elektřiny a následné definování pravidel pro společné minimální požadavky, plánování, sledování, podávání zpráv a řešení krizí (viz také Nařízení 2019/943, o vnitřním trhu s elektřinou z roku 2019, čl. 59, odst. 2, písm. e) [9.]).

Ač je primární zodpovědnost přiřazena v tomto směru provozovatelům přenosových soustav (v České republice společnost ČEPS, a.s.), resp. evropské asociaci těchto provozovatelů (European Network of Transmission System Operators, ENTSO-E [10]), následující odstavce popisují stručný vhled do dané problematiky z pohledu operátora trhu jako „stakeholdera" účastnícího se z pozice zástupce NEMO Committee (výbor nominovaných operátorů trhu s elektřinou [11]) přípravy návrhu příslušné energetické legislativy (dále také „Cybersecurity Network Code").

Síťový kodex pro aspekty přeshraničních toků elektřiny týkající se kybernetické bezpečnosti

Jak bylo vysvětleno výše, kromě obecných legislativních předpisů na evropské úrovni je nutné přijímat i specifické předpisy (tzv. síťové kodexy – viz rámeček), které plně reflektují různé potřeby odvětví infrastruktury. Jedním z nich je právě vznikající **Síťový kodex pro kybernetickou bezpečnost přeshraničních toků elektřiny:** *Network Code on Cybersecurity aspects of cross-border electricity flows*. Na základě Nařízení 2019/943 o vnitřním trhu s elektřinou z roku 2019 [12] požádala v lednu 2021 Evropská komise (EK) ENTSO-E, aby navrhla podobu příslušného síťového kodexu.

V červenci 2021 zveřejnila agentura ACER Rámcové pokyny [13], které se staly základem pro přípravu návrhu síťového kodexu, a předala je EK. Na přípravě samotného návrhu se od podzimu 2021 do ledna 2022 v rámci přípravného výboru (Drafting Committee) podílela řada entit zapojených do přeshraničního obchodování. Zástupci OTE byli v procesu přímo zapojeni právě přes aktivitu v rámci přípravného výboru.

Návrh textu byl průběžně konzultován – jak v rámci přípravného výboru, tak prostřednictvím veřejné konzultace, která se uskutečnila na přelomu listopadu a prosince 2021. Výsledný návrh síťového kodexu (dále jen kodex) byl dne 14. 1. 2022 postoupen agentuře ACER, která má 6 měsíců na jeho revizi a předložení EK.

Co jsou síťové kodexy

„Rámcové pokyny a Síťové kodexy vycházejí z článku 6 Nařízení Evropského parlamentu a Rady (EU) č. 714/2009 ze dne 13. července 2009 o podmínkách přístupu do sítě pro přeshraniční obchod s elektřinou a obsahují tržní a technická pravidla pro trh s elektřinou. Mají zpravidla přímý účinek (viz čl. 288 Smlouvy o fungování Evropské unie), tedy se vztahují na kterýkoliv subjekt práva v rámci Evropské unie a mají v zásadě charakter zákona s celounijní působností. Jsou zaměřeny primárně na provozovatele přenosových soustav, provozovatele distribučních soustav, výrobce elektřiny a energetické burzy. Sekundárně dopadají na ostatní účastníky elektroenergetického trhu, tj. obchodníky a spotřebitele."

Aktuálně platné síťové kodexy [4.]

Kodex má následující cíle:

» pokrýt nepopsaná místa v legislativě (především doplnit směrnici NIS a dále zacílit stávající směrnice a předpisy na kybernetickou bezpečnost a připravenost na rizika) v oblasti zajištění kybernetické bezpečnosti přeshraničních toků elektřiny,
» ochránit důvěrné informace v kritické infrastruktuře,
» nastavit jednotné minimální standardy pro spolupráci a řešení kybernetických hrozeb a útoků v energetice (týká se pouze elektřiny, nikoli plynu), přeshraniční komunikaci apod.,
» předcházet, zmírnit či řešit potenciální velký dopad rizik kybernetické bezpečnosti (tzn. předcházet útokům či incidentům, které mohou ovlivnit chod kritické infrastruktury a způsobit kaskádový efekt),
» nastavit společný standard pro další vývoj technologií a procesů.

Jedná se tedy o položení společných základů pro spolupráci a definici **souboru minimálních požadavků na kybernetickou bezpečnost**. Kodex tak definuje například monitoring a vyhodnocování rizik, sdílení informací – s důrazem na jejich ochranu, ale také způsob společného řešení incidentů a krizí. Určuje také rámec pro organizaci bezpečnostních cvičení a zahrnuje rovněž požadavky na zadávání zakázek. Text zohledňuje jak úroveň jednotlivých entit, tak národní a celoevropské ~~(EU)~~ hledisko. Kodex předpokládá rozdělení entit na základě provedeného hodnocení rizik (tzv. Risk Assessment) do dvou kategorií: entita s vysokým nebo kritickým dopadem (tzv. Critical Risk a High Risk Entity).

Protože se očekává, že se Kodex bude v některých bodech vztahovat i na nominované organizátory trhu s elektřinou díky jejich zapojení do tvorby a organizaci jednotného evropského trhu s elektřinou (jehož výsledkem jsou ve spolupráci s provozovateli přenosových soustav mj. přeshraniční toky), NEMO Committee možnost zapojení do přípravného výboru uvítal. Operátor trhu, vědom si své zodpovědnosti, se snaží aktivně ve své roli NEMO k danému tématu přispět, a proto byl mezi zástupci reprezentující NEMO Committee. Nominovaní organizátoři trhu s elektřinou (NEMOs) si v souvislosti s účastí vytyčili následující cíle:

» vyvarovat se riziku, že se bude Kodex překrývat s existující národní nebo evropskou legislativou, případně s právě připravovanou směrnicí NIS 2:
  – během přípravného procesu došlo k vyjasnění řady bodů a harmonizaci termínů s jinými legislativními texty,
» vyjasnit, že Kodex se bude vztahovat na přeshraniční toky s elektřinou a jakým způsobem spadají NEMOs do jeho působnosti:
  – návrh textu předaný ACER v lednu 2022 jasně určuje, že Kodex se aplikuje na aspekty kybernetické bezpečnosti u přeshraničních toků elektřiny – a toto upřesnění se dostalo i do samotného názvu Kodexu,
  – stejně tak se vyjasnilo, že malé a střední firmy jsou z působnosti Kodexu vyloučeny, pokud ovšem nejsou klasifikovány jako entita s vysokým nebo kritickým dopadem,
» zajistit zapojení NEMOs do procesu přípravy kritérií, na základě kterých se budou příjemci kodexu dělit do jednotlivých rizikových kategorií, a z nich plynoucí povinnosti:
  – kritéria a metodologie (např. právě pro rozlišení entit s vysokým a kritickým dopadem) bude vytvářet ENTSO-E a Asociace evropských provozovatelů distribučních soustav (EU-DSO) s podporou tzv. pracovní skupiny, v poslední verzi textu Kodexu jsou NEMOs explicitně uvedeni mezi členy této pracovní skupiny,
» zajistit, že bude brán ohled na specifika působení (různých) NEMOs v různých státech, případně stejných NEMOs ve více státech:
  – u plánovaného srovnávání (tzv. benchmarking guide) se podařilo dát důraz především na celkovou efektivitu opatření, nikoliv na konkrétní údaje o výdajových položkách.

Konkrétní dopad na NEMOs pak bude mj. záviset na nastavení systému kritérií pro hodnocení a metodologie, které vzejdou z práce ENTSO-E, EU-DSO a zapojení pracovní skupiny, a jejich vyhodnocení ze strany příslušných národních autorit.

I přes to, že v tuto chvíli neznáme konečné znění kodexu a z toho vyplývající práva a povinnosti pro nominované organizátory trhu, OTE nový kodex vítá jako krok ke sjednocení požadavků pro evropské aktéry v oblasti kybernetické bezpečnosti a jejího dopadu na evropskou energetiku a přeshraniční obchodování. Díky nastavení jednotného systému komunikace, spolupráce a scénářů pro řešení hrozeb a kybernetických útoků přispěje kodex k bezpečnosti energetických sítí. Důležité ale je neduplikovat povinnosti a aktivity – to se týká například již zmíněné směrnice NIS 2, která se nyní připravuje. V této fázi je samozřejmě obtížné hodnotit rozsah dopadů na operátora trhu. Nicméně s ohledem na to, že již dnes má operátor trhu ve svém informačním systému implementované vysoké standardy v oblasti IT a kybernetické bezpečnosti, provozuje při organizaci jednotného evropského trhu s elektřinou své systémy v kooperaci s ostatními provozovateli přenosových soustav a nominovaných organizátorů trhů a využívá v tomto směru jednotných softwarových řešení a tzv. *best-practice*. Díky sdílení příslušeného technického know-how a informací neočekáváme výrazný dopad do vnitřního fungování společnosti. Jsme ale připraveni všechny zákonné požadavky implementovat v nejkratším možném čase, jak tomu bylo vždy.

Závěr

Zajištění kybernetické bezpečnosti je v posledních letech skloňováno v mnoha významech a obrana proti cíleným kybernetickým útokům je dnes jedním

z klíčových parametrů provozovaných i nově budovaných informačních systémů. Bez ohledu na to, zda společnost provozuje prvek nebo systém prvků kritické infrastruktury, nebo obecně působí v energetice, podcenění rizik v této oblasti může vést ke značným přímým i nepřímým hmotným škodám. Operátor trhu v rámci svých činností v českém i evropském energetickém prostoru věnuje významnou pozornost posílení ochrany před kybernetickými útoky a pravidelně své systémy oblasti kybernetické bezpečnosti udržuje tak, aby odpovídaly nejnovějším bezpečnostním poznatkům. Zaměstnanci operátora trhu aktivně spolupracují i na mezinárodní scéně na přípravě příslušných mezinárodních legislativních aktů vedoucích k posílení bezpečnosti (obchodní, fyzické i kybernetické) přeshraniční výměny elektřiny. Příkladem je spolupráce na vytvoření připravovaného Síťového kodexu pro aspekty přeshraničních toků elektřiny týkajícího se kybernetické bezpečnosti.

Literatura:
[1] Zákon č. 458/2000 Sb., a příslušných prováděcích právních předpisů
[2] International Energy Agency: Digitalization and Energy (2017), https://www.iea.org/reports/digitalisation-and-energy , s. 128
[3] Směrnice ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii
[4] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA
[5] https://www.enisa.europa.eu/
[6] https://www.zakonyprolidi.cz/cs/2014-181
[7] https://www.nukib.cz/
[8] Nařízení Komise (EU) 2015/1222 ze dne 24. července 2015, kterým se stanoví rámcový pokyn pro přidělování kapacity a řízení přetížení (CACM)
[9] Nařízení Evropského parlamentu a Rady (EU) 2019/943 ze dne 5. června 2019 o vnitřním trhu s elektřinou
[10] https://www.entsoe.eu/
[11] https://www.nemo-committee.eu/
[12] Nařízení Evropského parlamentu a Rady (EU) 2019/943 ze dne 5. června 2019 o vnitřním trhu s elektřinou
[13] https://www.acer.europa.eu/events-and-engagement/news/acer-publishes-its-framework-guideline-establish-network-code

Ing. Igor Chemišinec, Ph.D., MBA *– v roce 2002 absolvoval Elektrotechnickou fakultu Českého vysokého učení technického v Praze, ┼Katedru elektroenergetiky. V roce 2005 ukončil doktorské studium na téže katedře obhajobou disertační práce. V roce 2010 absolvoval Master of Business Administration Program (MBA) na Czech Management Institute v Praze. Na Fakultě elektrotechnické ČVUT v Praze je místopředseda oborové rady studijního oboru Elektroenergetika. V letech 2000 až 2005 pracoval ve společnosti ČEZ, a. s., v oblasti přípravy provozu zdrojů a optimalizace portfolia zdrojů. Ve společnosti OTE působil od 1. 9. 2005 v oddělení podpory provozu a od 1. 10. 2006 do 30. 6. 2011 v pozici senior manažera zodpovědného za oblast strategie bilancování nabídky a poptávky. Členem představenstva se stal dne 1. 6. 2011.*

Ing. Martina Gabriel *– pracuje jako specialistka odboru Rozvoj trhu v OTE, a.s. Zaměřuje se především na design propojených krátkodobých trhů s elektřinou s důrazem na optimalizační nástroje a algoritmy používané pro vyhodnocení trhů. Absolvovala Sciences Po v Paříži a bakalářské studium na IMS FSV UK, dříve působila v poradenství ve Francii.*

Ing. Kateřina Novotná *– je absolventkou Národohospodářské fakulty VŠE v Praze. Mezi lety 2014-2019 pracovala jako poradkyně místopředsedy Evropského parlamentu se zaměřením na cirkulární ekonomiku, průmysl, energetiku a kybernetickou bezpečnost. Má ale zkušenosti i z oblasti PR a event managementu. V současnosti pracuje jako specialistka odboru Rozvoj trhu v OTE, a.s., kde se zaměřuje především na evropský legislativní proces a komunikaci v rámci jednotlivých evropských projektů propojování trhu.*