EVERY1

Finansuoja Europos Sąjunga

Privatumas, sauga ir saugumas skaitmeninėje energetikos aplinkoje

Kaip veikia šis kursas

Šis trumpas, 30 minučių trukmės kursas paaiškina, ką reiškia privatumas, sauga ir saugumas energetikos skaitmeninimo kontekste. Kursas taip pat nagrinėja susirūpinimą keliančius klausimus, susijusius su pažangiųjų energetikos technologijų naudojimu.

Jūs galite būti:

- Domina pažangių technologijų naudojimas, siekiant geriau suprasti savo energijos naudojimą, bet nežinote, kaip apsaugoti savo asmeninę informaciją.
- Esate smalsūs, kaip jūsų asmeninė informacija naudojama ir dalijamasi naudojant skaitmenines technologijas.
- Norite geriau suprasti privatumą, saugumą ir apsaugą energetikos skaitmeninimo kontekste.

Šis kursas padės jums geriau suprasti skaitmeninį energetikos perėjimą ir padės jums pradėti savo skaitmeninę energetikos kelionę! Jis yra vienas iš 12 kursų, vadinamų *„Skaitmeninės energetikos pagrindai“*, kuriuos parengė projektas „Every1“, kurio tikslas – sudaryti sąlygas ir įgalinti visus dalyvauti energetikos perėjime. Daugiau informacijos apie projektą rasite adresu: https://every1.energy

Kurso pabaigoje siūlome jums susipažinti su papildomomis mokymosi medžiagomis. Tai apima kursą *„Kas yra skaitmeninis energetikos perėjimas?“*, kuriame nagrinėjama, kas yra skaitmeninė energetika ir kokios priežastys skatina pereiti prie energijos gamybos ir vartojimo skaitmeninimo.

Tai yra originalaus anglų kalbos kurso vertimas, kuriame yra galimybė atlikti trumpą testą ir gauti „Every1“ skaitmeninį ženklelį.

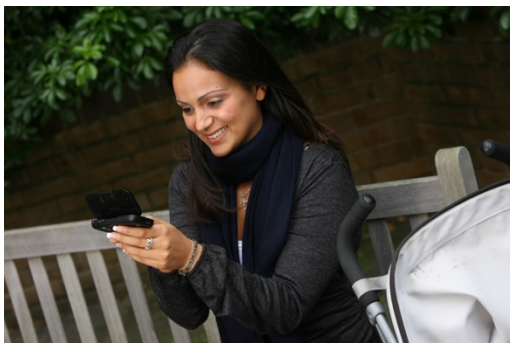
Šis projektas finansuojamas pagal Europos Sąjungos mokslinių tyrimų ir inovacijų programą „Horizontas“ (2021–2027 m.) pagal dotacijos sutartį Nr. 101075596. Vienintelė atsakomybė už šio kurso turinį tenka projektui „Every1“ ir nebūtinai atspindi Europos Sąjungos nuomonę.

Mokymosi rezultatai

Baigę šį trumpą kursą, turėtumėte gebėti:

- Skirti privatumą, saugą ir saugumą energijos skaitmeninimo srityje.
- Suprasti pagrindinius iššūkius užtikrinant privatumą, saugumą ir saugumą naudojant skaitmenines technologijas energetikoje.
- Žinoti savo teises pagal Bendrąjį duomenų apsaugos reglamentą (BDAR) energetikos duomenų atžvilgiu.
- Taikyti praktinius patarimus, kaip apsaugoti savo duomenis ir padidinti savo skaitmeninį energetinį saugumą.

Įvadas



Skaitmeninės technologijos tampa neatsiejama mūsų gyvenimo dalimi, todėl privatumas, sauga ir saugumas, susiję su mūsų asmenine informacija energetikos skaitmeninimo kontekste, tampa vis svarbesni.

Pažangieji skaitikliai, mobiliosios programėlės ir kiti skaitmeniniai įrenginiai renka ir dalijasi duomenimis, siekdami padidinti energijos vartojimo efektyvumą, tačiau tai taip pat gali kelti susirūpinimą dėl duomenų privatumo ir saugumo. Prieš pradėdami, panagrinėkime, ką reiškia duomenų privatumas, sauga ir saugumas. Tai tarpusavyje susijusios, bet skirtingos sąvokos:

- **Privatumas** susijęs su asmeninės informacijos apsauga.
- **Saugumas** reiškia užtikrinimą, kad skaitmeninių technologijų naudojimas nekelia fizinės ar psichologinės žalos.
- **Saugumas** yra susijęs su duomenų apsauga nuo neteisėtos prieigos ar atakų.

Šiame kurse ne tik aptarsime įvairius iššūkius, susijusius su mūsų energetikos privatumu, sauga ir saugumu, bet ir veiksmus, kurių galite imtis, kad apsisaugotumėte. Taip pat aptarsime, kaip vyriausybės ir energijos tiekėjai saugo jus ir jūsų duomenis, taip pat infrastruktūrą, kuri leidžia naudoti skaitmenines technologijas energijos gamybai ir vartojimui.

Skaitmeninės technologijos ir skaitmeninis energetikos perėjimas

Kaip galbūt matėte kurse *„Išmanieji prietaisai ir skaitmeninės energetikos technologijos“*, kuriame išsamiau nagrinėjami įvairūs išmaniųjų prietaisų tipai, yra daugybė skaitmeninių technologijų, kurios palaiko energetikos skaitmeninimą.

Skaitmeninė energetika yra sudėtinga tarpusavyje susijusių technologijų ir suinteresuotųjų šalių ekosistema. Pagrindiniai komponentai yra šie:

- **Pažangieji skaitikliai:** įrenginiai, kurie automatiškai renka ir perduoda duomenis apie energijos naudojimą energijos tiekėjams. Pažangieji skaitikliai užtikrina tikslesnį atsiskaitymą, suteikia informacijos apie vartojimo modelius ir galimybę dalyvauti paklausos reagavimo programose, kuriose galite reguliuoti energijos naudojimą pagal paklausą ir kainų signalus.
- **Pažangieji tinklai:** modernizuoti elektros tinklai, kurie naudoja skaitmenines technologijas elektros srautui stebėti ir valdyti. Jie užtikrina dvipusį ryšį tarp tiekėjo ir vartotojo, leidžia realiuoju laiku stebėti energijos suvartojimą ir integruoti atsinaujinančius energijos šaltinius.

- **Daiktų internetas (IoT) energetikoje:** sujungtų prietaisų (termostatų, buitinių prietaisų, elektromobilių įkroviklių) tinklas, kuris renka ir keičiasi duomenimis, leidžiantis nuotoliniu būdu valdyti ir optimizuoti energijos naudojimą.

Duomenys apie energiją gali apimti vartojimo modelius, naudojimo laiko duomenis, informaciją apie prietaisus ir netgi elgesio duomenis, nustatytus pagal naudojimą. Šie duomenys gali padėti jums suprasti savo energijos naudojimą, galbūt sutaupyti pinigų ir priimti pagrįstus sprendimus. Jie taip pat gali padėti energijos tiekėjams (pavyzdžiui, jūsų elektros tiekėjui) optimizuoti tinklą, pasiūlyti jums individualizuotas paslaugas ir nustatyti sukčiavimą.

Jūsų energijos duomenis paprastai renka jūsų energijos tiekėjas, tačiau jie taip pat gali būti perduodami arba prieinami skaitiklių operatoriams, duomenų agregatoriams, trečiųjų šalių paslaugų teikėjams ir galbūt vyriausybinėms agentūroms. Energijos duomenys yra naudingi politikos formuotojams, pavyzdžiui, padedant kurti veiksmingą energetikos politiką ir reglamentus.

Duomenys apie energijos naudojimą gali apimti konfidencialią informaciją. Kadangi prieigą prie jūsų duomenų gali turėti įvairios organizacijos ir juos naudoti įvairiais būdais, tai gali kelti susirūpinimą. Vėliau kurso metu pasiūlysime keletą būdų, kaip galite padidinti savo energijos privatumą, saugumą ir apsaugą. Pirmiausia pažvelkime į kai kurias dažnas kibernetines grėsmes ir tai, kas daroma siekiant užtikrinti skaitmeninių sistemų saugumą.

Kibernetinis saugumas energetikos sektoriuje

Dėl skaitmeninės energetikos sektoriaus transformacijos jis tapo kibernetinių atakų taikiniu, kurios gali sutrikdyti energijos tiekimą ir kelti pavojų konfidencialiai informacijai. Dažnos kibernetinės grėsmės yra šios:

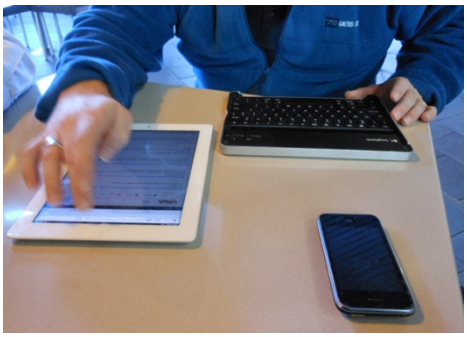
- **Kenkėjišką programinę įrangą** (kenkėjišką programinę įrangą, kuri gali pakenkti kompiuterinėms sistemoms ir duomenims).
- **Išpirkos reikalaujanti programinė įranga** (kenksminga programinė įranga, kuri užšifruoja jūsų failus, padarydama juos neprieinamus, ir reikalauja išpirkos už prieigos atkūrimą).
- **Paslaugų atsisakymo atakos** (šios atakos siekia užkimšti sistemą ar tinklą srautu, kad ji taptų neprieinama teisėtiems naudotojams).
- **Sukčiavimo apsimetant** (sukčiavimo bandymai gauti konfidencialią informaciją, pvz., slaptažodžius ar kredito kortelių duomenis, apsimetant patikimu subjektu).

Kritinės infrastruktūros apsaugai reikalingos tokios priemonės kaip tinklo segmentavimas, t. y. didesnio tinklo padalijimas į mažesnius, izoliuotus segmentus. Tai riboja kibernetinių atakų

plitimą ir sumažina galimą žalą, riboja prieigą prie valdymo priemonių, aptinka ir užkerta kelią įsibrovėliams bei leidžia pritaikyti prieigą prie valdymo priemonių.

ES kibernetinio saugumo aktas stiprina kibernetinį saugumą visoje ES ir nustato produktų ir paslaugų saugumo sertifikavimo taisykles. Svarbu užtikrinti skaitmeninių energetikos sistemų saugumą. Tai apima:

- **Kiberfizinės sistemos:** šių sistemų, kuriose fizinė infrastruktūra valdoma skaitmeniniu būdu, apsauga nuo kibernetinių atakų, kurios gali turėti realių pasekmių.
- **Saugos standartai:** ES saugos standartų laikymasis skaitmeniniams įrenginiams ir energetikos sistemoms, siekiant užtikrinti jų saugų naudojimą ir priežiūrą.



Bendrasis duomenų apsaugos reglamentas (BDAR) suteikia jums konkrečias teises, susijusias su jūsų asmeniniais duomenimis, įskaitant energijos duomenis. Šios teisės, susijusios su jūsų asmeniniais duomenimis, apima:

- **Teisė susipažinti:** galite paprašyti savo tiekėjo pateikti jūsų energijos duomenų kopiją.
- **Teisė į ištaisymą:** galite paprašyti, kad bet kokie netikslūs ar trūkstami duomenys būtų ištaisyti ar atnaujinti.
- **Teisė į ištrynimą:** tam tikromis aplinkybėmis galite paprašyti, kad jūsų duomenys būtų ištrinti.
- **Teisė apriboti tvarkymą:** galite apriboti savo duomenų naudojimą.
- **Teisė į duomenų perkeliamumą:** galite gauti savo duomenis perkeliamu formatu.

Jūsų energijos privatumo, saugos ir saugumo stiprinimas

Kadangi energijos skaitmeninimas ir skaitmeninių technologijų naudojimas energijos suvartojimui ir gamybai valdyti tampa įprastu reiškiniu, čia pateikiame keletą patarimų, kurie padės jums padidinti energijos privatumą, saugumą ir apsaugą.

- **Apsaugokite savo išmaniuosius įrenginius:** naudokite stiprius slaptažodžius, įjunkite dviejų veiksnių autentifikavimą ir nuolat atnaujinkite programinę įrangą.
- **Apsaugokite savo tinklą:** apsaugokite savo „Wi-Fi“ tinklą, vengiate naudoti viešąjį „Wi-Fi“ tinklą jautrioms veikloms ir apsvarstykite galimybę naudoti ugniasienę.
- **Kontroliuokite savo duomenis:** atidžiai perskaitykite privatumo politiką, naudokitės savo BDAR teisėmis ir atsisakykite duomenų dalijimosi, jei tai jums nepatogu.

Skaitmeninė energetikos sritis nuolat vystosi, reguliariai atsiranda naujos technologijos ir grėsmės. Norint užtikrinti savo privatumą, saugą ir saugumą, svarbu būti informuotam apie šias tendencijas.

Štai keletas pavyzdžių naujų technologijų, kurios dabar arba ateityje gali vaidinti svarbesnį vaidmenį energetikos skaitmeninimo srityje:

- **Blokų grandinės technologija:** blokų grandinė, decentralizuota buhalterinės apskaitos technologija, gali revoliucionizuoti energijos duomenų valdymą, nes suteikia saugų, skaidrų ir apsaugotą nuo klastojimo būdą stebėti ir dalytis duomenimis.
- **Dirbtinis intelektas (DI) ir mašininis mokymasis (MM):** DI ir MM algoritmai gali būti naudojami energijos duomenims analizuoti, anomalijoms aptikti ir potencialioms saugumo grėsmėms prognozuoti, taip didinant bendrą energijos sistemų saugumą.
- **Kvantiniai skaičiavimai:** nors kvantiniai skaičiavimai dar yra ankstyvoje stadijoje, jie gali pakeisti esamus šifravimo metodus, o tai kelia naują iššūkį duomenų saugumui energetikos sektoriuje.

Išvada

Energijos sektoriaus skaitmeninė transformacija teikia didžiules viltis sukurti tvaresnę, efektyvesnę ir į klientą orientuotą energetikos sistemą. Tačiau šios transformacijos privalumai gali būti visiškai realizuoti tik tuo atveju, jei aktyviai ir nuolat spręsime energetikos privatumo, saugos ir saugumo iššūkius.

Kaip energijos vartotojai, mes atliekame svarbų vaidmenį kuriant saugią skaitmeninę energetikos ateitį. Suprasdami savo teises pagal BDAR, imdamiesi aktyvių veiksmų savo duomenims apsaugoti ir pasirinkdami energijos tiekėjus bei paslaugų teikėjus, kurie teikia pirmenybę privatumui ir saugumui, mes galime užtikrinti, kad mūsų asmeninė informacija liktų apsaugota. Be to, nuolat informuodamiesi apie kibernetinio saugumo grėsmes ir geriausią praktiką, mes galime padėti apsaugoti energetikos infrastruktūrą, kuria visi naudojamės.

Perėjimas prie skaitmeninės energetikos sistemos yra ne tik technologijų klausimas, bet ir galimybė įgalinti asmenis ir bendruomenes aktyviai dalyvauti skaitmeninės energetikos perėjime. Naudodami skaitmenines priemones ir priimdami pagrįstus sprendimus, galime prisidėti prie švaresnės, patikimesnės ir teisingesnės energetikos ateities.

Papildomi ištekliai

- Daugiau apie savo teises pagal ES duomenų apsaugos taisykles skaitykite skyriuje *„Kokios yra mano teisės?“.* https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_en#:~:text=object%20to%20the%20processing%20of,controller%20(‘data%20portability’)%3B

- Sužinokite daugiau apie ES kibernetinio saugumo aktą ir kaip jis jus apsaugo https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
- Peržiūrėkite duomenų apsaugos poveikio vertinimą (DPIA) dėl pažangiųjų tinklų ir pažangiųjų skaitiklių. https://energy.ec.europa.eu/topics/markets-and-consumers/smart-grids-and-meters/data-protection-impact-assessment-smart-grid-and-smart-metering-environment_en
- Daugiau informacijos apie tai, kaip Europos Komisija mus saugo, rasite šiame straipsnyje apie *kritinę infrastruktūrą ir kibernetinį saugumą.* https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en

Padėkos

„Privatumas, sauga ir saugumas skaitmeninėje energetikos erdvėje“ yra adaptuota medžiaga iš Tarptautinės energetikos agentūros (IEA) „Duomenų privatumas skaitmeninės energetikos eroje“ https://www.iea.org/reports/digitalisation-and-energy ir „Kiberatsparumo stiprinimas elektros sistemose“ https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems, (toliau – „Originalūs darbai“), kurie abu yra licencijuoti pagal CC BY 4.0. Šis adaptavimas yra parengtas ir paskelbtas „Every1 Project“ („Adaptuotojas“) ir licencijuotas CC BY 4.0., jei nenurodyta kitaip. Tai yra „Every1“ projekto darbas, sukurtas remiantis IEA medžiaga, ir „Every1“ projektas yra vienintelis atsakingas už šį adaptuotą darbą. Adaptuotas darbas nėra jokiu būdu patvirtintas IEA.

Adapteris pakeitė originalius kūrinius šiais aspektais:

- Adaptacija ypač daug dėmesio skiria originalių kūrinių energetikos privatumo, saugos ir saugumo aspektams.
- Techninė kalba buvo supaprastinta, kad būtų suprantama plačiajai auditorijai.
- Pridėti praktiniai patarimai.
- Įtraukta nauja informacija iš Europos Komisijos šaltinių, susijusi su BDAR ir ES kibernetinio saugumo aktu.

Nuotraukų autoriai

Pagrindinis kurso vaizdas: „Untitled“ autorius Mike Fritcher, licencija CC BY-SA 2.0.
Įvadas: Moteris su vaiku parke naudojanti „Windows Mobile“ įrenginį, autorius Gail, licencija CC BY-ND 2.0.
Skaitmeninės technologijos ir skaitmeninis energetikos perėjimas: „Echelon“ išmanusis skaitiklis, autorius Patrik Tschudin, licencija CC BY 2.0.
Kibernetinis saugumas energetikos sektoriuje: „Mobile Worker“ autorius Michael Coghlan, licencija CC BY-SA 2.0.
Jūsų energetinio privatumo, saugos ir saugumo stiprinimas: duomenys, autorius Arismendy Polanco, yra bendrai naudojami pagal Public Domain Mark 1.0.