Privaatsus, ohutus ja turvalisus digitaalses energiamaastikus

Kuidas see kursus toimib

See lühike, 30-minutiline kursus selgitab, mida tähendavad privaatsus, ohutus ja turvalisus energia digitaliseerimise kontekstis. Kursus käsitleb ka muresid seoses arukate energiatehnoloogiate kasutamisega.

Võib-olla olete:

- Huvitatud nutikate tehnoloogiate kasutamisest, et paremini mõista oma energiatarbimist, kuid ebakindel, kuidas kaitsta oma isiklikke andmeid.
- Huvitatud sellest, kuidas teie isikuandmeid digitaaltehnoloogiate kasutamisel kasutatakse ja jagatakse.
- Soovite paremini mõista privaatsust, ohutust ja turvalisust energia digitaliseerimise kontekstis.

See kursus süvendab teie arusaama digitaalsest energiaüleminekust ja toetab teie enda digitaalset energiateekonda! See on osa 12-kursuselisesarjast *„Digital Energy Essentials*" (Digitaalse energia olulised elemendid), mille on välja töötanud Every1 projekt, mille eesmärk on võimaldada ja toetada kõigi osalemist energiaüleminekus. Lisateavet projekti kohta leiate aadressilt: https://every1.energy

Kursuse lõpus soovitame teile mõningaid täiendavaid õppematerjale. Nende hulka kuulub kursus *„Mis on digitaalne energiaüleminek?"*, milles uuritakse, mis on digitaalne energia ja millised on põhjused, miks meie energia tootmine ja tarbimine digitaliseeritakse.

See on kursuse originaalversiooni tõlge inglise keelest, mis sisaldab võimalust täita lühike test ja teenida Every1 digitaalne märgis.

See projekt on saanud rahastust Euroopa Liidu teadusuuringute ja innovatsiooni programmi Horizon (2021–2027) raames toetuslepingu nr 101075596 alusel. Kogu vastutus käesoleva kursuse sisu eest lasub Every1 projektil ja ei pruugi kajastada Euroopa Liidu seisukohta.

Õpitulemused

Pärast selle lühikursuse läbimist peaksite olema võimeline:

- Eristama privaatsust, ohutust ja turvalisust energia digitaliseerimisel.
- Mõistma peamisi väljakutseid privaatsuse, ohutuse ja turvalisuse tagamisel digitaaltehnoloogiate kasutamisel energeetikas.
- Olla teadlik oma õigustest seoses energiaandmetega vastavalt isikuandmete kaitse üldmäärusele (GDPR).
- Rakendama praktilisi nõuandeid oma andmete kaitsmiseks ja digitaalse energiajulgeoleku parandamiseks.

Sissejuhatus

Kuna digitaaltehnoloogiad on muutunud meie elu lahutamatuks osaks, on energia digitaliseerimise kontekstis üha olulisemaks muutumas meie isikuandmete privaatsus, ohutus ja turvalisus.

Arukad arvestid, mobiilirakendused ja muud digitaalsed seadmed koguvad ja jagavad andmeid energiatõhususe parandamiseks, kuid see võib tekitada ka muret andmete privaatsuse ja turvalisuse pärast.
Enne alustamist vaatame lähemalt, mida me mõistame andmete privaatsuse, turvalisuse ja kaitse all. Need on omavahel seotud, kuid erinevad mõisted:

- **Privaatsus** on seotud isikuandmete kaitsega.
- **Turvalisus** tähendab digitaaltehnoloogiate kasutamisega füüsilise või psühholoogilise kahju tekitamise vältimist.
- **Turvalisus** keskendub andmete kaitsmisele volitamata juurdepääsu või rünnakute eest.

Selles kursuses vaatame mitte ainult meie energia privaatsuse, ohutuse ja turvalisuse erinevaid väljakutseid, vaid ka meetmeid, mida saate enda kaitsmiseks võtta. Vaatame ka, kuidas valitsused ja energiatarnijad kaitsevad teid ja teie andmeid, samuti infrastruktuuri, mis võimaldab digitaaltehnoloogiate kasutamist energia tootmiseks ja tarbimiseks.

Digitaaltehnoloogiad ja digitaalne energiaüleminek

Nagu te võisite näha kursusel *„Nutikad seadmed ja digitaalne energiatehnoloogia”*, mis uurib põhjalikumalt erinevaid nutikate seadmete tüüpe, on olemas mitmesuguseid digitaaltehnoloogiaid, mis toetavad energia digitaliseerimist.

Digitaalne energiamaastik on omavahel seotud tehnoloogiate ja huvirühmade keerukas ökosüsteem. Peamised komponendid on järgmised:

- **Nutikad arvestid:** seadmed, mis koguvad ja edastavad automaatselt andmeid energiatarbimise kohta energiatarnijatele. Nutikad arvestid pakuvad täpsemat arveldust, ülevaadet tarbimisharjumustest ja võimalust osaleda nõudluse reageerimise programmides, kus saate kohandada oma energiatarbimist vastavalt nõudlusele ja hinnasignaalidele.
- **Arukad võrgud:** moderniseeritud elektrivõrgud, mis kasutavad digitaaltehnoloogiaid elektri voolu jälgimiseks ja juhtimiseks. Need võimaldavad kahesuunalist suhtlust kommunaalteenuste pakkuja ja tarbija vahel, võimaldades energia tarbimise reaalajas jälgimist ja taastuvate energiaallikate integreerimist.

- **Asjade internet (IoT) energeetikas:** ühendatud seadmete (termostaadid, kodumasinad, elektriautode laadijad) võrk, mis kogub ja vahetab andmeid, võimaldades energia kasutamise kaugjuhtimist ja optimeerimist.

Energiaandmed võivad hõlmata tarbimisharjumusi, kasutusaega, kodumasinate andmeid ja isegi kasutamisest tuletatud käitumist. Need andmed aitavad teil mõista oma energiatarbimist, potentsiaalselt raha säästa ja teha teadlikke valikuid. Samuti aitavad need energiaettevõtjatel (nt teie elektrienergia tarnijal) võrku optimeerida, pakkuda teile personaliseeritud teenuseid ja avastada pettusi.

Teie energiatarbimise andmeid kogub tavaliselt teie energiatarnija, kuid neid võivad jagada või neile juurdepääsu omada ka arvestite operaatorid, andmete koondajad, kolmandate osapoolte teenusepakkujad ja potentsiaalselt ka valitsusasutused. Energiatarbimise andmed on kasulikud poliitikakujundajatele, näiteks toetades tõhusate energiapoliitikate ja -eeskirjade väljatöötamist.

Energiakasutuse andmed võivad sisaldada tundlikku teavet. Kuna teie andmetele võib juurdepääs olla mitmetel erinevatel organisatsioonidel, kes võivad neid erineval viisil kasutada, võib see tekitada muret. Kursuse hilisemas osas pakume välja mõned viisid, kuidas saate parandada oma energiaalast privaatsust, ohutust ja turvalisust. Esmalt vaatame mõningaid levinud küberohtusid ja seda, mida tehakse digitaalsüsteemide ohutuse tagamiseks.

Küberjulgeolek energeetikasektoris

Energiasektori digitaalne ümberkujundamine on muutnud selle küberrünnakute sihtmärgiks, mis võivad häirida energiavarustust ja ohustada tundlikku teavet. Tüüpilised küberohud on järgmised:

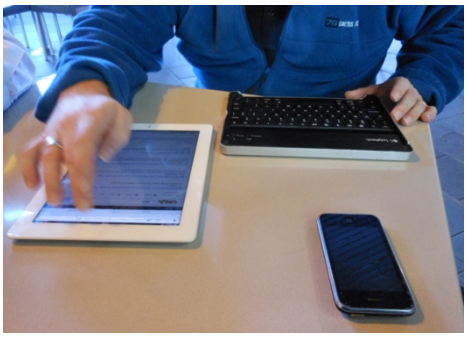
- **Pahavara** (pahatahtlik tarkvara, mis võib kahjustada arvutisüsteeme ja andmeid).
- **Lunavara** (pahatahtlik tarkvara, mis krüpteerib teie failid, muutes need kättesaamatuks, ja nõuab lunaraha maksmist juurdepääsu taastamiseks).
- **Teenuse keelamise rünnakud** (need rünnakud on suunatud süsteemi või võrgu ülekoormamisele liiklusega, muutes selle kättesaamatuks seaduslikele kasutajatele).
- **Phishing-pettused** (pettused, mille eesmärk on saada tundlikku teavet, nagu paroolid või krediitkaardiandmed, teeseldes, et tegemist on usaldusväärse asutusega).

Kriitilise infrastruktuuri kaitsmiseks on vaja meetmeid, nagu võrgu segmentimine, mis tähendab suurema võrgu jagamist väiksemateks, isoleeritud segmentideks. See piirab küberrünnakute levikut ja hoiab ära võimaliku kahju, piirab juurdepääsu

juhtimissüsteemidele, tuvastab ja takistab sissetungijaid ning võimaldab juhtimissüsteemidele kohandatud juurdepääsu.

ELi küberjulgeoleku seadus parandab küberjulgeolekut kogu ELis ja kehtestab eeskirjad toodete ja teenuste turvalisuse sertifitseerimiseks. Digitaalsete energiasüsteemide turvalisuse tagamine on üliioluline. See hõlmab järgmist:

- **Küberfüüsilised süsteemid:** füüsilist infrastruktuuri digitaalselt haldavate süsteemide kaitsmine küberrünnakute eest, mis võivad avaldada reaalset mõju.
- **Ohutusstandardid:** ELi ohutusstandardite järgimine digitaalseadmete ja energiasüsteemide puhul, et tagada nende ohutu kasutamine ja hooldus.



Isikuandmete kaitse üldmäärus (GDPR) annab teile konkreetsed õigused seoses teie isikuandmetega, sealhulgas energiaandmetega. Need õigused seoses teie isikuandmetega hõlmavad järgmist:

- **Juurdepääsuõigus:** võite oma teenusepakkujalt taotleda oma energiaandmete koopia.
- **Õigus andmete parandamisele:** võite taotleda ebatäpsete või puuduvate andmete parandamist või ajakohastamist.
- **Õigus andmete kustutamisele:** teatud tingimustel võite taotleda oma andmete kustutamist.
- **Õigus piirata töötlemist:** võite piirata oma andmete kasutamist.
- **Õigus andmete ülekantavusele:** võite saada oma andmed ülekantavas formaadis.

Energiaalase privaatsuse, ohutuse ja turvalisuse parandamine

Kuna energia digitaliseerimine ja digitaaltehnoloogiate kasutamine energia tarbimise ja tootmise haldamiseks muutuvad üha tavalisemaks, on siin mõned näpunäited, mis aitavad teil parandada oma energia privaatsust, ohutust ja turvalisust.

- **Turvake oma nutiseadmed:** kasutage tugevaid paroole, võtke kasutusele kaheastmeline autentimine ja hoidke tarkvara ajakohasena.
- **Kaitse oma võrku:** turva oma Wi-Fi-võrk, vältä tundlike tegevuste jaoks avalikku Wi-Fi-võrku ja kaalu tulemüüri kasutamist.
- **Kontrollige oma andmeid:** lugege hoolikalt läbi privaatsuspoliitika, kasutage oma GDPR-õigusi ja loobuge andmete jagamisest, kui see teile ei sobi.

Digitaalne energiamaastik areneb pidevalt, uued tehnoloogiad ja ohud tekivad regulaarselt. Nende suundumustega kursis olemine on oluline teie privaatsuse, ohutuse ja turvalisuse tagamiseks.

Siin on mõned näited uutest tehnoloogiatest, mis mängivad või võivad tulevikus mängida keskset rolli energia digitaliseerimisel:

- **Blockchain-tehnoloogia:** Blockchain, detsentraliseeritud raamatupidamistehnoloogia, võib revolutsiooniliselt muuta energiaandmete haldamist, pakkudes turvalist, läbipaistvat ja võltsimiskindlat viisi andmete jälgimiseks ja jagamiseks.
- **Tehisintellekt (AI) ja masinõpe (ML):** AI ja ML algoritme saab kasutada energiaandmete analüüsimiseks, kõrvalekallete avastamiseks ja potentsiaalsete turvaohtude ennustamiseks, parandades energia süsteemide üldist turvalisust.
- **Kvantarvutid:** Kuigi kvantarvutid on veel algusjärgus, on neil potentsiaal häirida olemasolevaid krüpteerimismeetodeid, mis kujutab endast uut väljakutset andmete turvalisusele energiasektoris.

Kokkuvõte

Energiasektori digitaalne transformatsioon pakub suuri võimalusi jätkusuutlikuma, tõhusama ja kliendikeskse energia süsteemi loomiseks. Selle ülemineku eelised saavad aga täielikult realiseeruda ainult siis, kui tegeleme aktiivselt ja järjepidevalt energia privaatsuse, ohutuse ja turvalisuse väljakutsetega.

Energiatarbijatena on meil oluline roll turvalise digitaalse energia tuleviku kujundamisel. Mõistes oma õigusi GDPR-i alusel, võttes ennetavaid meetmeid oma andmete kaitsmiseks ja valides energia- ja teenusepakkujaid, kes seavad esikohale privaatsuse ja turvalisuse, saame tagada oma isikuandmete kaitse. Lisaks saame end kursis hoides küberjulgeoleku ohtude ja parimate tavadega aidata kaitsta energiainfrastruktuuri, millest me kõik sõltume.

Üleminek digitaalsele energiasüsteemile ei puuduta ainult tehnoloogiat, vaid ka üksikisikute ja kogukondade võimestamist aktiivselt osalema digitaalses energiaüleminekus. Digitaalsete vahendite kasutuselevõtu ja teadlike valikute tegemisega saame anda oma panuse puhtama, usaldusväärsema ja õiglasema energia tuleviku loomisesse.

Lisateave

- Loe lisateavet oma õiguste kohta ELi andmekaitse-eeskirjade alusel artiklist *„Millised on minu õigused?* 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
- Lisateave ELi küberjulgeoleku seaduse ja selle kohta, kuidas see teid kaitseb, leiate aadressilt https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
- Tutvuge andmekaitse mõju hindamisega (DPIA) arukate võrkude ja arukate arvestite kohta. https://energy.ec.europa.eu/topics/markets-and-consumers/smart-grids-and-

meters/data-protection-impact-assessment-smart-grid-and-smart-metering-environment_en

- Lisateave selle kohta, kuidas Euroopa Komisjon meid kaitseb, leiate artiklist *„Kriitiline infrastruktuur ja küberturvalisus”.* https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en

Tänud

„Privaatsus, ohutus ja turvalisus digitaalses energiamaastikus” on kohandatud versioon Rahvusvahelise Energiaagentuuri (IEA) valitud materjalidest (IEA) „Andmekaitse digitaalse energia ajastul” https://www.iea.org/reports/digitalisation-and-energy ja „Kübervastupidavuse suurendamine elektrisüsteemides” https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems (edaspidi „originaalteosed”), mis on mõlemad litsentsitud CC BY 4.0. Käesoleva kohanduse on koostanud ja avaldanud Every1 Project (edaspidi „kohandaja”) ning see on litsentsitud CC BY 4.0, kui ei ole märgitud teisiti. Käesolev teos on Every1 projekti poolt IEA materjalist tuletatud teos ning Every1 projekt vastutab täielikult käesoleva tuletatud teose eest. Tuletatud teost ei toeta IEA mingil viisil.

Adapter muutis originaalteoseid järgmistes aspektides:

- Kohandamine keskendub eelkõige originaalteoste energiaalase privaatsuse, ohutuse ja turvalisuse aspektidele.
- Tehnilist keelt on lihtsustatud, et see oleks arusaadav laiemale lugejaskonnale.
- Lisatud on praktilised näpunäited.
- Lisatud on Euroopa Komisjoni allikatest pärinev uus teave, mis hõlmab isikuandmete kaitse üldmäärust (GDPR) ja ELi küberjulgeoleku seadust.

Pildi autorid

Kursuse peamine pilt: Untitled, autor Mike Fritcher, litsentsitud CC BY-SA 2.0.
Sissejuhatus: Gaili pilt „Naine kasutab Windows Mobile'i seadet pargis koos lapsega” on litsentsitud CC BY-ND 2.0.
Digitaaltehnoloogiad ja digitaalne energiaüleminek: Patrik Tschudini nutikas arvesti „Echelon” on litsentsitud CC BY 2.0.
Küberjulgeolek energeetikasektoris: Michael Coghlan „Mobile Worker” on litsentsitud CC BY-SA 2.0.
Energia privaatsuse, ohutuse ja turvalisuse parandamine: andmed, autor Arismendy Polanco, jagatakse Public Domain Mark 1.0 alusel.