Privacy, veiligheid en beveiliging in het digitale energielandschap

Hoe deze cursus werkt

Deze korte cursus van 30 minuten legt uit wat privacy, veiligheid en beveiliging betekenen in de context van energiedigitalisering. De cursus gaat ook in op bezorgdheden over het gebruik van slimme energietechnologieën.

Misschien bent u:

- Geïnteresseerd in het gebruik van slimme technologieën om meer inzicht te krijgen in uw energieverbruik, maar onzeker over hoe u uw persoonlijke gegevens kunt beveiligen.
- Benieuwd naar hoe uw persoonlijke gegevens worden gebruikt en gedeeld bij het gebruik van digitale technologieën.
- Op zoek naar meer inzicht in privacy, veiligheid en beveiliging in de context van energiedigitalisering.

Deze cursus zal uw begrip van de digitale energietransitie verdiepen en u ondersteunen bij uw eigen digitale energietraject! De cursus maakt deel uit van een reeks van 12 cursussen genaamd *Digital Energy Essentials* (Essentiële elementen van digitale energie), ontwikkeld door het Every1-project, dat tot doel heeft iedereen in staat te stellen en te stimuleren om deel te nemen aan de energietransitie. Meer informatie over het project vindt u op: https://every1.energy

Aan het einde van de cursus stellen we u enkele aanvullende leermaterialen voor. Deze omvatten de cursus *What is the Digital Energy Transition? (Wat is de digitale energietransitie?)*, waarin wordt onderzocht wat digitale energie is en waarom we onze energieproductie en -consumptie digitaliseren.

Dit is een vertaling van de originele Engelstalige versie van de cursus, die de mogelijkheid biedt om een korte quiz te maken en een Every1 digitale badge te verdienen.

Dit project heeft financiering ontvangen uit het Horizon-programma voor onderzoek en innovatie (2021-2027) van de Europese Unie in het kader van subsidieovereenkomst nr. 101075596. De inhoud van deze cursus valt uitsluitend onder de verantwoordelijkheid van het Every1-project en geeft niet noodzakelijkerwijs de mening van de Europese Unie weer.

Leerresultaten

Na het volgen van deze korte cursus kunt u:

- Onderscheid maken tussen privacy, veiligheid en beveiliging bij de digitalisering van energie.
- De belangrijkste uitdagingen begrijpen bij het waarborgen van privacy, veiligheid en beveiliging bij het gebruik van digitale technologieën voor energie.

- U bewust zijn van uw rechten onder de Algemene Verordening Gegevensbescherming (AVG) met betrekking tot energiegegevens.
- Praktisch advies toe te passen om uw gegevens te beschermen en uw digitale energiebeveiliging te verbeteren.

Inleiding

Nu digitale technologieën een integraal onderdeel van ons leven worden, worden privacy, veiligheid en beveiliging van onze persoonlijke gegevens in de context van energiedigitalisering steeds belangrijker.

Slimme meters, mobiele apps en andere digitale apparaten verzamelen en delen gegevens om de energie-efficiëntie te verbeteren, maar dit kan ook vragen oproepen over gegevensprivacy en -beveiliging.
Voordat we beginnen, gaan we eerst eens nader bekijken wat we bedoelen met gegevensprivacy, veiligheid en beveiliging. Dit zijn onderling verbonden, maar toch verschillende begrippen:

- **Privacy** heeft betrekking op de bescherming van persoonlijke informatie.
- **Veiligheid** houdt in dat het gebruik van digitale technologieën geen fysieke of psychologische schade veroorzaakt.
- **Beveiliging** richt zich op het beschermen van gegevens tegen ongeoorloofde toegang of aanvallen.

In deze cursus kijken we niet alleen naar verschillende uitdagingen voor onze energieprivacy, veiligheid en beveiliging, maar ook naar maatregelen die u kunt nemen om uzelf te beschermen. We kijken ook naar hoe overheden en energieleveranciers u en uw gegevens beschermen, evenals de infrastructuur die het gebruik van digitale technologieën voor energieproductie en -verbruik mogelijk maakt.

Digitale technologieën en de digitale energietransitie

Zoals u wellicht hebt gezien in de cursus *Slimme apparaten en digitale energietechnologie*, waarin verschillende soorten slimme apparaten dieper worden onderzocht, zijn er verschillende digitale technologieën die de digitalisering van energie ondersteunen.

Het digitale energielandschap is een complex ecosysteem van onderling verbonden technologieën en belanghebbenden. De belangrijkste componenten zijn:

- **Slimme meters:** apparaten die automatisch gegevens over energieverbruik verzamelen en doorsturen naar energieleveranciers. Slimme meters zorgen voor een nauwkeurigere facturering, inzicht in verbruikspatronen en de mogelijkheid om deel

te nemen aan vraagresponsprogramma's, waarbij u uw energieverbruik kunt aanpassen op basis van vraag- en prijssignalen.

- **Slimme netwerken:** gemoderniseerde elektriciteitsnetwerken die digitale technologieën gebruiken om de stroom van elektriciteit te monitoren en te regelen. Ze maken tweerichtingscommunicatie mogelijk tussen het nutsbedrijf en de consument, waardoor realtime monitoring van het energieverbruik en de integratie van hernieuwbare energiebronnen mogelijk wordt.
- **Internet of Things (IoT) in energie:** netwerk van verbonden apparaten (thermostaten, apparaten, EV-laders) die gegevens verzamelen en uitwisselen, waardoor energieverbruik op afstand kan worden geregeld en geoptimaliseerd.

Gegevens over energie kunnen onder meer verbruikspatronen, gegevens over het tijdstip van gebruik, details op apparaatniveau en zelfs gedragsgegevens zijn die uit het gebruik worden afgeleid. Deze gegevens kunnen u helpen inzicht te krijgen in uw eigen energieverbruik, mogelijk geld te besparen en weloverwogen keuzes te maken. Ze kunnen ook energieleveranciers (zoals uw elektriciteitsleverancier) helpen om het netwerk te optimaliseren, u gepersonaliseerde diensten aan te bieden en fraude op te sporen.

Uw energiegegevens worden doorgaans verzameld door uw energieleverancier, maar kunnen ook worden gedeeld met of geraadpleegd door meterbeheerders, gegevensverzamelaars, externe dienstverleners en mogelijk overheidsinstanties. Energiegegevens zijn nuttig voor beleidsmakers, bijvoorbeeld door de ontwikkeling van effectief energiebeleid en regelgeving te ondersteunen.

Gegevens over energieverbruik kunnen gevoelige informatie bevatten. Aangezien verschillende organisaties toegang kunnen hebben tot uw gegevens en deze op verschillende manieren kunnen gebruiken, kan dit aanleiding geven tot bezorgdheid. Later in de cursus zullen we enkele manieren voorstellen om uw energieprivacy, veiligheid en beveiliging te verbeteren. Laten we eerst eens kijken naar enkele veelvoorkomende cyberdreigingen en wat er wordt gedaan om de veiligheid van digitale systemen te waarborgen.

Cyberbeveiliging in de energiesector

Door de digitale transformatie van de energiesector is deze sector een doelwit geworden voor cyberaanvallen, die de energievoorziening kunnen verstoren en gevoelige informatie in gevaar kunnen brengen. Veelvoorkomende cyberdreigingen zijn onder meer:

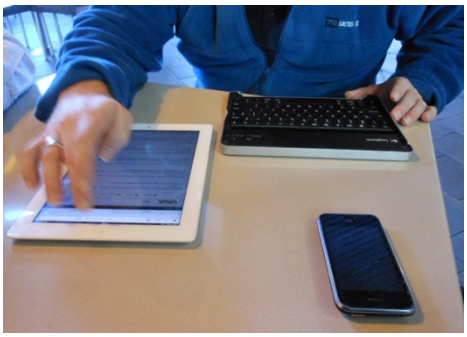
- **Malware** (kwaadaardige software die computersystemen en gegevens kan beschadigen).

- **Ransomware** (een type kwaadaardige software die uw bestanden versleutelt, waardoor ze ontoegankelijk worden, en losgeld eist om de toegang te herstellen).
- **Denial-of-service-aanvallen** (deze aanvallen zijn bedoeld om een systeem of netwerk te overbelasten met verkeer, waardoor het niet meer beschikbaar is voor legitieme gebruikers).
- **Phishing-scams** (frauduleuze pogingen om gevoelige informatie, zoals wachtwoorden of creditcardgegevens, te verkrijgen door zich voor te doen als een betrouwbare entiteit).

Om kritieke infrastructuur te beschermen zijn maatregelen nodig zoals netwerksegmentatie, waarbij een groter netwerk wordt opgedeeld in kleinere, geïsoleerde segmenten. Dit beperkt de verspreiding van cyberaanvallen en beperkt de potentiële schade, beperkt de toegang tot controles, detecteert en voorkomt indringers en maakt aangepaste toegang tot controles mogelijk.

De EU-cyberbeveiligingswet verbetert de cyberbeveiliging in de hele EU en stelt regels vast voor het certificeren van de veiligheid van producten en diensten. Het waarborgen van de veiligheid van digitale energiesystemen is van cruciaal belang. Dit omvat:

- **Cyberfysieke systemen:** het beschermen van deze systemen, waarbij fysieke infrastructuur digitaal wordt beheerd, tegen cyberaanvallen die gevolgen kunnen hebben in de echte wereld.
- **Veiligheidsnormen:** het naleven van EU-veiligheidsnormen voor digitale apparaten en energiesystemen om veilig gebruik en onderhoud ervan te garanderen.



De Algemene Verordening Gegevensbescherming (AVG) geeft u specifieke rechten met betrekking tot uw persoonsgegevens, waaronder energiegegevens. Deze rechten met betrekking tot uw persoonsgegevens omvatten:

- **Recht op toegang:** u kunt een kopie van uw energiegegevens opvragen bij uw leverancier.
- **Recht op rectificatie:** u kunt verzoeken om onjuiste of ontbrekende gegevens te corrigeren of bij te werken.
- **Recht op verwijdering:** u kunt onder bepaalde omstandigheden verzoeken om verwijdering van uw gegevens.
- **Recht op beperking van de verwerking:** u kunt het gebruik van uw gegevens beperken.
- **Recht op gegevensoverdraagbaarheid:** u kunt uw gegevens in een overdraagbaar formaat ontvangen.

Verbetering van uw energieprivacy, veiligheid en beveiliging

Nu de digitalisering van energie en het gebruik van digitale technologieën voor het beheer van ons energieverbruik en onze energieproductie steeds gangbaarder worden, volgen hier enkele tips om uw privacy, veiligheid en beveiliging op energiegebied te verbeteren.

- **Beveilig uw slimme apparaten:** gebruik sterke wachtwoorden, schakel tweefactorauthenticatie in en houd uw software up-to-date.
- **Bescherm uw netwerk:** beveilig uw wifi-netwerk, vermijd openbare wifi voor gevoelige activiteiten en overweeg het gebruik van een firewall.
- **Beheer uw gegevens:** lees het privacybeleid zorgvuldig door, maak gebruik van uw GDPR-rechten en meld u af voor het delen van gegevens als u zich daar niet prettig bij voelt.

Het digitale energielandschap is voortdurend in ontwikkeling, met regelmatig nieuwe technologieën en bedreigingen. Het is belangrijk om op de hoogte te blijven van deze trends om uw privacy, veiligheid en beveiliging te waarborgen.

Hier volgen enkele voorbeelden van nieuwe technologieën die nu of in de toekomst een centralere rol kunnen spelen in de digitalisering van energie:

- **Blockchaintechnologie:** Blockchain, een gedecentraliseerde grootboektechnologie, heeft het potentieel om het beheer van energiegegevens radicaal te veranderen door een veilige, transparante en fraudebestendige manier te bieden om gegevens bij te houden en te delen.
- **Kunstmatige intelligentie (AI) en machine learning (ML):** AI- en ML-algoritmen kunnen worden gebruikt om energiegegevens te analyseren, afwijkingen op te sporen en potentiële veiligheidsrisico's te voorspellen, waardoor de algehele veiligheid van energiesystemen wordt verbeterd.
- **Kwantumcomputing:** Hoewel kwantumcomputing nog in de kinderschoenen staat, heeft het de potentie om bestaande encryptiemethoden te ontwrichten, wat een nieuwe uitdaging vormt voor de gegevensbeveiliging in de energiesector.

Conclusie

De digitale transformatie van de energiesector biedt enorme mogelijkheden voor een duurzamer, efficiënter en klantgerichter energiesysteem. De voordelen van deze transitie kunnen echter alleen volledig worden gerealiseerd als we ons actief en continu bezighouden met de uitdagingen op het gebied van energieprivacy, veiligheid en beveiliging.

Als energieverbruikers spelen we een cruciale rol in het vormgeven van een veilige digitale energietoekomst. Door onze rechten onder de AVG te begrijpen, proactieve maatregelen te

nemen om onze gegevens te beschermen en energieleveranciers en dienstverleners te kiezen die privacy en veiligheid hoog in het vaandel hebben staan, kunnen we ervoor zorgen dat onze persoonlijke gegevens beschermd blijven. Bovendien kunnen we, door op de hoogte te blijven van cyberbeveiligingsrisico's en best practices, helpen de energie-infrastructuur te beschermen waar we allemaal op vertrouwen.

De overgang naar een digitaal energiesysteem gaat niet alleen over technologie, maar ook over het in staat stellen van individuen en gemeenschappen om actief deel te nemen aan de digitale energietransitie. Door digitale hulpmiddelen te omarmen en weloverwogen keuzes te maken, kunnen we bijdragen aan een schonere, betrouwbaardere en rechtvaardigere energietoekomst.

Aanvullende bronnen

- Lees meer over uw rechten onder de EU-regels voor gegevensbescherming in *Wat zijn mijn rechten?* 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
- Lees meer over de EU-cyberbeveiligingswet en hoe deze u beschermt https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
- Bekijk een gegevensbeschermingseffectbeoordeling (DPIA) voor slimme netwerken en slimme meters. https://energy.ec.europa.eu/topics/markets-and-consumers/smart-grids-and-meters/data-protection-impact-assessment-smart-grid-and-smart-metering-environment_en
- Lees meer over hoe de Europese Commissie ons beschermt in dit artikel over *kritieke infrastructuur en cyberbeveiliging.* https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en

Dankwoord

Privacy, veiligheid en beveiliging in het digitale energielandschap is een bewerking van geselecteerd materiaal uit de rapporten van het Internationaal Energieagentschap (IEA) (IEA) "Data Privacy in the Digital Energy Era" https://www.iea.org/reports/digitalisation-and-energy en "Enhancing cyber resilience in electricity systems" https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems, (de 'originele werken'), die beide onder licentie CC BY 4.0 vallen. Deze bewerking is gemaakt en gepubliceerd door het Every1 Project (de 'bewerker') en valt onder de licentie CC BY 4.0, tenzij anders vermeld. Dit is een werk dat door het Every1-project is afgeleid van IEA-materiaal en het Every1-project is als enige aansprakelijk en verantwoordelijk voor dit afgeleide werk. Het afgeleide werk wordt op geen enkele wijze door het IEA onderschreven.

De bewerker heeft het oorspronkelijke werk op de volgende punten gewijzigd:

- De aanpassing richt zich specifiek op de aspecten energieprivacy, veiligheid en beveiliging van de originele werken.
- De technische taal is vereenvoudigd voor een algemeen publiek.
- Er zijn praktische tips toegevoegd.
- Er is nieuwe informatie uit bronnen van de Europese Commissie opgenomen om de AVG en de EU-cyberbeveiligingswet te behandelen.

Afbeeldingen

Hoofdafbeelding van de cursus: Untitled door Mike Fritcher is gelicentieerd onder CC BY-SA 2.0.
Inleiding: Vrouw die Windows Mobile-apparaat gebruikt in park met kind door Gail is gelicentieerd onder CC BY-ND 2.0.
Digitale technologieën en de digitale energietransitie: Slimme meter "Echelon" door Patrik Tschudin is gelicentieerd onder CC BY 2.0.
Cyberbeveiliging in de energiesector: Mobiele werknemer door Michael Coghlan is gelicentieerd onder CC BY-SA 2.0.
Verbetering van uw energieprivacy, veiligheid en beveiliging: gegevens door Arismendy Polanco wordt gedeeld onder een Public Domain Mark 1.0.