EVERY1

Finansowane przez Unię Europejską

Prywatność, bezpieczeństwo i ochrona w cyfrowym świecie energii

Jak działa ten kurs

Ten krótki, 30-minutowy kurs wyjaśnia, co oznaczają prywatność, bezpieczeństwo i ochrona w kontekście cyfryzacji energetyki. Kurs porusza również kwestie związane z obawami dotyczącymi stosowania inteligentnych technologii energetycznych.

Być może:

- Jesteś zainteresowany wykorzystaniem inteligentnych technologii w celu lepszego zrozumienia swojego zużycia energii, ale nie masz pewności, jak zabezpieczyć swoje dane osobowe.
- Jesteś ciekawy, w jaki sposób Twoje dane osobowe są wykorzystywane i udostępniane podczas korzystania z technologii cyfrowych.
- Chcesz lepiej zrozumieć kwestie prywatności, bezpieczeństwa i ochrony w kontekście cyfryzacji energetyki.

Ten kurs pogłębi Twoją wiedzę na temat cyfrowej transformacji energetycznej i wesprze Cię w Twojej cyfrowej podróży energetycznej! Jest on częścią zestawu 12 kursów o nazwie *„Digital Energy Essentials”* (*Podstawy cyfrowej energii*), opracowanego w ramach projektu Every1, którego celem jest umożliwienie i wzmocnienie zaangażowania wszystkich w transformację energetyczną. Więcej informacji na temat projektu można znaleźć na stronie: https://every1.energy

Na koniec kursu proponujemy kilka dodatkowych materiałów edukacyjnych do zapoznania się. Obejmują one kurs *„Czym jest cyfrowa transformacja energetyczna?”*, który wyjaśnia, czym jest cyfrowa energia i jakie są powody przejścia na cyfryzację produkcji i zużycia energii.

Jest to tłumaczenie oryginalnej angielskiej wersji kursu, który obejmuje możliwość wypełnienia krótkiego quizu i zdobycia cyfrowej odznaki Every1.

Projekt ten otrzymał dofinansowanie z programu Unii Europejskiej „Horyzont” na rzecz badań naukowych i innowacji (2021–2027) w ramach umowy o dotację nr 101075596. Wyłączną odpowiedzialność za treść tego kursu ponosi projekt Every1 i niekoniecznie odzwierciedla on opinię Unii Europejskiej.

Efekty uczenia się

Po ukończeniu tego krótkiego kursu uczestnicy powinni umieć:

- Rozróżniać prywatność, bezpieczeństwo i ochronę w cyfryzacji energii.
- Zrozumieć główne wyzwania związane z zapewnieniem prywatności, bezpieczeństwa i ochrony podczas korzystania z technologii cyfrowych w energetyce.
- Być świadomym swoich praw wynikających z ogólnego rozporządzenia o ochronie danych (RODO) w odniesieniu do danych dotyczących energii.

- Stosować praktyczne porady dotyczące ochrony danych i zwiększania bezpieczeństwa cyfrowego w energetyce.

Wprowadzenie

W miarę jak technologie cyfrowe stają się integralną częścią naszego życia, prywatność, bezpieczeństwo i ochrona naszych danych osobowych w kontekście cyfryzacji energetyki stają się coraz ważniejsze.

Inteligentne liczniki, aplikacje mobilne i inne urządzenia cyfrowe gromadzą i udostępniają dane w celu zwiększenia efektywności energetycznej, ale może to również budzić obawy dotyczące prywatności i bezpieczeństwa danych.
Zanim zaczniemy, przyjrzyjmy się bliżej, co rozumiemy przez prywatność, bezpieczeństwo i ochronę danych. Są to pojęcia powiązane, ale odrębne:

- **Prywatność** odnosi się do ochrony danych osobowych.
- **Bezpieczeństwo** polega na zapewnieniu, że korzystanie z technologii cyfrowych nie powoduje szkód fizycznych ani psychicznych.
- **Ochrona** koncentruje się na ochronie danych przed nieuprawnionym dostępem lub atakami.

W tym kursie przyjrzymy się nie tylko różnym wyzwaniom związanym z prywatnością, bezpieczeństwem i ochroną naszych danych energetycznych, ale także działaniom, które można podjąć, aby się chronić. Przyjrzymy się również, w jaki sposób rządy i dostawcy energii chronią Ciebie i Twoje dane, a także infrastrukturę, która umożliwia wykorzystanie technologii cyfrowych do produkcji i zużycia energii.

Technologie cyfrowe i cyfrowa transformacja energetyczna

Jak można było zobaczyć w kursie *„Inteligentne urządzenia i cyfrowe technologie energetyczne”*, który bardziej szczegółowo omawia różne rodzaje inteligentnych urządzeń, istnieje szereg technologii cyfrowych, które wspierają cyfryzację energii.

Cyfrowy krajobraz energetyczny to złożony ekosystem połączonych ze sobą technologii i interesariuszy. Kluczowe elementy to:

- **Inteligentne liczniki:** urządzenia, które automatycznie gromadzą i przekazują dane dotyczące zużycia energii do dostawców energii. Inteligentne liczniki zapewniają dokładniejsze rozliczenia, wgląd w wzorce zużycia oraz możliwość uczestnictwa w programach reagowania na zapotrzebowanie, w ramach których można dostosować zużycie energii w oparciu o sygnały dotyczące zapotrzebowania i cen.
- **Inteligentne sieci energetyczne:** zmodernizowane sieci elektryczne, które wykorzystują technologie cyfrowe do monitorowania i kontrolowania przepływu

energii elektrycznej. Umożliwiają one dwukierunkową komunikację między dostawcą energii a konsumentem, co pozwala na monitorowanie zużycia energii w czasie rzeczywistym oraz integrację odnawialnych źródeł energii.

- **Internet rzeczy (IoT) w energetyce:** sieć połączonych urządzeń (termostaty, urządzenia gospodarstwa domowego, ładowarki pojazdów elektrycznych), które gromadzą i wymieniają dane, umożliwiając zdalne sterowanie i optymalizację zużycia energii.

Dane dotyczące energii mogą obejmować wzorce zużycia, dane dotyczące czasu użytkowania, szczegóły dotyczące urządzeń, a nawet dane behawioralne wywnioskowane na podstawie zużycia. Dane te mogą pomóc w zrozumieniu własnego zużycia energii, potencjalnie zaoszczędzić pieniądze i dokonywać świadomych wyborów. Mogą one również pomóc dostawcom energii (takim jak dostawca energii elektrycznej) w optymalizacji sieci, oferowaniu spersonalizowanych usług i wykrywaniu oszustw.

Dane dotyczące energii są zazwyczaj gromadzone przez dostawcę energii, ale mogą być również udostępniane lub wykorzystywane przez operatorów liczników, agregatorów danych, zewnętrznych dostawców usług, a potencjalnie także agencje rządowe. Dane dotyczące energii są przydatne dla decydentów, na przykład poprzez wspieranie opracowywania skutecznych polityk i regulacji w zakresie energii.

Dane dotyczące zużycia energii mogą zawierać informacje wrażliwe. Ponieważ dostęp do danych użytkownika może mieć wiele różnych organizacji, które mogą je wykorzystywać na różne sposoby, może to budzić obawy. W dalszej części kursu zaproponujemy kilka sposobów na zwiększenie prywatności, bezpieczeństwa i ochrony energii. Najpierw przyjrzyjmy się niektórym typowym zagrożeniom cybernetycznym i działaniom podejmowanym w celu zapewnienia bezpieczeństwa systemów cyfrowych.

Cyberbezpieczeństwo w sektorze energetycznym

Cyfrowa transformacja sektora energetycznego sprawiła, że stał się on celem cyberataków, które mogą zakłócić dostawy energii i narazić poufne informacje. Typowe cyberzagrożenia obejmują:

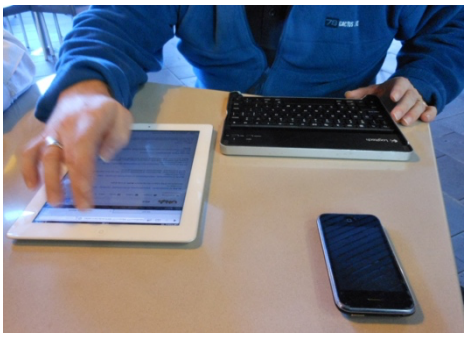
- **Złośliwe oprogramowanie** (złośliwe oprogramowanie, które może uszkodzić systemy komputerowe i dane).
- **Oprogramowanie ransomware** (rodzaj złośliwego oprogramowania, które szyfruje pliki, uniemożliwiając dostęp do nich, i żąda okupu za przywrócenie dostępu).
- **Ataki typu „odmowa usługi”** (ataki te mają na celu przeciążenie systemu lub sieci ruchem, uniemożliwiając dostęp legalnym użytkownikom).

- **Oszustwa phishingowe** (nieuczciwe próby uzyskania poufnych informacji, takich jak hasła lub dane kart kredytowych, poprzez podszywanie się pod godną zaufania jednostkę).

Ochrona infrastruktury krytycznej wymaga takich środków, jak segmentacja sieci, czyli podział większej sieci na mniejsze, izolowane segmenty. Ogranicza to rozprzestrzenianie się cyberataków i powstrzymuje potencjalne szkody, ogranicza dostęp do elementów sterujących, wykrywa i zapobiega wtargnięciom oraz umożliwia dostosowany do potrzeb dostęp do elementów sterujących.

Unijna ustawa o cyberbezpieczeństwie wzmacnia cyberbezpieczeństwo w całej UE i ustanawia zasady certyfikacji bezpieczeństwa produktów i usług. Zapewnienie bezpieczeństwa cyfrowych systemów energetycznych ma kluczowe znaczenie. Obejmuje to:

- **Systemy cyberfizyczne:** Ochronę tych systemów, w których infrastruktura fizyczna jest zarządzana cyfrowo, przed cyberatakami, które mogą mieć realne konsekwencje.
- **Normy bezpieczeństwa:** przestrzeganie norm bezpieczeństwa UE dotyczących urządzeń cyfrowych i systemów energetycznych w celu zapewnienia ich bezpiecznego użytkowania i konserwacji.



Ogólne rozporządzenie o ochronie danych (RODO) przyznaje użytkownikom określone prawa dotyczące ich danych osobowych, w tym danych dotyczących energii. Prawa te obejmują:

- **Prawo dostępu:** możesz zażądać od dostawcy kopii swoich danych dotyczących energii.
- **Prawo do sprostowania:** Możesz zażądać poprawienia lub aktualizacji wszelkich nieprawidłowych lub brakujących danych.
- **Prawo do usunięcia:** Możesz zażądać usunięcia swoich danych w określonych okolicznościach.
- **Prawo do ograniczenia przetwarzania:** użytkownik może ograniczyć sposób wykorzystania swoich danych.
- **Prawo do przenoszenia danych:** możesz otrzymać swoje dane w formacie umożliwiającym ich przenoszenie.

Zwiększanie prywatności, bezpieczeństwa i ochrony energii

Wraz z upowszechnianiem się cyfryzacji energetyki i wykorzystaniem technologii cyfrowych do zarządzania zużyciem i produkcją energii, poniżej przedstawiamy kilka wskazówek, które pomogą Ci zwiększyć prywatność, bezpieczeństwo i ochronę w zakresie energii.

- **Zabezpiecz swoje urządzenia inteligentne:** używaj silnych haseł, włącz uwierzytelnianie dwuskładnikowe i aktualizuj oprogramowanie.
- **Chroń swoją sieć:** zabezpiecz swoją sieć Wi-Fi, unikaj publicznych sieci Wi-Fi podczas wykonywania wrażliwych czynności i rozważ użycie zapory sieciowej.

- **Kontroluj swoje dane:** dokładnie zapoznaj się z polityką prywatności, korzystaj z praw wynikających z RODO i zrezygnuj z udostępniania danych, jeśli czujesz się z tym niekomfortowo.

Cyfrowy krajobraz energetyczny nieustannie się zmienia, a nowe technologie i zagrożenia pojawiają się regularnie. Aby zapewnić sobie prywatność, bezpieczeństwo i ochronę, ważne jest, aby być na bieżąco z tymi trendami.

Oto kilka przykładów nowych technologii, które obecnie lub w przyszłości mogą odgrywać bardziej centralną rolę w cyfryzacji energetyki:

- **Technologia blockchain:** Blockchain, zdecentralizowana technologia rejestru transakcji, ma potencjał, aby zrewolucjonizować zarządzanie danymi energetycznymi, zapewniając bezpieczny, przejrzysty i odporny na manipulacje sposób śledzenia i udostępniania danych.
- **Sztuczna inteligencja (AI) i uczenie maszynowe (ML):** Algorytmy AI i ML mogą być wykorzystywane do analizy danych energetycznych, wykrywania anomalii i przewidywania potencjalnych zagrożeń bezpieczeństwa, zwiększając ogólne bezpieczeństwo systemów energetycznych.
- **Obliczenia kwantowe:** Chociaż obliczania kwantowe są nadal w początkowej fazie rozwoju, mają one potencjał, aby zrewolucjonizować istniejące metody szyfrowania, stwarzając nowe wyzwanie dla bezpieczeństwa danych w sektorze energetycznym.

Wniosek

Cyfrowa transformacja sektora energetycznego niesie ze sobą ogromne nadzieje na bardziej zrównoważony, wydajny i zorientowany na klienta system energetyczny. Jednak korzyści płynące z tej transformacji można w pełni wykorzystać tylko wtedy, gdy aktywnie i nieustannie angażujemy się w rozwiązywanie problemów związanych z prywatnością, bezpieczeństwem i ochroną energii.

Jako konsumenci energii mamy do odegrania istotną rolę w kształtowaniu bezpiecznej cyfrowej przyszłości energetycznej. Rozumiejąc nasze prawa wynikające z RODO, podejmując proaktywne działania w celu ochrony naszych danych oraz wybierając dostawców energii i usługodawców, którzy priorytetowo traktują prywatność i bezpieczeństwo, możemy zapewnić ochronę naszych danych osobowych. Ponadto, pozostając na bieżąco z zagrożeniami dla cyberbezpieczeństwa i najlepszymi praktykami, możemy pomóc chronić infrastrukturę energetyczną, z której wszyscy korzystamy.

Przejście na cyfrowy system energetyczny nie dotyczy tylko technologii, ale także umożliwienia osobom i społecznościom aktywnego udziału w cyfrowej transformacji energetycznej. Korzystając z narzędzi cyfrowych i dokonując świadomych wyborów, możemy

przyczynić się do stworzenia czystszej, bardziej niezawodnej i sprawiedliwszej przyszłości energetycznej.

Dodatkowe zasoby

- Więcej informacji na temat praw przysługujących użytkownikom zgodnie z przepisami UE o ochronie danych można znaleźć w sekcji *„Jakie są moje prawa?* 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
- Dowiedz się więcej o unijnej ustawie o cyberbezpieczeństwie i tym, jak chroni ona użytkowników https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
- Zapoznaj się z oceną skutków dla ochrony danych (DPIA) w odniesieniu do inteligentnych sieci i inteligentnych liczników. https://energy.ec.europa.eu/topics/markets-and-consumers/smart-grids-and-meters/data-protection-impact-assessment-smart-grid-and-smart-metering-environment_en
- Dowiedz się więcej o tym, jak Komisja Europejska chroni nas w tym artykule na temat *infrastruktury krytycznej i cyberbezpieczeństwa.* https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en

Podziękowania

Prywatność, bezpieczeństwo i ochrona w cyfrowym świecie energii to adaptacja wybranych materiałów Międzynarodowej Agencji Energetycznej (IEA) „Ochrona danych osobowych w erze cyfrowej energii" https://www.iea.org/reports/digitalisation-and-energy oraz „Zwiększanie cyberodporności systemów elektroenergetycznych" https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems (zwanych dalej „dziełami oryginalnymi"), które są objęte licencją CC BY 4.0. Niniejsza adaptacja została opracowana i opublikowana przez Every1 Project („Adaptator") i jest objęta licencją CC BY 4.0, o ile nie zaznaczono inaczej. Jest to dzieło pochodne projektu Every1 oparte na materiałach IEA, a projekt Every1 ponosi wyłączną odpowiedzialność za to dzieło pochodne. Dzieło pochodne nie jest w żaden sposób popierane przez IEA.

Adapter zmodyfikował oryginalne dzieła w następujących aspektach:

- Adaptacja koncentruje się w szczególności na aspektach oryginalnych dzieł związanych z prywatnością, bezpieczeństwem i ochroną energii.
- Język techniczny został uproszczony dla ogółu odbiorców.
- Dodano praktyczne wskazówki.
- Dodano nowe informacje pochodzące ze źródeł Komisji Europejskiej, dotyczące RODO i unijnej ustawy o cyberbezpieczeństwie.

Źródło zdjęć

Główne zdjęcie kursu: Untitled autorstwa Mike'a Fritchera jest objęte licencją CC BY-SA 2.0.
Wprowadzenie: Kobieta korzystająca z urządzenia z systemem Windows Mobile w parku z dzieckiem autorstwa Gail jest objęte licencją CC BY-ND 2.0.
Technologie cyfrowe i cyfrowa transformacja energetyczna: Inteligentny licznik „Echelon" autorstwa Patrika Tschudina na licencji CC BY 2.0.
Cyberbezpieczeństwo w sektorze energetycznym: Mobile Worker autorstwa Michaela Coghlana na licencji CC BY-SA 2.0.
Zwiększanie prywatności, bezpieczeństwa i ochrony energii: dane autorstwa Arismendy Polanco są udostępniane na licencji Public Domain Mark 1.0.