Adatvédelem, biztonság és védelem a digitális energiaiparban

A kurzus felépítése

Ez a rövid, 30 perces tanfolyam elmagyarázza, mit jelent a magánélet, a biztonság és a védelem az energia digitalizációjának kontextusában. A tanfolyam az intelligens energiatechnológiák használatával kapcsolatos aggályokat is tárgyalja.

Lehet, hogy:

- Érdekli az intelligens technológiák használata az energiafogyasztás jobb megértése érdekében, de nem tudja, hogyan biztosíthatja személyes adatainak biztonságát.
- Kíváncsi arra, hogy személyes adatait hogyan használják és osztják meg a digitális technológiák használata során.
- Szeretné jobban megérteni az adatvédelmet, a biztonságot és a védelmet az energia digitalizációjának kontextusában.

Ez a tanfolyam elmélyíti a digitális energiaátállásról szóló ismereteit, és támogatja saját digitális energiaútját! A tanfolyam az Every1 projekt által kidolgozott, 12 tanfolyamból álló *Digital Energy Essentials* (Digitális energia alapjai) sorozat része, amelynek célja, hogy mindenki részt vehessen az energiaátállásban. A projektről további információkat talál a következő weboldalon: https://every1.energy

A tanfolyam végén további tanulási anyagokat javaslunk Önnek. Ezek között szerepel a *„Mi a digitális energiaátállás?” című* tanfolyam, amely azt vizsgálja, mi is az a digitális energia, és miért érdemes digitalizálni az energiatermelést és -fogyasztást.

Ez a tanfolyam angol nyelvű eredeti változatának fordítása, amely lehetőséget kínál egy rövid kvíz kitöltésére és egy Every1 digitális jelvény megszerzésére.

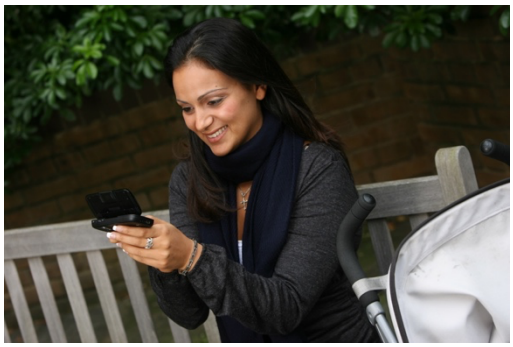
Ez a projekt az Európai Unió Horizont kutatási és innovációs programjának (2021–2027) támogatásában részesült, a 101075596 számú támogatási megállapodás keretében. A tanfolyam tartalmáért kizárólag az Every1 projekt felel, és az nem feltétlenül tükrözi az Európai Unió véleményét.

A tanulás eredményei

A rövid tanfolyam elvégzése után Ön képes lesz:

- Megkülönböztetni a magánélet, a biztonság és a védelem fogalmát az energia digitalizációjában.
- Megérteni a magánélet, a biztonság és a védelem biztosításának főbb kihívásait az energiaiparban alkalmazott digitális technológiák használata során.
- Ismerni az általános adatvédelmi rendelet (GDPR) szerinti jogait az energiaadatokkal kapcsolatban.
- Gyakorlati tanácsokat alkalmazni az adatok védelme és a digitális energiabiztonság javítása érdekében.

Bevezetés



Ahogy a digitális technológiák egyre inkább szerves részévé válnak életünknek, az energia digitalizációja kapcsán egyre fontosabbá válik személyes adataink adatvédelme, biztonsága és védelme.

Az intelligens mérőórák, mobilalkalmazások és egyéb digitális eszközök adatokat gyűjtenek és osztanak meg az energiahatékonyság javítása érdekében, de ez adatvédelmi és biztonsági aggályokat is felvethet.
Mielőtt belekezdenénk, nézzük meg közelebbről, mit értünk adatvédelem, biztonság és védelem alatt. Ezek egymással összefüggő, de egymástól elkülönülő fogalmak:

- **Az adatvédelem** a személyes adatok védelmével kapcsolatos.
- **A biztonság** azt jelenti, hogy a digitális technológiák használata nem okoz fizikai vagy pszichológiai kárt.
- **A biztonság** az adatok jogosulatlan hozzáféréssel vagy támadásokkal szembeni védelmére összpontosít.

Ebben a kurzusban nemcsak az energiaadat-védelem, -biztonság és -biztonság különböző kihívásait vizsgáljuk meg, hanem azokat a lépéseket is, amelyeket Ön tehet a saját védelme érdekében. Megvizsgáljuk azt is, hogy a kormányok és az energiaszolgáltatók hogyan védik Önt és adatait, valamint az energia termelésére és fogyasztására szolgáló digitális technológiák használatát lehetővé tevő infrastruktúrát.

Digitális technológiák és a digitális energiaátállás

Ahogyan azt az intelligens eszközöket *és a digitális energiatechnológiát* részletesebben bemutató *„Intelligens* eszközök *és digitális* energiatechnológia” kurzusban láthattuk, számos digitális technológia támogatja az energia digitalizálását.

A digitális energiaipar összetett ökoszisztéma, amely egymással összekapcsolt technológiákból és érdekelt felekből áll. A legfontosabb elemei a következők:

- **Intelligens mérők:** Az energiafogyasztásra vonatkozó adatokat automatikusan gyűjtő és az energiaszolgáltatóknak továbbító eszközök. Az intelligens mérők pontosabb számlázást, betekintést a fogyasztási szokásokba, valamint lehetőséget nyújtanak a keresletre reagáló programokban való részvételre, ahol a kereslet és az árjelzések alapján lehet szabályozni az energiafogyasztást.
- **Intelligens hálózatok:** Modernizált villamos hálózatok, amelyek digitális technológiákat használnak az áramáramlás figyelemmel kísérésére és szabályozására. Kétirányú kommunikációt tesznek lehetővé a közüzemi szolgáltató és a fogyasztó között, lehetővé téve az energiafogyasztás valós idejű figyelemmel kísérését és a megújuló energiaforrások integrálását.

- **Az internet of things (IoT) az energetikában:** összekapcsolt eszközök (termosztátok, háztartási gépek, elektromos járművek töltői) hálózata, amely adatokat gyűjt és cserél, lehetővé téve az energiafelhasználás távoli vezérlését és optimalizálását.

Az energiával kapcsolatos adatok között szerepelhetnek a fogyasztási minták, a használati időre vonatkozó adatok, a készülékek szintjén megadott részletek, sőt a használatból következtetett viselkedési adatok is. Ezek az adatok segíthetnek megérteni a saját energiafelhasználását, potenciálisan pénzt megtakarítani és tájékozott döntéseket hozni. Emellett segíthetnek az energiaszolgáltatóknak (például az áramszolgáltatónak) a hálózat optimalizálásában, személyre szabott szolgáltatások nyújtásában és a csalások felderítésében.

Az energiaadatokat általában az energiaellátó gyűjti, de azok megoszthatók vagy hozzáférhetők lehetnek a mérőműszer-üzemeltetők, adatgyűjtők, harmadik fél szolgáltatók és potenciálisan kormányzati szervek számára is. Az energiaadatok hasznosak a politikai döntéshozók számára, például a hatékony energiapolitikák és szabályozások kidolgozásának támogatásában.

Az energiafogyasztásra vonatkozó adatok érzékeny információkat is tartalmazhatnak. Mivel számos különböző szervezet férhet hozzá az adatokhoz, és azokat különböző módon használhatja fel, ez aggodalmakat kelthet. A tanfolyam későbbi részében javaslatokat fogunk tenni arra, hogyan javíthatja energiaadatainak magánéletét, biztonságát és védelmét. Először nézzük meg néhány gyakori kiberfenyegetést, és azt, hogy mit tesznek a digitális rendszerek biztonságának biztosítása érdekében.

Kiberbiztonság az energiaszektorban

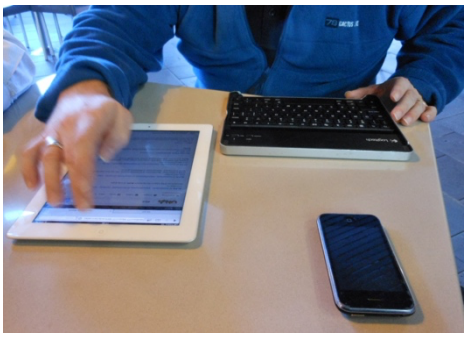
Az energiaágazat digitális átalakulása miatt az ágazat kiberfenyegetések célpontjává vált, amelyek megzavarhatják az energiaellátást és veszélybe sodorhatják az érzékeny információkat. A gyakori kiberfenyegetések közé tartoznak:

- **Malware** (rosszindulatú szoftver, amely károsíthatja a számítógépes rendszereket és az adatokat).
- **Ransomware** (olyan rosszindulatú szoftver, amely titkosítja a fájlokat, így azok hozzáférhetetlenné válnak, és váltságdíjat követel a hozzáférés visszaállításáért).
- **Denial-of-service támadások** (ezek a támadások célja, hogy a forgalommal túlterheljék a rendszert vagy a hálózatot, így azok a jogos felhasználók számára elérhetetlenné válnak).
- **Adathalász csalások** (csalárd kísérletek érzékeny információk, például jelszavak vagy hitelkártyaadatok megszerzésére, megbízható szervezetnek álcázva magukat).

A kritikus infrastruktúra védelme olyan intézkedéseket igényel, mint a hálózati szegmentálás, amely egy nagyobb hálózat kisebb, egymástól elszigetelt szegmensekre való felosztását jelenti. Ez korlátozza a kibertámadások terjedését és visszatartja a potenciális károkat, korlátozza a vezérlőkhöz való hozzáférést, felismeri és megakadályozza a behatolókat, valamint lehetővé teszi a vezérlőkhöz való személyre szabott hozzáférést.

Az EU kiberbiztonsági törvénye javítja a kiberbiztonságot az EU egész területén, és szabályokat állapít meg a termékek és szolgáltatások biztonságának tanúsítására. A digitális energiarendszerek biztonságának biztosítása elengedhetetlen. Ez a következőket foglalja magában:

- **Kiberfizikai rendszerek:** A fizikai infrastruktúrát digitálisan kezelő rendszerek védelme a valós világban következményekkel járó kibertámadásoktól.
- **Biztonsági szabványok:** A digitális eszközökre és energiarendszerekre vonatkozó uniós biztonsági szabványok betartása azok biztonságos használatának és karbantartásának biztosítása érdekében.



Az általános adatvédelmi rendelet (GDPR) konkrét jogokat biztosít Önnek személyes adatai, beleértve az energiaadatokat is, tekintetében. A személyes adataira vonatkozó jogok a következők:

- **Hozzáféréshez való jog:** Kérhet egy másolatot az energiaadatokról a szolgáltatótól.
- **Helyesbítéshez való jog:** Kérheti a pontatlan vagy hiányzó adatok helyesbítését vagy frissítését.
- **Törléshez való jog:** Bizonyos körülmények között kérheti adatai törlését.
- **A feldolgozás korlátozásához való jog:** Korlátozhatja adataik felhasználását.
- **Adathordozhatósághoz való jog:** Adatait átvihető formátumban kaphatja meg.

Energiaadatainak védelmének, biztonságának és biztonságosságának javítása

Mivel az energia digitalizálása és a digitális technológiák használata az energiafogyasztás és -termelés kezelésére egyre inkább elterjedt, íme néhány tipp, amely segít növelni az energiaellátás adatvédelmét, biztonságát és védelmét.

- **Biztosítsa okos eszközeit:** Használjon erős jelszavakat, engedélyezze a kétfaktoros hitelesítést, és tartsa naprakészen a szoftvereket.
- **Védje hálózatát:** Biztosítsa Wi-Fi hálózatát, kerülje a nyilvános Wi-Fi használatát érzékeny tevékenységekhez, és fontolja meg tűzfal használatát.
- **Adatainak ellenőrzése:** Gondosan olvassa el az adatvédelmi irányelveket, gyakorolja GDPR-jogait, és ha kényelmetlenül érzi magát, lépjen ki az adatmegosztásból.

A digitális energiaipar folyamatosan fejlődik, rendszeresen jelennek meg új technológiák és fenyegetések. Fontos, hogy tájékozott maradjon ezekről a trendekről, hogy biztosíthassa adatvédelmét, biztonságát és védelmét.

Íme néhány példa olyan új technológiákra, amelyek jelenleg vagy a jövőben központi szerepet játszhatnak az energiaipar digitalizálásában:

- **Blockchain technológia:** A decentralizált főkönyvi technológia, a blockchain forradalmasíthatja az energiaadatok kezelését azáltal, hogy biztonságos, átlátható és hamisíthatatlan módot kínál az adatok nyomon követésére és megosztására.
- **Mesterséges intelligencia (AI) és gépi tanulás (ML):** Az AI és ML algoritmusok felhasználhatók az energiaadatok elemzésére, az anomáliák észlelésére és a potenciális biztonsági fenyegetések előrejelzésére, javítva ezzel az energiarendszerek általános biztonságát.
- **Kvantumszámítás:** Bár még korai stádiumban van, a kvantumszámítás felforgathatja a meglévő titkosítási módszereket, ami új kihívást jelent az energiaszektor adatbiztonsága számára.

Következtetés

Az energiaszektor digitális átalakulása óriási lehetőségeket kínál egy fenntarthatóbb, hatékonyabb és ügyfélközpontúbb energiarendszer kialakítására. Az átállás előnyei azonban csak akkor valósulhatnak meg teljes mértékben, ha aktívan és folyamatosan foglalkozunk az energiaipari adatvédelem, biztonság és védelem kihívásaival.

Energiafogyasztóként fontos szerepet játszunk a biztonságos digitális energiajövő kialakításában. Ha megértjük a GDPR szerinti jogainkat, proaktív lépéseket teszünk adataink védelme érdekében, és olyan energia- és szolgáltatókat választunk, akik prioritásként kezelik az adatvédelmet és a biztonságot, akkor biztosíthatjuk személyes adataink védelmét. Ezenkívül ha tájékozottak maradunk a kiberbiztonsági fenyegetésekről és a bevált gyakorlatokról, akkor hozzájárulhatunk mindannyiunk számára fontos energiainfrastruktúra védelméhez.

A digitális energiarendszerre való átállás nem csak a technológiáról szól, hanem arról is, hogy az egyének és a közösségek aktívan részt vehessenek a digitális energiaátállásban. A digitális eszközök elfogadásával és tájékozott döntések meghozatalával hozzájárulhatunk egy tisztább, megbízhatóbb és igazságosabb energiaellátáshoz.

További források

- Az EU adatvédelmi szabályai szerinti jogairól bővebben a *„Milyen jogaim vannak?”* című részben olvashat. 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

- További információk az EU kiberbiztonsági törvényéről és arról, hogyan védi Önt: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
- Olvassa el az intelligens hálózatok és intelligens mérőeszközök adatvédelmi hatásvizsgálatát (DPIA). https://energy.ec.europa.eu/topics/markets-and-consumers/smart-grids-and-meters/data-protection-impact-assessment-smart-grid-and-smart-metering-environment_en
- Tudjon meg többet arról, hogyan védi meg minket az Európai Bizottság *a kritikus infrastruktúráról és a kiberbiztonságról* szóló cikkben. https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en

Köszönetnyilvánítás

A *„Adatvédelem, biztonság és védelem a digitális energiaiparban”* című tanulmány az Nemzetközi Energiaügynökség (IEA) „Adatvédelem a digitális energia korszakában” https://www.iea.org/reports/digitalisation-and-energy és „A kiberbiztonság javítása az elektromos hálózatokban” https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems című kiadványokból (az „eredeti művek”), amelyek mindegyike CC BY 4.0 licenc alatt áll. Ezt az adaptációt az Every1 Project (az „adaptáló”) készítette és tette közzé, és CC BY 4.0 licenc alatt áll, hacsak másképp nem jelezzük. Ez az Every1 projekt által az IEA anyagából származtatott mű, és az Every1 projekt kizárólagos felelősséggel tartozik ezért a származtatott műért. A származtatott művet az IEA semmilyen formában nem támogatja.

Az adapter a következő szempontokból módosította az eredeti művet:

- Az adaptáció kifejezetten az eredeti művek energiaellátás, biztonság és védelem szempontjaira összpontosít.
- A műszaki nyelvet a széles közönség számára egyszerűsítették.
- Gyakorlati tippeket is hozzáadtak.
- Az Európai Bizottság forrásaiból származó új információkat építettünk be a GDPR és az EU kiberbiztonsági törvényének lefedése érdekében.

Képek forrása

Fő kurzus kép: Untitled by Mike Fritcher, CC BY-SA 2.0 licenc.
Bevezetés: Nő Windows Mobile készüléket használ a parkban gyermekével, Gail, CC BY-ND 2.0 licenc alapján.
Digitális technológiák és a digitális energetikai átállás: Patrik Tschudin „Echelon” című képe CC BY 2.0 licenc alatt áll.
Kiberbiztonság az energiaszektorban: Mobil munkavállaló, Michael Coghlan, CC BY-SA 2.0 licenc.
Energiaellátás adatainak védelme, biztonsága és biztonságossága: Arismendy Polanco adatai Public Domain Mark 1.0 licenc alatt állnak.