EVERY1

Financira Evropska unija

Zasebnost, varnost in zaščita v digitalnem energetskem okolju

Kako poteka ta tečaj

Ta kratek, 30-minutni tečaj pojasnjuje, kaj pomenijo zasebnost, varnost in zaščita v kontekstu digitalizacije energije. Tečaj obravnava tudi pomisleke glede uporabe pametnih energetskih tehnologij.

Morda ste:

- Zainteresirani za uporabo pametnih tehnologij, da bi bolje razumeli svojo porabo energije, vendar niste prepričani, kako zavarovati svoje osebne podatke.
- vas zanima, kako se vaši osebni podatki uporabljajo in delijo pri uporabi digitalnih tehnologij.
- želite bolje razumeti zasebnost, varnost in zaščito v kontekstu digitalizacije energije.

Ta tečaj bo poglobil vaše razumevanje digitalnega prehoda na energijo in podprl vašo lastno digitalno energetsko pot! Je del niza 12 tečajev z naslovom *Digital Energy Essentials* (Bistveni elementi digitalne energije), ki jih je razvil projekt Every1, katerega cilj je omogočiti in spodbuditi sodelovanje vseh v energetskem prehodu. Več o projektu lahko izveste na: https://every1.energy

Na koncu tečaja vam predlagamo nekaj dodatnih učnih gradiv, ki jih lahko raziskate. To vključuje tečaj *Kaj je digitalni energetski prehod?* ki raziskuje, kaj je digitalna energija in razloge za prehod na digitalizacijo naše proizvodnje in porabe energije.

To je prevod izvirne angleške različice tečaja, ki vključuje možnost izpolnitve kratkega kviza in pridobitve digitalnega znaka Every1.

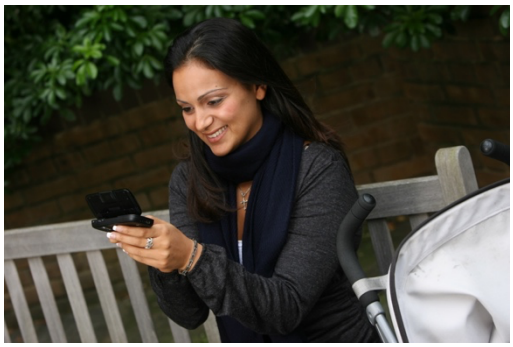
Ta projekt je prejel finančna sredstva iz programa Evropske unije za raziskave in inovacije Obzorje (2021–2027) v okviru sporazuma o dodelitvi sredstev št. 101075596. Za vsebino tega tečaja je odgovoren izključno projekt Every1 in ne odraža nujno mnenja Evropske unije.

Učni izidi

Po zaključku tega kratkega tečaja boste sposobni:

- Razlikovati med zasebnostjo, varnostjo in zaščito pri digitalizaciji energije.
- Razumeti glavne izzive pri zagotavljanju zasebnosti, varnosti in zaščite pri uporabi digitalnih tehnologij za energijo.
- Poznati svoje pravice v skladu z Splošno uredbo o varstvu podatkov (GDPR) v zvezi z energetskimi podatki.
- Uporabiti praktične nasvete za zaščito svojih podatkov in izboljšanje svoje digitalne energetske varnosti.

Uvod



Ker digitalne tehnologije postajajo sestavni del našega življenja, so zasebnost, varnost in zaščita naših osebnih podatkov v kontekstu digitalizacije energetike vse pomembnejše.

Pametni števci, mobilne aplikacije in druge digitalne naprave zbirajo in delijo podatke za izboljšanje energetske učinkovitosti, vendar to lahko sproži tudi zaskrbljenost glede zasebnosti in varnosti podatkov.
Preden začnemo, si podrobneje oglejmo, kaj mislimo s pojmi zasebnost, varnost in zaščita podatkov. To so medsebojno povezani, vendar različni pojmi:

- **Zasebnost** se nanaša na zaščito osebnih podatkov.
- **Zaščita** vključuje zagotavljanje, da uporaba digitalnih tehnologij ne povzroča fizične ali psihične škode.
- **Varnost** se osredotoča na zaščito podatkov pred nepooblaščenim dostopom ali napadi.

V tem tečaju ne bomo obravnavali le različnih izzivov za zasebnost, varnost in zaščito na področju energije, ampak tudi ukrepe, ki jih lahko sprejmete za svojo zaščito. Poglejali bomo tudi, kako vas in vaše podatke ščitijo vlade in dobavitelji energije, ter infrastrukturo, ki omogoča uporabo digitalnih tehnologij za proizvodnjo in porabo energije.

Digitalne tehnologije in digitalni prehod na energijo

Kot ste morda videli v tečaju *Pametne naprave in digitalna energetska tehnologija*, ki podrobneje raziskuje različne vrste pametnih naprav, obstaja vrsta digitalnih tehnologij, ki podpirajo digitalizacijo energije.

Digitalno energetsko okolje je zapleten ekosistem medsebojno povezanih tehnologij in zainteresiranih strani. Ključne komponente vključujejo:

- **Pametni števci:** naprave, ki samodejno zbirajo in prenašajo podatke o porabi energije dobaviteljem energije. Pametni števci omogočajo natančnejše zaračunavanje, vpogled v vzorce porabe in možnost sodelovanja v programih odziva na povpraševanje, kjer lahko prilagodite svojo porabo energije glede na povpraševanje in cenovne signale.
- **Pametna omrežja:** modernizirana električna omrežja, ki uporabljajo digitalne tehnologije za spremljanje in nadzor pretoka električne energije. Omogočajo dvosmerno komunikacijo med dobaviteljem in potrošnikom, kar omogoča spremljanje porabe energije v realnem času in integracijo obnovljivih virov energije.

- **Internet stvari (IoT) v energetiki:** Mreža povezanih naprav (termostati, aparati, polnilniki za električna vozila), ki zbirajo in izmenjujejo podatke, kar omogoča daljinsko upravljanje in optimizacijo porabe energije.

Podatki o energiji lahko vključujejo vzorce porabe, podatke o času uporabe, podrobnosti na ravni gospodinjskih aparatov in celo podatke o vedenju, ki jih je mogoče sklepati iz porabe. Ti podatki vam lahko pomagajo razumeti lastno porabo energije, potencialno prihraniti denar in sprejeti premišljene odločitve. Pomagajo lahko tudi dobaviteljem energije (kot je vaš dobavitelj električne energije) optimizirati omrežje, vam ponuditi prilagojene storitve in odkriti goljufije.

Vaše podatke o energiji običajno zbira vaš dobavitelj energije, vendar se lahko delijo tudi z operaterji merilnikov, zbiralci podatkov, zunanjimi ponudniki storitev in potencialno tudi z vladnimi agencijami ali pa imajo ti dostop do njih. Podatki o energiji so koristni za oblikovalce politik, na primer pri podpori razvoja učinkovitih energetskih politik in predpisov.

Podatki o porabi energije lahko vključujejo občutljive informacije. Ker lahko do vaših podatkov dostopa vrsta različnih organizacij in jih uporablja na različne načine, lahko to vzbuja zaskrbljenost. V nadaljevanju tečaja bomo predlagali nekaj načinov, kako lahko izboljšate svojo zasebnost, varnost in zaščito na področju energije. Najprej si oglejmo nekaj pogostih kibernetskih groženj in ukrepe, ki se izvajajo za zagotavljanje varnosti digitalnih sistemov.

Kibernetska varnost v energetskem sektorju

Digitalna preobrazba energetskega sektorja ga je naredila za tarčo kibernetskih napadov, ki lahko motijo oskrbo z energijo in ogrozijo občutljive informacije. Pogoste kibernetske grožnje vključujejo:

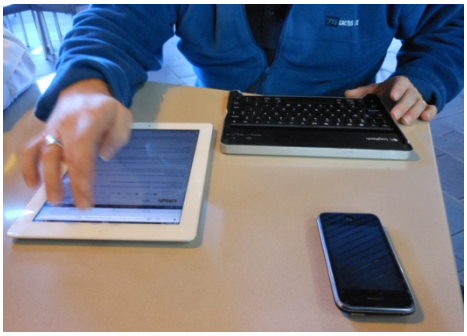
- **Zlonamerna programska oprema** (zlonamerna programska oprema, ki lahko poškoduje računalniške sisteme in podatke).
- **Izsiljevalsko programsko opremo** (vrsta zlonamerne programske opreme, ki šifrira vaše datoteke, jih naredi nedostopne in zahteva plačilo odkupnine za ponovno vzpostavitev dostopa).
- **Napadi z zavrnitvijo storitve** (ti napadi imajo za cilj preobremeniti sistem ali omrežje s prometom, tako da postane nedostopno za legitimne uporabnike).
- **Phishing prevare** (goljufivi poskusi pridobivanja občutljivih informacij, kot so gesla ali podatki o kreditnih karticah, s pretvarjanjem, da gre za zaupanja vredno osebo).

Za zaščito kritične infrastrukture so potrebni ukrepi, kot je segmentacija omrežja, ki pomeni razdelitev večjega omrežja na manjše, izolirane segmente. To omejuje širjenje kibernetskih

napadov in omejuje potencialno škodo, omejuje dostop do nadzora, zazna in preprečuje vdor nepooblaščenih oseb ter omogoča prilagojen dostop do nadzora.

Zakon EU o kibernetski varnosti izboljšuje kibernetsko varnost v vsej EU in določa pravila za certificiranje varnosti proizvodov in storitev. Zagotavljanje varnosti digitalnih energetskih sistemov je ključnega pomena. To vključuje:

- **Kiberfizični sistemi:** zaščita teh sistemov, v katerih se fizična infrastruktura upravlja digitalno, pred kibernetskimi napadi, ki lahko imajo posledice v realnem svetu.
- **Varnostni standardi:** upoštevanje varnostnih standardov EU za digitalne naprave in energetske sisteme, da se zagotovi njihova varna uporaba in vzdrževanje.



Splošna uredba o varstvu podatkov (GDPR) vam daje posebne pravice v zvezi z vašimi osebnimi podatki, vključno z energetskimi podatki. Te pravice v zvezi z vašimi osebnimi podatki vključujejo:

- **Pravico do dostopa:** od svojega ponudnika lahko zahtevate kopijo svojih energetskih podatkov.
- **Pravico do popravka:** lahko zahtevate, da se netočni ali manjkajoči podatki popravijo ali posodobijo.
- **Pravico do izbrisa:** pod določenimi pogoji lahko zahtevate izbris svojih podatkov.
- **Pravico do omejitve obdelave:** lahko omejite način uporabe svojih podatkov.
- **Pravico do prenosljivosti podatkov:** lahko prejmete svoje podatke v prenosljivem formatu.

Izboljšanje vaše energetske zasebnosti, varnosti in zaščite

Ker digitalizacija energije in uporaba digitalnih tehnologij za upravljanje naše porabe in proizvodnje energije postajajo vse bolj pogoste, vam ponujamo nekaj nasvetov, ki vam bodo pomagali izboljšati zasebnost, varnost in zaščito na področju energije.

- **Zaščitite svoje pametne naprave:** uporabljajte močna gesla, omogočite dvofaktorsko avtentikacijo in posodabljajte programsko opremo.
- **Zaščitite svoje omrežje:** zavarujte svoje omrežje Wi-Fi, se izogibajte javnim omrežjem Wi-Fi za občutljive dejavnosti in razmislite o uporabi požarnega zidu.
- **Nadzorujte svoje podatke:** pazljivo preglejte politike zasebnosti, uveljavljajte svoje pravice iz GDPR in se odjavite od deljenja podatkov, če vam to ni všeč.

Digitalno energetsko okolje se nenehno razvija, redno pa se pojavljajo nove tehnologije in grožnje. Da bi zagotovili svojo zasebnost, varnost in zaščito, je pomembno, da ste obveščeni o teh trendih.

Tukaj je nekaj primerov novih tehnologij, ki imajo ali bi v prihodnosti lahko imele pomembnejšo vlogo v digitalizaciji energije:

- **Tehnologija verižnih blokov:** Verižni bloki, decentralizirana tehnologija knjigovodstva, imajo potencial, da revolucionirajo upravljanje energetskih podatkov, saj zagotavljajo varen, pregleden in zaščiten način sledenja in izmenjave podatkov.
- **Umetna inteligenca (AI) in strojno učenje (ML):** Algoritmi AI in ML se lahko uporabljajo za analizo energetskih podatkov, odkrivanje anomalij in napovedovanje potencialnih varnostnih groženj, s čimer se izboljša splošna varnost energetskih sistemov.
- **Kvantno računalništvo:** Čeprav je kvantno računalništvo še v zgodnji fazi razvoja, ima potencial, da bi lahko ogrozilo obstoječe metode šifriranja, kar predstavlja nov izziv za varnost podatkov v energetskem sektorju.

Zaključek

Digitalna transformacija energetskega sektorja ponuja ogromne možnosti za bolj trajnosten, učinkovit in na stranke usmerjen energetski sistem. Vendar pa se lahko prednosti tega prehoda v celoti uresničijo le, če se aktivno in neprekinjeno ukvarjamo z izzivi na področju zasebnosti, varnosti in zaščite energije.

Kot porabniki energije imamo ključno vlogo pri oblikovanju varne digitalne energetske prihodnosti. Z razumevanjem naših pravic v skladu z GDPR, proaktivnimi ukrepi za zaščito naših podatkov in izbiro ponudnikov energije in storitev, ki dajejo prednost zasebnosti in varnosti, lahko zagotovimo, da bodo naši osebni podatki ostali zaščiteni. Poleg tega lahko z obveščanjem o grožnjah kibernetski varnosti in najboljših praksah pomagamo zaščititi energetsko infrastrukturo, na katero se vsi zanašamo.

Prehod na digitalni energetski sistem ni povezan le s tehnologijo, ampak tudi z omogočanjem posameznikom in skupnostim, da aktivno sodelujejo v digitalnem energetskem prehodu. Z uporabo digitalnih orodij in sprejemanjem informiranih odločitev lahko prispevamo k čistejši, zanesljivejši in pravičnejši energetski prihodnosti.

Dodatni viri

- Več o vaših pravicah v skladu s pravili EU o varstvu podatkov preberite v članku *Kaj so moje pravice?* 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
- Več o Zakonu EU o kibernetski varnosti in kako vas ščiti https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
- Preglejte oceno učinka na varstvo podatkov (DPIA) za pametna omrežja in pametne števce. https://energy.ec.europa.eu/topics/markets-and-consumers/smart-grids-

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

- Več o tem, kako nas Evropska komisija ščiti, si preberite v tem članku o *kritični infrastrukturi in kibernetski varnosti.* https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en

Zahvala

Zasebnost, varnost in zaščita v digitalnem energetskem okolju je priredba izbranega gradiva Mednarodne agencije za energijo (IEA) „Varstvo podatkov v digitalni energetski dobi“ https://www.iea.org/reports/digitalisation-and-energy in „Krepitev kibernetske odpornosti v elektroenergetskih sistemih“ https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems (v nadaljnjem besedilu: „izvirna dela“), ki sta licencirana pod licenco CC BY 4.0. Ta priredba je bila izdelana in objavljena v okviru projekta Every1 (»prireditelj«) in je licencirana pod licenco CC BY 4.0, če ni drugače navedeno. To je delo, ki ga je projekt Every1 izpeljal iz gradiva IEA, in projekt Every1 je edini odgovoren za to izpeljano delo. Izpeljano delo IEA na noben način ne podpira.

Adapter je izvirna dela spremenil v naslednjih pogledih:

- Prilagoditev se osredotoča zlasti na vidike energetske zasebnosti, varnosti in zaščite izvirnih del.
- Tehnični jezik je bil poenostavljen za splošno občinstvo.
- Dodani so bili praktični nasveti.
- Vključene so bile nove informacije iz virov Evropske komisije, ki zajemajo GDPR in zakon EU o kibernetski varnosti.

Avtorske pravice za slike