

# A napenergia kiberbiztonsági szabványának meghatározása

## Növekvő veszélyek a globális energiaszektorra

Napjaink összekapcsolt világában az energiaágazat a több forrásból származó kiberfenyegetések elsődleges célpontja. Ezek a fenyegetések a kiberbűnözők által pénzügyileg irányított tervektől a nemzetállamok által szervezett, politikai indíttatású támadásokig terjednek. Csak 2023-ban a kiberhackelés áldozatai világszerte (minden ágazatból) 1,1 milliárd dollárt fizettek ki a zsarolóprogram támadások után – és ez csak a jelentésekben szereplő összeg.\*

40.000

Holland háztartási és vállalati napelemes rendszer sebezhető a távvezérléssel szemben, állapította meg a holland kormány ([2022. július](#))

130.000

Napelemes rendszer (különböző invertergyártó) sebezhető a kibertámadásokkal szemben, számolt be egy kiberbiztonsági vállalat (USA, [2023. július](#))

200 millió dollár

A Target vállalat becsült vesztesége, miután 2013-ban az Egyesült Államokban feltörték a HVAC szolgáltató hálózatát.

## A nem biztosított PV-rendszerek kritikus üzleti kockázatot jelentenek

A napenergia a globális energiamix gyorsan növekvő összetevője, amely számos országban, például Hollandiában, Németországban és Egyesült Államokban a teljes energiatermelés jelentős részét teszi ki. Már most is kritikus fontosságú energiaforrás, amely számos vállalat számára segít csökkenteni a villamosenergia-költségeket és biztosítja az üzletmenet folyamatoságát. Miközben fenntartható energiamegoldásokat kínálnak, a PV-rendszerek új utakat nyitnak a kiberfenyegetések számára is. Az egyes rendszerek középpontjában az inverter áll, a tárgyak internetét (IoT) használó eszköz, amely általában az internethez kapcsolódik, hogy lehetővé tegye a rendszer felügyeletét és vezérlését. Ez sokkal érzékenyebb teszi a kibertámadásokkal szemben, mint egy jól védett gáz- vagy szénerőművet.

A napenergiát egyre több helyszíni energiafogyasztás, például akkumulátorok, EV-töltők és HVAC-rendszerek energiaellátására használják, és ez egyre inkább így lesz, ahogyan az energiagazdálkodási rendszerek korába lépünk. Egy nem biztonságos PV-rendszer nemcsak az üzletmenet folytonosságát veszélyezteti, hanem akaratlanul is kapuként szolgálhat a hackerek számára, hogy hozzáférjenek a fogyasztókhoz, valamint a szervezet szélesebb körű digitális platformjaihoz, további anyagi, pénzügyi és hírnévteli károkat okozva.

# A gyakori kiberkockázatok közé tartoznak:

## Adatszivárgás és szankciók

A hackerek kihasználhatják a sebezhető PV-rendszereket, hogy ellopják a szervezet belső hálózatain található személyes adatokat, ami olyan adatvédelmi incidenshez vezet, amely az áldozatot súlyos bírságok megfizetésére kényszeríti.

## Távvezérlés és szolgáltatásmegtagadás (DoS)

Ha egy vállalkozás DoS-támadások vagy távvezérlésű jogsértések áldozatává válik, jelentős zavarokkal kell szembenéznie. A zsarolóprogramok túszként tarthatják fogva a kritikus adatokat, míg a távvezérléses és DoS-támadások, valamint a jogsértések az alapvető szolgáltatásokat teljesen leállíthatják.

## Megfelelési kitettség

Az új kiberszabályozások bevezetésével a fotovoltaiikus telephelyek tulajdonosainak proaktív intézkedéseket kell hozniuk annak érdekében, hogy rendszereik megfeleljenek a követelményeknek, és elkerüljék a termékviSSzahívások vagy a pénzügyi szankciók kockázatát, ha hálózataik veszélybe kerülnek.

# A napelemes rendszerekre vonatkozó új kibertörvények és szabályozások kidolgozás alatt állnak

A fotovoltaiikus rendszerek kritikus energetikai infrastruktúrává váltak, és mint ilyenek, komoly figyelmet kapnak a szabályozó hatóságoktól. Ez már most a készülő új törvények és rendeletek "hullámában" is megmutatkozik.



### UL 2941

Az intelligens inverterek és elosztott energiaforrások kiberbiztonságára vonatkozó nemzetközi szabvány. (Várhatóan 2025)

### The "U.S Cyber Trust Mark"

A kiberbiztonsági tanúsítási és címkézési program. (Várhatóan 2025)

### Szabályozási

#### Közműbizottságok Országos Szövetsége (NARUC/NASEO)

Az elektromos elosztórendszerek és a DER kiberbiztonsági alapjai. (Várhatóan 2025)

### IEEE P1547.10

elosztott energiaforrások (DER) átjáró platformok munkacsoport. (Folyamatban lévő munka)



### UK PSTI (2023)

A termékbiztonsági és távközlési infrastruktúra.



### RED 2014/53/EU

Az európai rádióberendezésekről szóló irányelv.

### Kiberrezilienciáról szóló törvény

Unió szintű jogszabály az IoT és a kapcsolódó eszközök kiberbiztonságáról. (Várhatóan 2026-2027)

### NIS 2 irányelv

Az EU egészére kiterjedő irányelv az EU-ban a kiberbiztonság magas szintjének elérésére. (Hatályos 2024 októberében)



# SolarEdge - A napelemes kiberbiztonság globális vezetője

A SolarEdge a napelemes iparág vezetőjeként, amely több millió IoT-eszközzel rendelkezik globálisan, kiváló helyzetben van ahhoz, hogy felismerje a napelemes

eszközök tulajdonosainak kiberbiztonsági kockázatait, valamint az energiahálózatokat fenyegető veszélyeket.



## Az Ön biztonságát üzletünk középpontjába helyeztük.

Jelentős befektetéseket eszközöltünk egy elkötelezett szakértői csapat toborzásába, amely a kibervédelemmel kapcsolatos folyamatos erőfeszítéseinket vezeti.



## Segítünk a nemzetközi szabályozási kiberbiztonsági szabványok kidolgozásában

A SolarEdge aktívan részt vesz különböző műszaki bizottságokban, és azon dolgozik, hogy terméktervezésünk összhangban legyen a készülő szabályozásokkal. Eszközeink megfelelnek a legújabb referencia-útmutatók és a DER kiberbiztonsági szabványok előírásainak.



## A SolarEdge termékek fejlesztése során a kiberbiztonság alapvető prioritásként jelenik meg

Arra törekszünk, hogy ügyfeleinket folyamatosan védve tartsuk a folyamatosan fejlődő kiberfenyegetésekkel szemben azáltal, hogy a terméktervezés minden egyes lépésénél, az összes SolarEdge szoftver és hardver esetében intézkedéseket hajtunk végre.

# Maximalizálja a CyberEDGE-t

A SolarEdge-dzsel való együttműködés azt jelenti, hogy a rendszer teljes élettartama alatt extra védelmet kap. A kiberbiztonsággal kapcsolatos többszintű megközelítésünk célja az adatintegritás, a kommunikáció és az üzleti műveletek védelme a telephely üzembe helyezésétől a termelésig. A rendszercsatlakozás, a funkcionalitás és az ügyfeladatok védelme érdekében a

SolarEdge a Kiberinformált tervezés (CIE) elvét követi, és az információbiztonsági mechanizmusokat már a tervezés kezdeti szakaszától kezdve beépíti termékeinkbe. Folyamatosan adaptáljuk és fejlesztjük megoldásainkat a változó igényekhez és szabályozási előírásokhoz való igazodás érdekében.

Azzal, hogy termékeinket úgy tervezzük meg, hogy ne csak biztonságosak legyenek, hanem maximális láthatóságot és ellenőrzést is biztosítsanak a felhasználók számára, kiemelten kezeljük ügyfeleink biztonsági csapatainak igényeit.

Az energia alhálózat úgy van felépítve, hogy biztonságosan integrálható legyen a szervezet IT és OT hálózataival.

A felhasználói adatok és az energiafelhasználási adatok biztonságos átvitele és tárolása maximális adatvédelmet és kiberfenyegetettség elleni védelmet biztosít.

A SolarEdge inverterek a napelemes rendszer szíve, és más SolarEdge eszközökkel együtt úgy vannak kialakítva, hogy megelőzzék és felismerjék a napelemes rendszer egészére kiterjedő kibertámadásokat.

 Láthatóság és ellenőrzés

 Hálózati biztonság

 Adatbiztonság

 Eszközbiztonság

## A fotovoltaikus biztonsághoz hasonlóan a fotovoltaikus kiberbiztonság is elengedhetetlen.

Minimalizálja kiberkockázatát, ha a SolarEdge partnereként dönt. Biztosítsa, hogy vállalkozása biztonságos és ellenálló maradjon a folyamatosan fejlődő fenyegetésekkel szemben.

### A SolarEdge-ről

A SolarEdge Technologies a megújuló energiaforrások technológiájának globális vezetője, amely világszínvonalú mérnöki és innovációs megoldásokat kínál a lakossági, kereskedelmi és közüzemi szegmensek számára. A SolarEdge optimalizált megközelítést kínál az energia előállításához, tárolásához, kezeléséhez és fogyasztásához. A vállalat PV-invertereket és teljesítmény-optimalizálókat, energiagazdálkodási és optimalizálási megoldásokat, energiatárolási és hálózati szolgáltatásokat fejleszt és gyárt. A SolarEdge DC-optimalizált technológiáját több mint 140 országban több millió otthonban telepítették, és a Fortune 100 vállalat több mint 50%-ának van SolarEdge technológiája a háztetőn. A SolarEdge felgyorsítja az átmenetet az elosztott, fenntartható energiahálózatok felé, amelyek mindenhol optimalizálják az energiát.