SAMMANFATTNING TILL LEDARE OCH BESLUTSFATTARE

Förslag på åtgärder för att möta cyberhot mot elsystemet

Rapporten belyser cybersäkerheten för uppkopplade energiprodukter.

RISE RAPPORT 2023:MARS

Centrum för Cybersäkerhet
ri.se/sv/centrum-for-cybersakerhet

Följ oss på Sociala Medier

Kontaktperson:
Kim Elman, kim.elman@ri.se

Sammanfattning

Idag utgör cyberattacker ett konkret hot mot vårt elsystem. Samtidigt genomgår elsystemet en stor förändring med fler aktörer och mer väderberoende produktion i elmixen. Flexibla energiprodukter såsom solceller, elbilar, stora batterier och värmepumpar behövs för att skapa balans mellan den el som används och den el som produceras. Detta elsystem och elmarknad är beroende av digitala system för att fungera väl. När produkter i elsystemet digitaliseras och kopplas upp kan till exempel hushåll och bostadsrättsföreningar styra elanvändningen, lagra energi och leverera el till elsystemet mot betalning och på så sätt bidra till balans i elsystemet. Denna flexibilitet medför många fördelar såsom förbättrad energieffektivitet, ökad kontroll över energianvändningen, minskade kostnader hos hushållen, minskade effekttoppar i systemet och därmed bättre utnyttjande av elsystemet.

Men, så fort energiprodukterna kopplas upp mot internet skapas en möjlig väg in för **cyberattacker mot elsystemet.** Energibolag och nätägare har rutiner för att hantera cybersäkerhet som riktas mot deras anläggningar, däremot kan inte alla elanvändare förväntas ha lika god cybersäkerhet. Det kan leda till problem för den enskilde, men även **hela elsystemet kan störas** i en samordnad attack. Därför undersöker RISE påverkan på elsystemet av potentiella attacker och cybersäkerheten för uppkopplade energiprodukter.

RISE har i denna studie främst fokuserat på uppkopplade värmepumpar. Värmepumpar är dels stora elkonsumenter, dels har de varit uppkopplade länge och dels har de lång livslängd. Det finns också ett **ökat intresse bland värmepumpsägare** att **spara pengar** genom att koppla upp sin värmepump. Kombinationen av bristande uppdateringar och exponeringen mot internet skapar risker för cyberattacker. RISE har inte sett några tecken på att värmepumpar skiljer sig från övriga uppkopplade produkter i dessa avseenden. Det finns också många paralleller mellan potentiella sårbarheter hos värmepumpar och typiska sårbarheter hos andra uppkopplade energiprodukter att dra lärdom av.

RISE har funnit att de uppkopplade värmepumparna i landet nu tillsammans utgör en tillräckligt stor mängd för att kunna **orsaka störningar på elsystemet** vid en synkroniserad attack mot många värmepumpar. Situationen är liknande för andra uppkopplade energiprodukter. Vi har därför valt att informera om riskerna, eftersom det är många aktörer som behöver agera för att stärka säkerheten.

För att skydda elsystemet behövs bland annat fler skyddsmekanismer i elsystemet, säkra och systematiska uppdateringar för produkter och tjänster, bra lösenordshantering, samt rätt och tillgänglig information till användarna. Ett starkare **systematiskt cybersäkerhetsarbete behövs** inom energibranschen på alla nivåer eftersom riskerna med uppkopplade energiprodukter är så stora. Alla aktörer har ett ansvar; myndigheter och beslutsfattare, leverantörer och installatörer samt inte minst den enskilde användaren.

Om centrum för cybersäkerhet

Centrum för cybersäkerhet på RISE stärker den tillämpade forskningen och kompetensutvecklingen inom cybersäkerhet i Sverige.

RISE är ett oberoende, statligt ägt forskningsinstitut. Centret skapar en neutral nationell plattform som stöttar näringsliv och offentlig sektor genom expertstöd, forskningspartnerskap, innovationsledning samt test-och demonstrationsmöjligheter.

Ett samarbete med RISE innebär tillgång till ett stort nätverk av tvärvetenskapliga team som innehar både en bred domänkompetens såväl som en djup cybersäkerhetsexpertis.

Vi kan erbjuda stöd inom olika tillämpningsnivåer av cybersäkerhet – från forskning och utveckling, certifiering, utbildning/träning till systemtest i kontrollerade virtuella miljöer.

Läs mer på vår hemsida:
www.ri.se/sv/centrum-for-cybersakerhet

”RISE undersöker påverkan på elsystemet av potentiella attacker och cybersäkerheten för uppkopplade energiprodukter.”

1. Inledning

Antalet cyberattacker ökar och incidenter som tidigare varit extraordinära känns nu alltmer alldagliga. Intrång kan leda till att angripare får kontroll över viktiga processer inom exempelvis värme, vatten, el, eller transport. Det kan i sin tur störa den svenska infrastrukturen, och en sådan störning kan få omfattande konsekvenser för samhället.

Riskerna ökar också kontinuerligt. Exempelvis genomgår det svenska energisystemet stora förändringar och som en del i detta är det fler och fler av elsystemets komponenter som digitaliseras och kopplas upp mot internet för att möjliggöra ett mer resurseffektivt och optimerat system. När dessa komponenter kopplas upp skapas dock en möjlig väg in för cyberattacker mot elsystemet. Redan idag utgör cyberattacker ett konkret hot mot energisystemet. Ett proaktivt och brett arbete behövs för att skydda mot olika typer av dataintrång.

Det svenska elsystemet blir också alltmer **sammankopplat med andra länder**. Under de senaste åren har antalet cyberattacker fortsatt att öka samtidigt som deras påverkan blir allt större. European Union Agency for Cybersecurity (ENISA, 2021) har också sett att fler cyberattacker nu riktar in sig på samhällsviktig infrastruktur så som **sjukvård, transport och energi**. Cyberattacken som slog ut Ukrainas elsystem 2015 har pekats ut som det stora uppvaknandet i samhället. Ett exempel på hur cybersäkerhetsrisker påverkat elsystemet är också den ransomware-attack som drabbade New Orleans år 2019 (Forbes, 2019). Attacken orsakade omfattande störningar i stadens datorsystem inklusive de som användes för att hantera distributionsnätet. Som ett resultat var staden tvungen att förklara undantagstillstånd.

Energibolag och nätägare har rutiner för att hantera cybersäkerhet, däremot kan inte elanvändarna förväntas ha lika goda rutiner för sin cybersäkerhet. Därför undersöker RISE effekterna av potentiella cyberattacker mot uppkopplade energiprodukter såsom solceller, elbilar, stora batterier och värmepumpar. En viktig komponent i arbetet är att öka medvetenheten hos den enskilda individen.

Denna rapport beskriver potentiella sårbarheter och risker på systemnivå och inte specifika sårbarheter hos enskilda produkter.

”Syftet med rapporten är att beskriva potentiella sårbarheter och risker på systemnivå och inte specifika sårbarheter hos enskilda produkter.”

1.1 Flexibilitet med hjälp av uppkopplade energiprodukter

Ju mer väderberoende elproduktion vi har i systemet, desto viktigare blir det att ha flexibel energikonsumtion som skapar balans i systemet. I och med att produkter i elsystemet digitaliseras och kopplas upp kan till exempel hushåll och bostadsrättsföreningar lagra och leverera el tillbaka till elsystemet mot betalning för att skapa balans mellan den el som används och den el som produceras. Denna flexibilitet medför flera fördelar såsom förbättrad energieffektivitet, ökad kontroll av energianvändningen (även på distans), minskade kostnader hos hushållen, minskade effekttoppar i systemet och därmed bättre utnyttjande av elsystemet. Detta förväntas leda till **lägre kostnader och högre resiliens** i systemet.

1.2 Urval av produkter som kan få påverkan på elsystemet

Några produkter som RISE funnit intressanta att analysera är **solceller, batterier, elbilar med tillhörande laddare, samt värmepumpar.** Tillsammans kan dessa bidra med omfattande flexibilitet i framtiden. Redan nu finns potential där solcellsanläggningar regleras ned eller laddar hembatterier, elbilsladdning styrs till fördelaktiga timmar för elsystemet eller hjälper till med frekvensreglering och värmepumpar som flyttar energi över tid genom att värma mer de timmar det är överskott och drar ned värmeproduktionen under bristtimmar. Ännu saknas dock storskalig och effektiv hantering av mekanismerna bakom flexibiliteten i nätet, något RISE arbetar med att överbrygga i projektet Storskalig Laststyrning Av Värmepumpar i Elnätet (2023).

Antalet installerade **solcellsanläggningar** ökar stadigt i Sverige. År 2021 levererade de 92 359 anläggningarna 1,1 TWh el och hade en samlad effekt på 1,6 GW, (Svenska kraftnät och Energimyndigheten, 2022). Dock är inte alla uppkopplade. Energimyndigheten uppskattar elproduktionen från solceller år 2050 till mellan 9 och 11 TWh (Energimyndigheten, 2021). Samtidigt uppger forskare från Totalförsvarets forskningsinstitut, FOI, att vissa privatägda svenska solcellsanläggningar inte är tillräckligt skyddade för att motstå en cyberattack (Sveriges radio, 2022).

Enligt PowerCircle fanns 438 000 **laddbara bilar** i januari 2023, varav 199 000 rena elbilar (Elbilsstatistik, 2023). År 2030 prognostiseras Sverige ha 2,5 miljoner laddbara bilar varav 2/3 är rena elbilar (Andersson & Kulin, 2018). Dessa kommer behöva 10 TWh el per år (Bixia, 2019). Till skillnad mot solcellsanläggingar och värmepumpar är bilar inte alltid fysiskt kopplade till elsystemet, då de används för förflyttning.

Värmepumpar började användas i Sverige redan i början av 80-talet, nu har vi 1,5 miljoner värmepumpar i Sverige (Energimyndigheten 2022), vilket gör oss till det näst värmepumpstätaste landet i världen. Bara Norge har fler per invånare (Energy Monitor, 2020). Den installerade kompressoreffekten i landets värmepumpar är i storleksordningen några GW (Borgström, 2019). Vid kallt väder förbrukar de alltså lika mycket el som några kärnkraftsreaktorer producerar.

1.3 Varför valde RISE att fokusera på värmepumpar i denna studie?

RISE uppskattar att det finns ca 300 000 **vätskeburna värmepumpar** som går att koppla upp mot internet. Utöver det finns ett stort antal uppkopplingsbara **luftvärmepumpar**, men antalet har inte skattats av RISE, delvis därför att statistiken är bristfällig. Idag är i princip alla nya värmepumpar **uppkopplingsbara** vid leverans. Det betyder att potentialen, när dessa styrs efter elsystemets behov, är stor och växer för varje år som går.

Värmepumpar är alltså dels stora elkonsumenter, dels har de varit uppkopplade länge och dels har de lång livslängd. RISE uppskattar att de uppkopplade värmepumparna nu tillsammans närmar sig en kritisk massa för att kunna orsaka störningar på elsystemet, vilket gör problemen aktuella redan nu.

Därför har RISE i denna studie valt att fokusera på värmepumpar. De är inte på något vis unika när det gäller cybersäkerhetsrisker, utan är ett **tydligt exempel** på ett **generellt problem**.

2. Risker via värmepumpar

Värmepumpar kan attackeras på flera olika sätt. Dels **via den enskilda värmepumpen**, dels genom **svagheter i dess app** eller i andra system. **I båda fallen kan en hacker rekrytera ett stort antal värmepumpar långt innan attacken sker**. En av huvudriskerna är användarens handhavande av produkten.

Notera att det inte bara handlar om att en enskild värmepump eller annan produkt kan bli obrukbar eller på annat sätt kapad. Det större problemet är att **många enheter samtidigt** kan attackeras i det tysta, för att sedan plötsligt och koordinerat användas för att störa elsystemet. Enheterna kan också orsaka stora kostnader för konsumenterna, genom att exempelvis förbruka stora mängder energi.

Nedan följer en lista med **exempel på risker** som kan uppstå för uppkopplade produkter i allmänhet. RISE har inte sett några tecken på att värmepumpar skiljer sig från övriga uppkopplade produkter i dessa avseenden.

2.1 Produkten i sig

Produkter som är **gamla eller dåligt tillverkade** kan lämna oanvända tjänster exponerade med svaga eller hårdkodade lösenord, eller via okrypterade kanaler. Produkters **uppdateringar** sker inte alltid på ett tillräckligt säkert sätt. Värst är att säkerhetshål som kontinuerligt upptäcks i de mjukvarubibliotek som används i produkterna hela tiden måste åtgärdas, trots att leverantörens underhållsgaranti löpt ut.

2.2 Molntjänster

Molntjänster är praktiska och höjer i många fall säkerheten, men de är inte ofelbara. De kan ha **otillräcklig isolering** mellan olika kunder eller ha **bristande rutiner** för användarhantering och åtkomsthantering. De kan råka ut för attacker som riktats mot sina underleverantörer (”supply chain attacks”) eller från missnöjda eller utpressade egna anställda.

2.3 Användare

Användare kan vara exempelvis hushåll, bostadsrättsföreningar, fastighetsägare, lantbrukare eller företag. Några vanliga misstag är att man använder samma **lösenord** på flera ställen, använder korta eller på andra sätt lättgissade lösenord, att man inte installerar **säkerhetsuppdateringar,** eller att man inte ser och åtgärdar attacker förrän de fått fäste och sprider sig under lång tid. Många produkter som värmepumpar, solceller, laddstolpar och batterilager har lång livslängd och är dessutom en stor investering som gör att man helst inte reparerar dem eller byter ut dem så länge de fungerar.

”En hacker kan rekrytera ett stort antal värmepumpar långt innan attacken sker.”

3. Konsekvenser av en attack

Idag hanteras last- och produktionsbalansen i elsystemet med balansmarknader för att återställa systemet vid en störning. Normalfrekvensen för det svenska elsystemet är 50 ± 0.1 Hz, därefter börjar stödtjänster aktiveras för att avhjälpa störningen. Det finns även nödkraft från HVDC-länkar (högspända likströmslänkar) och lastbortkoppling vid stora händelser.

Genom simuleringar i det nordiska testsystemet Nordic32 (N32) har RISE funnit att en tillräckligt stor attack mot värmepumpar kan orsaka att frekvensen går tillräckligt långt utanför den normala och på så sätt **skapa betydande störningar** och obalans i större områden av elsystemet. Osäkerhet om stabilitet i elsystemet kan även skapa andra effekter i andra delar av samhället, till exempel att företags vilja att investera och etablera sig i landet kan minska. Det riskerar också att påverka förtroendet för Sverige som nation, vår export och förtroendet för våra produkter.

Även för den enskilda villaägaren och bostadsrättsföreningen kan konsekvenserna bli stora. Ett lyckat angrepp mot villaägarens eller bostadsrättsföreningens utrustning kan konsumera stora mängder el och ge en stor elräkning, utöver att utrustningen kan användas som en del i att störa hela Sveriges elförsörjning. Sker attacken under vintern kan bostäder bli utkylda eller till och med bli förstörda om rör hinner frysa sönder. Oskyddad utrustning hos hushållen kan kapas och användas till allt från **stöld av information, spionage, sabotage och utpressning** till att undergräva tilltron till system och samhällsfunktioner, som mål eller medel för angrepp, eller för att förstärka angrepp som exempelvis överbelastning av datorsystem.

”Ett lyckat angrepp kan konsumera stora mängder el och ge en stor elräkning, utöver att utrustningen kan användas som en del i att störa hela Sveriges elförsörjning”

4. Förslag på åtgärder

Riskerna som följer med allt fler uppkopplade enheter hos användarna behöver lyftas, och denna rapport gör så med fokus på värmepumpar som ett exempel. I denna rapport har vi belyst vilken påverkan en cyberattack kan få på både en enskild värmepump men också på aggregerad nivå. Vi kan visa att när många enheter synkroniserat och systematiskt hackas, kan störningar i elsystemet uppstå och dessa kan i sin tur leda till störningar i samhället. Det kan också leda till andra effekter, exempelvis ekonomiska då investeringar kan hämmas om det svenska elsystemet uppfattas som instabilt och osäkert, eller om produktionsbortfall på grund av störningar påverkar förtroendet för svensk export av exempelvis energiprodukter.

4.1 Vem kan göra vad för att förbättra situationen?

Riskberedskapsarbete och cybersäkerhetsstandarder har hittills fokuserat mycket på energiproduktion och distribution, med deras specifika system och enheter. Däremot brister kunskapen om hur elsystemet kan påverkas från elanvändarsidan och vad som sker när en antagonist avsiktligt rekryterar produkter hos användarna för att orsaka problem för elnätsägare och distributionsnät. Det finns idag diverse initiativ, standarder och regelverk som reglerar uppkopplade IoT-produkter och EU driver fler initiativ för att förbättra säkerheten i dessa produkter, till exempel Cyber Resilience Act.

Samhällets beredskap, kompetens och samarbete kring cybersäkerhet behöver förbättras på flera nivåer. Cybersäkerhet är en **kontinuerlig process** som alla behöver vara medvetna om för att vi ska kunna ha en trygg tillgång på energi i vårt samhälle.

4.2 Myndigheter och beslutsfattare

Sverige behöver ständigt stärka sin samlade förmåga att **förebygga, upptäcka och hantera cyberhot**. Myndigheter och beslutsfattare behöver **förmedla råd och stöd**, främja **samverkan** och informationsutbyte samt koordinera arbetet genom att exempelvis:

- Tydligt kliva fram som en pålitlig och neutral informationskälla
- Ta fram lämpligt och anpassat informationsmaterial
- Öka kunskapen hos nätägare att utveckla sina elnät så att de blir mindre känsliga för attacker via uppkopplade enheter
- Se till att frågor om cybersäkerhet alltid finns med vid utvecklingen av flexibilitet i elsystemet
- Ställa krav på cybersäkerhet i standardiseringsverksamhet
- Underlätta för utbildning och certifiering av tillverkare
- Öka medvetenheten och kunskapsnivån kring cybersäkerhet i hela samhället.

4.3 Energibolag

Energibolagen behöver **uppfylla grundläggande informationssäkerhetskrav** och ständigt arbeta med att utveckla sitt eget och sina kunders säkerhetsarbete genom att exempelvis:

- Göra riskanalyser på nätverk och informationssystem
- Öka kunskap och medvetenhet hos egen personal och underleverantörer, liksom hos sina kunder och de hushåll som levererar el (prosumenter) i sina nät
- Hjälpa sina kunder att hålla sin utrustning uppdaterad och att välja bra lösenord och använda övriga säkerhetsmekanismer
- Se till att hot begränsas genom partitionering och att systemen har redundant styrning.

4.4 Leverantörer

Med ökat hot och risker som kommer med vår digitala öppenhet kommer **krav på kunskap** och en större mognadsgrad när det gäller säkerhet. Till exempel kan leverantörer av produkter och tjänster arbeta för att:

- Öka kunskap och medvetenhet hos sin egen personal, underleverantörer, säljare och installatörer, liksom hos sina slutkunder
- Se till att varje producerad utrustning levereras med exempelvis ett unikt lösenord med rimlig längd och komplexitet och med genomtänkta, säkra uppstartsinstruktioner
- Se till att hålla uppkopplad utrustning uppdaterad och försedd med lämpliga och uppdaterade säkerhetsmekanismer, även efter garantitidens utgång
- Se till att attackytorna minimeras genom att exempelvis spärra kommunikationsprotokoll som inte används i installerade standardbibliotek
- Se till att funktioner och kommunikationsgränssnitt ej är aktiverade och oskyddade vid leverans, utan behöver sättas upp individuellt som en del av installationen.

4.5 Installatörer

Installatörer bör hjälpa till så att systemen som kopplas upp blir tillräckligt säkra och följer de **normer** som finns genom att:

- Säkerställa installatörers och andra anställdas kunskaper inom IT-säkerhet
- Hjälpa kunden så att utrustningen ansluts korrekt bakom en brandvägg
- Hjälpa kunden att se till att enbart kommunikationsgränssnitt och kommunikationsprotokoll som behöver användas är påslagna
- Hjälpa kunden att hantera lösenord på ett säkert sätt
- Ha rutiner för rensning av känsliga data och inte spara kundernas lösenord och övrig känslig information efter installationen. Det är särskilt viktigt att inget lämnas på exempelvis oskyddade bärbara datorer.

4.6 Användare

Elanvändaren kan vara exempelvis ett hushåll, en bostadsrättsförening, en fastighet, ett lantbruk eller företag. Elanvändaren kan göra sina system säkrare genom att:

» Välja en pålitlig leverantör med gott renommé

» Ställa krav på god säkerhet i utrustningen vid köp och kontinuerligt installera mjukvaruuppdateringar från sin leverantör

» Följa råden från myndigheter och sitt elbolag om säkerhetsåtgärder – hot och skydd utvecklas helas tiden

» Vara medveten! Ha koll på vilka enheter i huset som kan kommunicera med varandra. Ett uppkopplat spel med säkerhetsproblem kan ge åtkomst till din värmepump, elbil och andra uppkopplade saker

» Använda långa, svårgissade lösenord. En rekommendation idag är att använda minst 14 tecken, med blandade små och stora bokstäver, siffror och skiljetecken. Undvik ord som finns i en ordlista. I valet mellan ett kort lösenord som du kommer ihåg eller ett långt lösenord som du behöver skriva upp, så är ett långt lösenord mycket bättre. Använd inte samma lösenord för olika tjänster

» Vara uppmärksam på avvikande beteende. Om din uppkopplade enhet plötsligt börjar bete sig annorlunda bör du ta kontakt med din leverantör för att få hjälp att agera rätt.

4.7 RISE

Genom en tvärdisciplinär arbetsgrupp har RISE möjlighet att hjälpa olika aktörer i arbetet. RISE kan:

» Ta fram underlag till informationsspridning

» Undersöka cybersäkerheten i olika produkter som kopplas upp mot internet

» Analysera effekterna av attacker mot uppkopplade produkter

» Ta fram metoder för att förhindra och mildra påverkan från attacker – både i elsystemet och i uppkopplade produkter

» Ge utbildning till olika aktörer i branschen.

”Cybersäkerhet är en kontinuerlig process som alla behöver vara medvetna om för att vi ska kunna ha en trygg tillgång på energi i vårt samhälle.”

5. Källor

Andersson A., Kulin D., 2018. Elbilsläget 2018. Power Circle.

Borgström, S., Norrsén, T., Lindahl, M., Förstudie Laststyrning av värmepumpar i småhus samt Småhusens bidrag till minskade topplaster, 2019

Elbilsstatistik, 2022. Elbilsstatistik.se, Stycken laddbara fordon i Sverige. URL: https://www.elbilsstatistik.se. [2023-02-22]

Energimyndigheten, Energistatistik för småhus, 2018 (se_ca_2020_se.pdf).

Energimyndigheten, 2021. Nationell riskberedskapsplan för Sveriges elförsörjning, URL: http://www.energimyndigheten.se/globalassets/trygg-energiforsorjning/el/riskberedskapsplan-ver-0.1.pdf. [2021-03-03].

Energimyndigheten, https://www.energimyndigheten.se/nyhetsarkiv/2022/kraftig-okning-av-installerade-solcellsanlaggningar/, [2023-02-27]

Energimyndigheten, https://www.energimyndigheten.se/statistik/den-officiella-statistiken/statistikprodukter/energistatistik-for-smahus-flerbostadshus-och-lokaler/?currentTab=0#mainheading, [2023-01-23]

Energy Monitor, URL: https://www.energymonitor.ai/sectors/heating-cooling/heat-pumps-are-on-the-rise-in-europe/, [2023-02-28]

ENISA 2021, ”ENISA Threat Landscape 2021”, Url: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Forbes 2019, ”New Orleans Declares State Of Emergency Following Cyber Attack”, Davey Winder, URL: https://www.forbes.com/sites/daveywinder/2019/12/14/new-orleans-declares-state-of-emergency-following-cyber-attack/

Kesselfors S., 2019. Bixias långtidsprognos: Räkna med högre elpriser år 2030. URL: https://www.vindkraftsnyheter.se/20190802/5789/bixias-langtidsprognos-rakna-med-hogre-elpriser-ar-2030. [2022-02-17]

PowerCircle, URL: https://www.elbilsstatistik.se/elbilsstatistik, [2023-02-27]

Power System Dynamic Performance Committee, 2015. Test Systems for Voltage Stability Analysis and Security Assessment. IEEE Power and Energy Society.

Scenarier över Sveriges energisystem 2020, Energimyndigheten, 2021

Svenska Kraftnät, URL: https://www.svk.se/om-kraftsystemet/kraftsystemdata/elstatistik/, [2023-02-28]

Sveriges Radio, Lekholm K, Solceller kan vara säkerhetsrisk – hacker tog över en miljon anläggningar, Sveriges radio, 2022-10-29. URL: https://sverigesradio.se/artikel/solceller-kan-vara-sakerhetsrisk-hacker-tog-over-en-miljon-anlaggningar, [2023-02-24]

10 common security mistakes and how to avoid them, URL: https://www.welivesecurity.com/2022/11/09/10-common-digital-security-mistakes-how-avoid/ [2023-03-22]

När produkter i elsystemet digitaliseras och kopplas upp skapas en möjlig väg in för cyberattacker i elsystemet. Rapporten syftar till att belysa cybersäkerheten för uppkopplade energiprodukter, samt vara ett stöd för chefer och beslutsfattare i den offentliga och privata sektorn.

RISE – Research Institutes of Sweden
ri.se / info@ri.se / 010-516 50 00
Isafjordsgatan 22, 6 tr | SE-164 40 Kista

Grants Office/Informationscenter
RISE Rapport: 2023:mars