FORBRUKERRÅDET

Justis- og beredskapsdepartementet 15.03.2019

Svar på høring NOU: 2018:14 IKT-sikkerhet i alle ledd

Forbrukerrådet viser til høringsbrev datert 21.12.2018 fra Justis- og beredskapsdepartementet, med frist 22. 03.2019 for å komme med merknader til NOU 2018: 14 IKT-sikkerhet i alle ledd, og forslag til gjennomføring av EUs direktiv om sikkerhet i nettverk og informasjonssystemer (NIS-direktivet). Innspillene fra Forbrukerrådet gjelder NOU 2018:14 'IKT-sikkerhet i alle ledd'. Vi har valgt å ikke gi innspill til NIS-direktivet.

Forbrukerrådet mener Holte-utvalget har foretatt en grundig og god gjennomgang av utfordringene som kan oppstå når produkter kobles på nett, og det pekes på en rekke gode og relevante tiltak som bør iverksettes.

Våre hovedsynspunkter til høringen er:

- Forbrukerrådet ønsker bindende minstekrav for IKT-sikkerhet i tilkoblede forbrukerprodukter.
- Tydeligere rollefordeling og samarbeid mellom relevante sektortilsyn, samt økt tilsyn.
- Tilrettelagt samarbeid mellom relevante bransjeaktører og myndigheter, for å bidra med veiledning og råd.
- Koordinerte mekanismer for å ivareta og respondere på varsler om sikkerhetsbrister.
- IKT-sikkerhet må bli en del av offentlige anskaffelser.
- Norske myndigheter må støtte EU-prosesser for å sikre framtidsrettet regulering for IKT-sikkerhet i tilkoblede forbrukerprodukter.

Under følger Forbrukerrådets merknader til høringen, hvor vi innledningsvis gir noen generelle innspill som kan bedre IKT-sikkerheten for tilkoblede forbrukerprodukter og tilhørende digitale tjenester, deretter gir vi våre

Forbrukerrådet Postboks 463 Sentrum, 0105 Oslo, Org.nr 871 033 382
Telefon 23 400 500, post@forbrukerradet.no

merknader til den delen av høringen som er knyttet til regulering og ansvar for tilkoblede produkter og tjenester. Vi vil også gi noen kommentarer til relevante og parallelle prosesser som utspiller seg i EU, der norske myndigheter har god mulighet til å engasjere seg i arbeidet for bedre IKT-sikkerhet.

Generelle innspill og kommentarer

Forbrukerrådet har de siste årene prioritert arbeidet med utfordringer knyttet til tilkoblede forbrukerprodukter. I vårt arbeid har vi avdekket store sikkerhetshull i tilkoblede leker[1] og i GPS-klokker for barn.[2] Uvedkommende kunne ta styring over produktene, få innsyn i sensitiv informasjon om eierne, eller kunne tvinge GPS-klokker til å ringe dyre telefonnumre og slik svindle eierne for penger. Dette arbeidet ble brukt som begrunnelse da Europakommisjonen i begynnelsen av februar 2019 la frem et veikart knyttet til en aktivering av en delegert rettsakt i radioutstyrsdirektivet. I veikartet foreslås det å tilføye regler slik at IKT-sikkerhet og personvern i tilkoblede produkter skal ivaretas i radioutstyrsdirektivet.[3]

Det er et stort og økende antall tilkoblede produkter på markedet og i norske hjem. Tingenes internett omfatter alt fra smarthus, vannkokere, leketøy, biler til helseverktøy.

Tilkoblede forbrukerprodukter kan misbrukes av uvedkommende, blant annet gjennom målrettede hackerangrep, svindel, personvernbrudd, og identitetstyveri. Manglende IKT-sikkerhet kan også føre til at produkter ikke fungerer som de skal. Uvedkommende kan ta over kontrollen på mange tusen tilkoblede panelovner med manglende IKT-sikkerhet og kreve løsepenger for å gi eier styringen tilbake, eller de kan til og med overbelaste strømnettet.[4] Det finnes allerede eksempler på at dataangrep har ført til at oppvarming i boligblokker i Finland ble skrudd av midt på vinteren.[5] Medisinsk utstyr uten

[1] https://www.forbrukerradet.no/siste-nytt/cayla-og-i-que-bryter-flere-norske-lover/
[2] https://www.forbrukerradet.no/siste-nytt/elendig-sikkerhet-i-smartklokker-for-barn/
[3] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-6426936_en
[4] https://nrkbeta.no/2019/01/16/kunne-sendt-kommandoer-til-alle-tilkoblede-smartovner-fra-norske-mill/
[5] https://www.forbes.com/sites/leemathews/2016/11/07/ddos-attack-leaves-finnish-apartments-without-heat/#49a9bb941a09

tilstrekkelig IKT-sikkerhet kan få potensielt fatale konsekvenser, for eksempel ved at hackere får kontroll over en tilkoblet pacemaker.[6]

Forbrukerrådets undersøkelser viser tilfeller der tilkoblede produkter tilgjengelig for norske forbrukere produseres og importeres av aktører med manglende erfaring og kompetanse når det gjelder IKT-sikkerhet. Det økte antall enheter fører dessuten til flere potensielle sårbarheter og mulige angrepsflater.

Myndighetene i Norge og i EU har satt i gang et viktig arbeid gjennom implementeringen av NIS-direktivet. Direktivet tilrettelegger for nødvendige tiltak for å sikre samfunnskritiske institusjoner og infrastruktur gjennom å stille krav til IKT-sikkerhet. Siden direktivet i hovedsak tar for seg samfunnskritiske funksjoner, har Forbrukerrådet valgt å ikke svare på høringen om implementeringen. Forbrukerrådet har merket seg at høringen primært fokuserer på de samfunnskritiske funksjonene, og savner en noe bredere behandling som også inkluderer forbrukerprodukter og tjenesteleverandører. For å ivareta IKT-sikkerhet i samfunnet er det avgjørende at hele verdikjeden er sikker, både infrastruktur og nettverk, og produkter som havner hos sluttbrukere

Tilsynelatende harmløse produkter som kobles på internett kan bli en trussel for samfunnets sikkerhet, for eksempel ved at de inngår i såkalte «botnet».[7] Dersom uvedkommende tar kontroll over et stort antall enheter, kan det også få alvorlige konsekvenser. For eksempel kan man se for seg en situasjon hvor en ondsinnet aktør tar kontroll over en mengde tilkoblede termostater, og overbelaster strømnettet ved å skru opp temperaturen på samtlige enheter. For å gjennomføre helhetlige grep på IKT-sikkerhet, er det derfor viktig at forbrukerprodukter også inngår i helhetsbildet, og at forbrukerperspektivet også representeres i et nasjonalt IKT-sikkerhetssenter.

[6] https://www.bbc.com/news/technology-34899713

[7] Botnet-angrep skjer ved at en angriper tar kontroll over en stor antall enheter. Disse enhetene kan for eksempel brukes til å sende massiv trafikk mot en sentral server, som kan overbelaste serveren, et såkalt Distributed Denial of Service-angrep (DDoS). https://securityintelligence.com/thingbots-the-future-of-botnets-in-the-internet-of-things/

Bindende minstekrav for IKT-sikkerhet (kapittel 8)

Forbrukerrådet støtter utvalgets forslag om at ansvaret for IKT-sikkerhet i tilkoblede produkter må flyttes fra forbruker og over på leverandør og produsent. Dette bør gjøres gjennom bindende minstekrav for IKT-sikkerhet. Eksempler på minstekrav kan være kryptering, verifikasjonsmekanismer, jevnlige sikkerhetsoppdateringer og lignende.

Dersom det oppstår problemer med produkter som følge av manglende IKT-sikkerhet, er det avgjørende at forbruker får informasjon om hvem de skal forholde seg til. Forbrukerrådet mener at ansvaret i slike situasjoner må ligge hos selger, og at forbruker har rett til å klage og å kreve penger tilbake for produkter som har alvorlige sikkerhetsbrister. Det må også stilles krav om at leverandører av tilkoblede forbrukerprodukter oppgir hvor lenge produktet støttes med sikkerhetsoppdateringer, hvilke sikkerhetsrutiner de har, og at de oppgir et kontaktpunkt for sikkerhetsrelaterte henvendelser. Det er også ønskelig at leverandører av tilkoblede forbrukerprodukter kan dokumentere at de har gjennomført en tredjepartsverifisering av IKT-sikkerheten i sine produkter og tjenester.

Siden det kan være problematisk for Norge å innføre slike krav alene, bør norske myndigheter støtte opp under EU-initiativer for å innføre bindende minimumskrav på tilkoblede forbrukerprodukter. Dette kan blant annet skje gjennom nye bestemmelser som kan tilføyes radioutstyrsdirektivet (se under).

Tydeliggjøre tilsynsmyndighetenes roller (kapittel 5, 8)

Forbrukerrådet erfarte at forhandlere fortsatte å selge GPS-klokker for barn selv etter Datatilsynet fattet vedtak om at importørene ikke lenger fikk behandle personopplysninger på grunn av manglende IKT-sikkerhet i produktet. En årsak til utfordringer med tilsyn på feltet kan være en uklar rollefordeling mellom sektortilsyn for tilkoblede forbrukerprodukter. Vi støtter derfor utvalgets forslag om å tydeliggjøre rollefordelingen mellom Datatilsynet, Forbrukertilsynet, Direktoratet for Samfunnssikkerhet og Beredskap (DSB) og Nasjonal kommunikasjonsmyndighet (Nkom). Det bør legges til rette for dialog og tverrfaglig samarbeid mellom relevante sektortilsyn, ved å etablere en arena for informasjonsutveksling og kompetanseoverføring. Dette kan være en funksjon for det planlagte nasjonale IKT-sikkerhetssenteret. Tilsyn på feltet bør prioriteres.

Det er avgjørende at produkter som ikke oppfyller minstekrav for IKT-sikkerhet raskt og effektivt kan trekkes fra markedet. Forbrukere må også ha mulighet til å heve kjøp av produkter hvor det avdekkes alvorlige sikkerhetsmangler. Vi registrerer at NOUen anbefaler at DSB skal ha en sentral rolle. Dersom bindende minstekrav for IKT-sikkerhet innføres gjennom radioutstyrsdirektivet, er det mer aktuelt at Nkom har en ledende rolle.

Veiledning av bransjeaktører (kapittel 8)

Forbrukerrådet støtter utvalgets forslag om styrket veiledning av relevante bransjeaktører, inkludert forhandlere, importører, produsenter og utviklere av tilkoblede forbrukerprodukter.

Utvalget foreslår at myndigheter og bransjeaktører må samarbeide om en generell veiledning for å bistå aktørene. Forbrukerrådet erfarer at mange bransjeaktører på feltet, spesielt små og mellomstore bedrifter, etterlyser veiledning for hvordan de best kan ivareta IKT-sikkerheten i sine produkter.

Veiledning bør skje både gjennom kontaktpunkter og arenaer som f.eks. et nasjonalt IKT-sikkerhetssenter, og i form av retningslinjer som beskriver hvordan IKT-sikkerhet bør implementeres i ulike produkter og tjenester.[8] Slike

[8] Se for eksempel den britiske regjeringens retningslinjer for IKT-sikkerhet i tilkoblede forbrukerprodukter https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security og Trust by Design Guidelines fra

retningslinjer og veiledning verken kan eller skal erstatte regulatoriske grep, men er et supplement som kan bidra til å øke kompetansen blant bransjeaktører. Forbrukerrådet støtter derfor utvalgets forslag om styrket veiledning av bransjen.

Tilrettelegge for varsling av sårbarheter (kapittel 17)

Forbrukerrådet støtter utvalgets forslag om at varsling av sårbarheter og respons bør koordineres i et nasjonalt IKT-sikkerhetssenter. I dag er uavhengige sikkerhetsforskere og eksperter viktige i arbeidet med å avdekke sårbarheter i tilkoblede produkter og tjenester. Når feil oppdages, kan berørte aktører kontaktes gjennom en varslingsprosess (vulnerability disclosure), men det er vårt inntrykk at varslene håndteres svært ulikt av ulike aktører som varsles om sikkerhetshull.

Forbrukerrådet erfarer for øvrig at enkelte virksomheter ikke oppgir kontaktpunkt for å varsle om sårbarheter, eller de møter varslerne med trusler om politianmeldelse eller lignende. Dette kan føre til at varslere ikke står fram eller informerer om potensielt alvorlige sårbarheter eller hendelser. Derfor støtter vi utvalgets forslag om at håndtering av sårbarheter bør skje av det offentlige, for eksempel gjennom et nasjonalt IKT-sikkerhetssenter. Et slikt senter bør legge til rette for at varslere kan kontakte myndighetene på en standardisert måte, og sørge for at varsler blir formidlet til de berørte aktørene slik at sårbarheter kan behandles på en forsvarlig måte.

Offentlige anskaffelser (kapittel 16)

Det offentlige har en avgjørende rolle for å fremme robust IKT-sikkerhet, også i forbrukerprodukter. Offentlige institusjoner bør bruke sin posisjon som stor innkjøper av tjenester til å stille krav til IKT-sikkerheten. En rekke tilfeller har understreket viktigheten av at det offentlige tar IKT-sikkerhet på alvor. I et nylig eksempel fra Sverige, lå millioner av potensielt sensitive samtaler om helse åpent tilgjengelig på nett.[9] Situasjonen kunne vært avverget dersom det ble stilt IKT-sikkerhetskrav til underleverandører av tjenesten.

Consumers International: https://www.consumersinternational.org/media/239715/trust-by-design-guidelines.pdf

[9] https://www.digi.no/artikler/skal-vaere-den-storste-it-skandalen-i-svensk-historie/455294

Det offentlige kan på denne måten styrke konkurransekraften til aktører som tar IKT-sikkerhet på alvor. Forbrukerrådet støtter derfor utvalgets forslag om at IKT-sikkerhet bør inngå i anskaffelsesregelverket, og ivaretas gjennom statens standardavtaler.

Prosesser i EU

Cybersecurity Act

I desember 2018 ble det oppnådd politisk enighet i EU om et IKT-sikkerhetsdirektiv («Cybersecurity Act»).[10] Dette direktivet omhandler blant annet IKT-sikkerhet for tilkoblede produkter, og legger til rette for sertifiseringsordninger som vil være frivillige. Forbrukerrådet mener at frivillige ordninger ikke vil være tilstrekkelig for å skape insentiver til å ivareta IKT-sikkerheten. Markedet er fragmentert og med mange tilbydere som ikke har midler eller vilje til å sertifisere seg på den ene siden og forbrukere på den andre siden, som har store utfordringer med å skille gode fra dårlige produkter når det gjelder IKT-sikkerhet. I en slik situasjon er ikke frivillighet nok for å ivareta forbrukernes personvern og sikkerhet.

Radioutstyrsdirektivet

I februar 2019 lanserte EU-kommisjonen et veikart for å vedta den delegerte rettsakten i artikkel 3.3(e) og (f) i radioutstyrsdirektivet.[11] Denne artikkelen åpner for at radioutstyrsdirektivet kan anvendes på alle tilkoblede forbrukerprodukter, og at slike enheter må tilfredsstille minstekrav for personvern og IKT-sikkerhet. Dersom rettsakten vedtas, vil Nkom få norsk sektortilsyn i saker som omfatter IKT-sikkerhet i tilkoblede produkter. Dette kan gi grunnlag for å trekke produkter med sviktende IKT-sikkerhet fra markedet.

Forbrukerrådet anmoder norske myndigheter om å arbeide aktivt for at den delegerte rettsakten i artikkel 3.3(e) og (f) blir en realitet. Forbrukerrådet er engasjert i Kommisjonens høring om veikartet frem mot en delegert rettsakt gjennom den europeiske forbrukerparaplyorganisasjon BEUC, hvor vi er

[10] https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en
[11] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-6426936_en

medlem. BEUC anbefaler at Kommisjonen vedtar den delegerte rettsakten i form av «Option 4» som beskrevet i veikartet.[12] Det innebærer at leverandører av tilkoblede produkter må sørge for at deres produkter har på plass nødvendige egenskaper for å forhindre personvernbrudd og svindel.

I februar 2019 innførte islandske myndigheter salgsforbud for to GPS-klokker for barn på bakgrunn av europeisk produktsikkerhetsregelverk fordi IKT-sikkerheten var for dårlig. Én av klokkene ble registrert i det europeiske varslingssystemet RAPEX, som er en felles database for europeiske produktsikkerhetsmyndigheter. [13] Det betyr at myndigheter i andre land på dette grunnlaget kan gjøre tilsvarende vurderinger.

Dette er, så vidt Forbrukerrådet er kjent med, første gang produkter er trukket fra markedet på grunn av sviktende IKT-sikkerhet med hjemmel i produktsikkerhetsregelverk.

For øvrig vil den ovennevnte tilføyelsen av nye bestemmelser i radioutstyrsdirektivet utvide direktivets rekkevidde. Dersom den delegerte rettsakten vedtas som skissert under Option 4, vil europeiske tilsynsmyndigheter få hjemmel til å hindre at usikre tilkoblede forbrukerprodukter kommer på markedet. Endringen vil således legge til rette for en proaktiv i stedet for en reaktiv kontroll på IKT-sikkerhet.

Vennlig hilsen

Forbrukerrådet

[12] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-6426936/feedback/F239298_en?p_id=380959

[13] https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/?event=viewProduct&reference=A12/0157/19&lng=en

Gro Mette Moen

Fungerende fagdirektør digitale tjenester