

Direktoratet for Samfunnssikkerhet og beredskap

postmottak@dsb.no

Oslo 6.12.2016

Bekymringsmelding om svak brukersikkerhet i leker som kan kobles på nett – dukken Cayla og roboten i-Que

Forbrukerrådet sender med dette bekymringsmelding på to leker som kan kobles til internett via en app. Lekene det gjelder er dukken Cayla og roboten i-Que, som begge selges i Norge.

Forbrukerrådet har sett på vilkår knyttet til nedlasting og bruk av appene, og fått utført en teknisk test av lekene. Den tekniske testen er utført av konsultentselskapet Bouvet, og viser at dukken og roboten har for svak brukersikkerhet.

Se den vedlagte rapporten «*Analysis of consumer and privacy issues in three internet-connected toys*» (vedlegg 1), og den tekniske rapporten «*Investigation of privacy and security issues with smart toys*» (vedlegg 2) som gir en gjennomgang av funnene.

Forbrukerrådets klage til Datatilsynet og Forbrukerombudet på lekenes brukervilkår vedlegges til orientering (vedlegg 3).

Forbrukerrådet anmoder tilsynsmyndigheten om å se nærmere på vedlagte underlagsmateriale, og vurdere om produktsikkerhetsregelverk kan anvendes.

Bakgrunn

Stadig flere gjenstander kobles til internett. Dette skaper mange muligheter, samtidig som det forsterker og skaper nye forbrukerutfordringer.

Forbrukerrådet har i 2016 gjennomført et prosjekt der vi ser på forbrukerutfordringene ved tingenes internett. Vi har sett på brukervilkår og personvernerklæringer i utvalgte produktkategorier, samt gjennomført teknisk testing av produktene. En del av prosjektet om tingenes internett har vært å undersøke leker. Det finnes ikke i dag et stort utvalg av internettilkoblede leker, men det er trolig et marked i utvikling og ekspansjon. Forbrukerrådet er opptatt av at barn er en sårbar forbrukergruppe som har krav på et særskilt vern.

Produktene Cayla og i-Que

Lekene produseres av Genesis Toys, der vi ikke kan finne noen selskapsinformasjon på nettsiden, www.genesis-toys.com. Imidlertid lenker nettsiden til en personvernpolicy for Genesis der en



adresse i Hong-Kong er angitt.¹ Det er ulike importører av lekene i Europa, og det kan være flere importører av lekene til de enkelte land. Etter det vi kan finne ut, er Top Toy Norge AS (organisasjonsnummer 991 492 704) importør av lekene til Norge. Lekene selges i Norge bl.a. hos de store leketøyskjedene Toys R Us og BR Leker.

Antall nedlastinger av appen kan gi en viss indikasjon på lekenes utbredelse. Dukken Cayla synes å være mest populær, og etter det vi kan se er den norske appen lastet ned fra Google Play mellom 10 og 50 000 ganger.² Appen som tilhører roboten i-Que har ikke tilsvarende popularitet, med mellom 1 og 5 000 nedlastinger fra Google Play.³

Antall nedlastinger fra Apple App Store er ikke offentlig tilgjengelig. Det er likevel grunn til å tro at det ikke er færre nedlastinger enn fra Google Play.

Dukken Cayla har blitt kåret til årets leketøy både i Norge og Sverige i 2014 ifølge merking på emballasjen. Lekene markedsføres aktivt i årets julekataloger fra både Toys R Us og BR Leker. Lekene selges globalt.

Cayla og i-Que er interaktive leker som kobles til en app på en mobiltelefon eller et nettbrett via blåttann. I lekene er det plassert en blåttann-tilkoblet mikrofon og høyttaler, og det er i appen selve data-prosesseringen foregår. Når barnet stiller Cayla eller i-Que et spørsmål, oversetter appen det barnet sier til tekst og søker i en database for svar på spørsmålet. Hvis barnet stiller lekene et personlig spørsmål, som "Hva er din yndlingsfarge?" henter lekene svaret fra databasen uten å bruke internett. Hvis barnet spør lekene om noe som ikke er i databasen deres, bruker lekene internettjenestene Wikipedia og Weather Underground for å finne et svar.

Lekene har sikkerhetsmekanismer/programvare som automatisk sjekker ord fra en liste med blokkerte ord før den svarer. Hvis spørsmålet eller svaret inneholder et ord fra listen med blokkerte ord, vil lekene fortelle barnet at den ikke kan svare.

Tekniske funn

Konsulentselskapet Bouvet fikk i oppdrag av Forbrukerrådet å gjennomføre en teknisk test av lekene. Bouvet undersøkte ulike sider av lekenes teknologi, både i selve dukken, appen og datatrafikken mellom disse to, og mellom appen og internett. Det er spesielt to egenskaper ved lekene vi ønsker å fremheve i denne bekymringsmeldingen.

1. Enkel og usikret tilkobling

Når leken og telefon/nettbrett skal kobles sammen slås leken først på, deretter må telefonen/nettbrettet søke etter blåttannenheter. Lekene dukker raskt opp på telefonen/nettbrettet med navnene Cayla og i-Que og ved ett tastetrykk er telefonen/nettbrettet og leken koblet sammen.

¹ Genesis Industries 8/F, HK Spinners Industrial Building, 818 Cheung Shan Wan Road, Kowloon, HK

² <https://play.google.com/store/apps/details?id=com.toyquest.Cayla.no>

³ <https://play.google.com/store/apps/details?id=com.toyquest.iQue.no>



Det er ikke nødvendig å ha fysisk tilgang til lekene for å koble seg på leken. Så lenge lekene er slått på, og ikke koblet til en annen enhet, kan en hvilken som helst blåtann-enhet søke opp leken og koble seg opp mot denne. Ved å benytte to telefoner kan leken brukes for å komme i kontakt med og kommunisere med barnet. Det kan være relativt stor avstand mellom leken/barnet og telefonene som benyttes for å oppnå kontakt.

Denne enkle og usikre tilkoblingen utgjør etter Forbrukerrådets vurdering en sikkerhetsrisiko. Denne sikkerhetsrisikoen kunne enkelt vært unngått ved at lekene har sikkerhetstiltak ved oppkobling. Sikkerhetstiltak kan være for eksempel at man må ha fysisk tilgang til leken før man kan koble til. Dette kan være en fysisk knapp på leken som må holdes inne under paring med en ny enhet, eller at brukeren må angi et passord når den skal kobles sammen med en ny enhet. Et slikt passord kunne for eksempel vært festet på selve leken. Slike metoder blir ofte brukt på andre tilkoblede produkter, for eksempel på aktivitetsarmbånd.

2. Sikkerhet i fysiske komponenter

Både I-Que og Cayla inneholder et tilpasset kretskort med en blåtann-modul basert på chip IS1685S fra ISSC. Blåtannmodulen i Cayla støtter Bluetooth 2.1 Secure Simple Pairing. I den tekniske rapporten utarbeidet av Bouvet fremhever de følgende fra en blåtann-ekspertgruppe, som spesifiserer at denne modulen er «*useful whenever product implementers want to make the user experience easier and have accepted the increased risk of security attacks.*»

Forbrukerrådet anser det derfor som sannsynlig at produsenten har vektet hensynet til brukervennlighet tyngre enn sikkerhetsaspektet.

Forbrukerrådet mener det er ekstra alvorlig at den svake brukersikkerheten har vært påpekt tidligere. Allerede i januar 2015 var dette en av flere brister offentliggjort av BBC, der en sikkerhetsekspert tok kontroll over Cayla og kunne påvirke hva hun sa.⁴ Produsentens tilbakemelding var at de skulle oppgradere appen. På tross av denne lovnaden finner vi i vår teknisk test at brukersikkerheten fortsatt er like svak. Vi tillater oss å bemerke at den fysiske brikken benyttet i Cayla har for svak sikkerhet, og at en oppdatering av appen neppe vil være tilstrekkelig.

Mulige konsekvenser av den svake brukersikkerheten

Ved bruk av en enkelt smarttelefon, kan hvem som helst koble seg til lekene og spille av lyd gjennom leken. Dette tillater for eksempel at uvedkommende kan spille av skremmende eller upassende lydklipp, som kan påføre barn stress og uhygge. Dersom det brukes to telefoner, kan den ene kobles til leken, og den andre telefonen brukes til å ringe opp den første telefonen. Da kan man både snakke og lytte gjennom leken, som om det var et vanlig blåtann-headset. Det betyr at lekene kan brukes til romavlytting, eller til å kommunisere direkte med barnet.

I verste fall kan uvedkommende dermed snakke med barn gjennom leken. Bruken av blåtann - navnene «Top Toy Cayla» og «I-Que Robot» gjør det også enkelt å finne usikrede enheter i f.eks. et

⁴ <http://www.bbc.com/news/technology-31059893>



nabolag. I denne sammenheng finner vi grunn til å trekke frem at Cayla markedsføres som «din nye bestevenn», og dermed kan den svake brukersikkerheten fremstå som et særlig alvorlig tillitsbrudd.

Man kan sikre seg mot at uvedkommende kobler seg på Cayla ved alltid å skru av dukken etter bruk, eller å ha dukken koblet til en annen enhet hele tiden. Det er grunn til å tro at telefonen/nettbrettet som brukes med leken ofte vil kobles av ved å være utenfor rekkevidde (f.eks. ved at foreldre tar med telefonen sin ut av hjemmet), og at små barn ikke tenker på å skru av lekene etter bruk. Dermed vil sårbarheten kunne være tilgjengelig for misbruk i mange situasjoner.

Det er særlig foruroligende at produkter rettet mot barn bruker kommunikasjon som blåtann uten sikkerhetstiltak som forhindrer uvedkommende fra å koble seg på leken.

Forbrukerrådets europeiske paraplyorganisasjon, BEUC vil henvende seg til EU- kommisjonens Expert Group on Toy Safety med et ønske om å få presentere Forbrukerrådets funn i de to nevnte rapportene.

Vi anmoder DSB om å undersøke om produktsikkerhetsregelverket kan anvendes i et tilfelle som beskrevet i denne bekymringsmeldingen, og som har den ekstra dimensjonen at det gjelder barn.

Vennlig hilsen
Forbrukerrådet

Randi Flesland
Direktør
Forbrukerrådet

Finn Myrstad
Fagdirektør Digitale tjenester
Finn.myrstad@forbrukerradet.no

Vedlegg 1: «*Analysis of consumer and privacy issues in three internet-connected toys*»

Vedlegg 2: «*Investigation of privacy and security issues with smart toys*»

Vedlegg 3: *Klage til Datatilsynet og Forbrukerombudet på lekenes brukervilkår*