Tidsskriftet
DEN NORSKE LEGEFORENING

Mitt liv som kyborg

GJESTESKRIBENT

MARIE MOE

E-post: marie.moe@sintef.no
Ph.d., seniorforsker
Forskningsleder Informasjonssikkerhet
SINTEF

Hvordan møter helsevesenet en pasient som spør: «Hvor datasikkert er mitt medisinske implantat?»

Foto: Chris Guldberg

Jeg har stor respekt for legeyrket som profesjon. Når jeg går til legen, stoler jeg på at han eller hun vet mer enn hva jeg selv kan google meg frem til av informasjon. Jeg er doktor i datasikkerhet, men rekker selvsagt ikke opp hånden når flybesetningen spør etter «doctor on board» over høyttaleranlegget.

Omtrent halvveis i livet har jeg hatt mange møter med helsevesenet, som pårørende, gravid, fødende og syk med «vanlige» sykdommer. Stort sett har dette vært positive erfaringer. Ingenting kunne likevel forberede meg på hvordan det ville føles å bli en kyborg – få høyteknologi operert inn i kroppen og havne i en posisjon hvor jeg har mye mer kunnskap om teknologien inne i meg enn det helsepersonellet har.

En høstmorgen i 2011 tok hjertet mitt en liten pause. Jeg kom til meg selv liggende på gulvet, forvirret og med en vond kul i bakhodet. Rundt meg lå skår fra glasset med appelsinjuice som jeg hadde drukket av før alt plutselig ble svart. På legevakten ble det konstatert hjerterytmeforstyrrelser, og jeg ble lagt inn til overvåkning. Etter noen dager fikk jeg diagnosen tredjegrads atrioventrikulær blokk og fikk implantert en pacemaker.

Det ble starten på mitt liv som kyborg.

Som sikkerhetsforsker hadde jeg mange ubesvarte spørsmål om datamaskinen i min egen kropp, som nå kontrollerte hvert hjerteslag. Spørsmålene gjorde helsepersonellet svar skyldig. De fleste jeg snakket med, hadde ikke engang tenkt over at pacemakeren var kontrollert av programvare og at eventuelle sårbarheter i koden kunne åpne for cyberangrep.

Jeg forsøkte å finne svar i manualen for pacemakeren min, men satt igjen med enda flere spørsmål. Samt en stor overraskelse.

Jeg fant nemlig ut at min pacemaker hadde en innebygd funksjonalitet for «hjemmemonitorering». Det vil si at pacemakeren min kan kobles til internett. Ikke via vanlig wifi, men via et modem som kan kommunisere trådløst med implantatet på flere meters avstand. Tilkoblingen skal i utgangspunktet være enveis, det vil si at man kun kan hente ut informasjon fra pacemakeren, ikke endre på innstillingene eller skru den av og på.

Internettkoblingen gjorde meg likevel bekymret. Jeg vet nemlig av erfaring at det å legge til internettkoblinger på tradisjonelt lukkede systemer medfører økt eksponering av sikkerhetshull som kan utnyttes i cyberangrep.

Sikkerhetshull finnes i all programvare, fordi de som designer systemet eller skriver koden gjør feil. Kodegjennomgang og testing brukes for å luke ut de fleste feil før produktet tas i bruk. Men feil må likevel ofte fikses i ettertid. Vi kjenner alle til hyppigheten av oppdateringer på de fleste nettilkoblede dingser vi omgir oss med.

Selv fikk jeg også føle på kroppen hvordan det var å bli offer for en feil i koden som styrer pacemakeren. Like etter inngrepet opplevde jeg at noe var galt når pulsen min ble høy. Jeg kunne ikke trene eller anstrenge meg som før. Det viste seg at pacemakeren var feilkonfigurert.

Makspulsen var blitt innstilt på 160 slag i minuttet. Kanskje greit for en på 80 år, men det fungerte ikke for meg. Da jeg sa at jeg følte meg utslitt av å gå opp trapper eller løpe etter bussen, ble jeg først ikke trodd av legen. For verdien som sto på skjermen på pacemakerprogrammereren var en helt annen enn 160. Det viste seg at det var en regnefeil i programmereren. Dette ble oppdaget under en belastningstest på sykkel tre måneder etter at jeg første gang hadde klaget på problemet.

Jeg kunne altså ikke stole på koden som styrte hjertet mitt. Siden jeg har spesialkunnskap om programvaresikkerhet, ønsket jeg å gjøre en kodegjennomgang for å sjekke hvordan sikkerheten var implementert. Men det var umulig å få tilgang til koden. Produsenten brukte ikke åpen kildekode, og kommunikasjonsprotokollene var ikke basert på åpne standarder. Jeg startet derfor et hackingprosjekt – på mitt eget hjerte.

Så langt kjenner vi heldigvis ingen tilfeller der ondsinnede aktører har hacket medisinske implantater. Men sikkerhetsforskere, også vi i SINTEF, har funnet sårbarheter. Mitt eget forsøk er blant dem som har demonstrert at hacking er mulig. Mangel på bevissthet rundt problematikken gjør at hundretusenvis av pasienter lever med implantater som er sårbare for hacking.

Det er på tide at pasienter og helsepersonell blir bevisst på risikoen, stiller krav om sikkerhet og kan ta et informert valg når det gjelder type implantat og eventuell nettverkstilkobling. Ville du hatt hjertet ditt tilgjengelig på internett? Hva ville du svart en pasient som lurer på om han eller hun kan hackes?

Publisert: 23. august 2017. Tidsskr Nor Legeforen. DOI: 10.4045/tidsskr.17.0658