TINGENES INTERNETT

Et gode, men også en trussel for nasjonen

Rammet også Norge: Et verdensomspennende dataangrep startet 13. mai. Britiske sykehus, Renault, Deutsche Bahn og en rekke russiske og kinesiske institusjoner var blant dem som mistet tilgang til datafiler.

DEBATT KYBERRISIKO

KETIL STØLEN
Sjefsforsker ved SINTEF,
professor II ved universitetet i Oslo

Intervjuer av 110 sikkerhetseksperter fra Asia og Europa utført av Radar Services identifiserte "angrep i kontekst av tingenes internett" som største sikkerhetstrussel i 2025. Det er en oppfatning jeg deler. Uten nasjonal regulering og kontroll vil vår sårbarhet med hensyn til terrorisme, sabotasje og krigslignende angrep på nasjonal infrastruktur øke dramatisk. Nasjonale aktiva som infrastruktur for strøm, helse, telekom, transport, beredskap etc. må, som jeg ser det, beskyttes, kontrolleres og driftes innenfor landets grenser på en slik måte at angrepsflaten og uvisshet relatert til avhengigheter reduseres til et håndterbart nivå.

Tingenes internett eksisterer alt i dag, men kun i en prematur tilstand. Tingenes internett er egentlig som vanlig internett, rent bortsett fra at det er skreddersydd for kommunikasjon mellom oss og tingene rundt oss, og ikke minst automatisk interaksjon mellom tingene selv. I dag er kun et fåtall av tingene som vi gjør bruk av på nettet, og interaksjonen er i hovedsak manuell. For eksempel, når vi skrur på varmen på hytta via internett kommuniserer vi manuelt med en ovn. I fremtiden vil de fleste menneskeskapte ting være tilgjengelig på nettet, og kommunikasjonen vil i stor grad skje automatisk og intelligent. Med hensyn til hytteeksemplet over vil det kanskje være bilen vi kjører som skrur på varmen på hytta når bilen skjønner at det er dit vi skal.

Fra et sikkerhetsperspektiv er tingenes internett svært utfordrende. Problemet kan oppsummeres som følger:

- ***Kolossal angrepsflate:*** I og med at alt fornettes og potensielt kan nås fra overalt i verden, oppstår en kolossal angrepsflate. Satt på spissen, en strømmast som tidligere kun kunne hogges ned eller sprenges, kan i fremtiden i verste fall settes ut av drift elektronisk fra den andre siden av kloden.
- ***Utilstrekkelig teknologi:*** IT-leverandørene kappes om å tilby nye plattformer for tingenes internett. På verdensbasis finnes alt i dag mer enn 400 slike plattformer. På toppen av disse lite testede og ofte umodne produktene, integreres så tingene – ting som i stor grad er bygget og designet for en helt annen bruk, et helt annet sikkerhetsbehov, og som det er vanskelig å sikre på grunn av svært liten batterikapasitet, beregningskraft og/eller hukommelse.

Tingenes internett vil utvilsomt lette mange gjøremål i vårt daglige virke, men det vil også forenkle livet til for eksempel terrorister. Det vil ikke lenger være nødvendig å kapre en lastebil eller et fly fysisk, eller å sprenge seg selv i lufta. Det holder å skaffe seg elektronisk tilgang til for eksempel tunnelbanen i en storby og derigjennom utløse en katastrofal hendelse. Statoil-skandalen i fjor høst hvor en IT-arbeider i India stanset produksjonen på Mongstad på grunn av en tastefeil, og Nødnett-skandalen fra i år hvor det fremgikk at det norske Nødnettet i lengre tid hadde blitt driftet fra India av indiske it-arbeidere uten sikkerhetsklarering, viser at det å skaffe seg tilgang til viktige nasjonale verdier er alt annet enn fremtidsutopi.

I disse tilfellene var det snakk om feil og ikke ondsinnede angrep, men eksemplene illustrerer hva vi har i vente hvis myndighetene ikke tar grep.

Dette er selvsagt ikke et problem spesifikt for Norge som nasjon. US Department of Energy registrerte for eksempel ifølge USA Today hele 150 suksessfulle cyberangrep (omtalt som "sucessfull compromises") over en 48 måneders periode frem til oktober 2014, og det finnes tilsvarende eksempler og tall fra andre land. Men problemene knyttet til sikring av våre nasjonale aktiva må løses i Norge og av norske myndigheter, og ikke av kommersielle/halvkommersielle selskaper som uten å blunke prioriterer økonomi fremfor nasjonal sikkerhet. ●

Intelligent armering i Revit

ISY CAD

NTI CADcenter: post@nticad.no | 480 03 300
Cad-Q: jan.tore.bugge@cad-q.no | 916 38 558 | isy.no

Norconsult Informasjonssystemer

Forutsigbar sluttkostnad