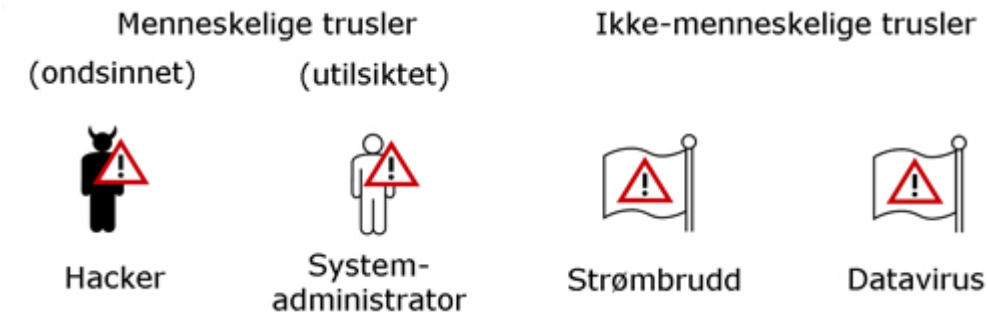
Avslører datatrusler i norske bedrifter

Norske IKT-forskere har forbedret metodene for å foreta risikoanalyser av datasystemer.

Gode risikoanalyser er vesentlig for å sikre bedrifters datasystem mot sikkerhetstrusler. Typiske sikkerhetstrusler kan være hackere, det vil si uvedkommende som med hensikt prøver å komme seg inn i datasystemene, strømbrudd eller datavirus (se figur).

Også ansatte i bedrifter kan utilsiktet gjøre noe som gjør at systemet blir usikkert. Det kan for eksempel være at de ikke følger rutinene for valg av passord og skifte av passord.



Eksempel på diagramsymboler som beskriver trusler. Symbolene skal gjøre det lett for bedriftene å forstå risikobildet. (Figur: SINTEF)

– Informasjonssikkerhet handler blant annet om at informasjon, slik som kundelister, passord og børsinformasjon, ikke må komme på avveie, sier professor Ketil Stølen ved SINTEF IKT.

– Dessuten må ingen, slik som et virus, kunne forandre informasjonen før den når fram til dem som skal ha den, og dataene og tjenestene må være tilgjengelige når noen trenger dem. Bedriftene må for eksempel ha tilgang på strøm, og leger må få tilgang på de dataene de trenger når de skal behandle deg.

Stølen viser til flere eksempler de siste par årene der informasjonssikkerheten har vært for dårlig. I fjor høst var nettet ved Akershus universitetssykehus HF nede i flerfoldige timer med den konsekvens at elektroniske pasientjournaler og telefonsystemet ikke var tilgjengelig.

Året før hadde vi datainnbrudd i regjeringens datanettverk der det ble stjålet dokumenter, og i fjor sommer ble det avdekket at datasystemet ved et stort vannanlegg i Oslo var dårlig sikret mot uvedkommende.

Fra analyse til håndtering
Risikoanalyser er viktig for informasjonssikkerheten innen de fleste samfunnsområder som strømforsyning, bankvesen, helsevesen, telekommunikasjon, offshore og for industribedrifter.

Basert på en risikoanalyse og risikobildet bedriften får fra den, kan den foreta en risikohåndtering for å bedre sikkerheten. Hvorvidt en risiko er høy eller lav, er en kombinasjon av sannsynligheten for at noe skjer kombinert med konsekvensen av at det skjer.

– Å gjøre en risikoanalyse er det samme som legene gjør før de behandler oss. De vurderer hva som feiler oss, før de bestemmer hvilken behandling vi trenger, forklarer Stølen.

– Tilsvarende må vi først stille diagnose på datasystemene vi jobber med for å vite hva som må «behandles» for å ivareta sikkerheten, sier Stølen som har ledet et forskningsprosjekt som har hatt støtte fra Forskningsrådets program VERDIKT.

Nytt modelleringsverktøy
Forskerne har laget en ny metode og et nytt dataprogram som kan brukes til å forutsi hvilken effekt endringer i et datasystem har på informasjonssikkerheten. Det kan for eksempel være endringer som gjøres for å tilpasse systemet til nye arbeidsprosesser.

– En mulighet er å implementere endringene og se hva som skjer, men det blir dyrt. Et alternativ er å predikere hva som blir effekten ved å modellere på datamaskinen slik vi har gjort, sier Stølen.

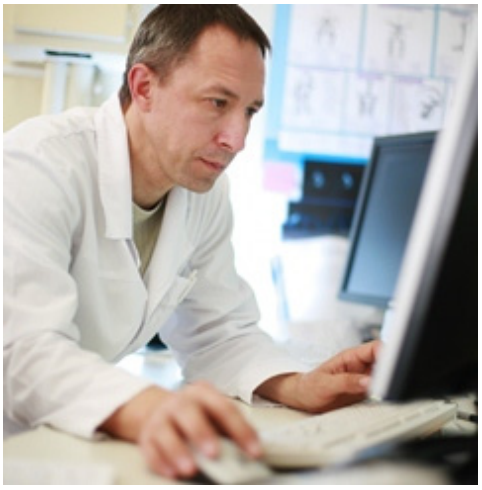
Ved hjelp av modellering ser forskerne hvilken effekt planlagte endringer har på kvaliteten til ulike deler av datasystemet med hensyn til blant annet sikkerhet, tilgjengelighet og brukervennlighet.

Analyse av komplekse systemer

En utfordring i dag er å utføre risikoanalyser for komplekse systemer der ulike prosesser eller systemer er gjensidig avhengig av hverandre. Dette gjelder for eksempel strømnettet der det er gjensidig avhengighet mellom ulike land.

– Hemmeligheten er å dele systemet opp i biter, kalkulere risikoen for hver enkelt bit og så sette det sammen igjen, forteller Stølen.

Han sier at metodikken herfra også kan brukes når et stort selskap som har fått utført for eksempel femten analyser over tre år, ønsker å danne seg et overordnet bilde av risikonivået. Dette har det hittil ikke funnes gode metoder for.


Helsevesenet kan rammes hardt av dårlig informasjonssikkerhet.

Tillitsforhandlinger
Forskerne har sett på hvordan datasystemene utfører tillitsliknende forhandlinger med hverandre.

Da vurderer datasystemene hvor mye informasjon de kan gi til hverandre basert på policydokumenter. Skal for eksempel ansatte kunne logge seg på hjemmefra og få tilgang til å utlevere data derfra?

– Det er det samme som skjer når vi bruker nettbanken. Vi gir informasjon som personnummer, pinkode og passord i flere trinn for å få tilgang til tjenesten. Da er det en tillitsforhandling mellom vår datamaskin og bankens, forklarer Stølen.

Ketil Stølen og hans forskningsgruppe. Bak fra venstre: Atle Refsdal, Fredrik Seehusen, Ketil Stølen og Olav Ligaarden. Framme fra venstre: Aida Omerovic, Mass Soldal Lund og Bjørnar Solhaug (Foto: Norunn K. Torheim)

Stemmer risikobildet?
Nå ønsker forskerne å forbedre metodene for risikoanalyse ytterligere. De vil finne ut hvordan de kan teste om risikobildet de har kommet fram til i risikoanalysen, stemmer.

– Risikobildet dannes ut fra intervjuer med bedriftenes eksperter på feltet og historiske data, slik som datalogger. Vi må imidlertid sjekke om risikobildet stemmer, forteller Stølen.

– Det gjør vi ved å triangulere, det vil si å prøve å måle det samme med ulike metoder for å se om vi får samme resultat. Når noen for eksempel sier at det er mulig å skaffe seg ekstern tilgang til en intern server, kan vi gå inn og undersøke dette nærmere ved hjelp av såkalt penetrasjonstesting eller ved å studere bedriftens datalogger.

FAKTA

Prosjektet «Digital Interoperability with Trust – DIGIT» har hatt støtte fra VERDIKT i Forskningsrådet fra 1.1.2007 til 30.4.2012.

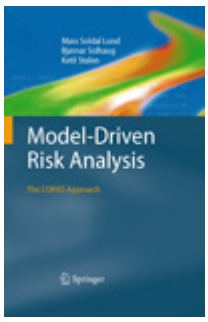
Professor Ketil Stølen ved SINTEF IKT og Universitetet i Oslo har vært prosjektleder.

Samarbeidspartnere: Statnett SF, Santander Consumer Bank AS og Det Norske Veritas AS.

SINTEFs forskning på risikoanalyser har resultert i en bok der de presenterer en åttetrinns modell for risikoanalyse – CORAS.

De har utviklet standardiserte diagrammer med egne symboler for å framstille trusselscenarioer på en måte som gjør det lett for bedriftene å forstå trusselbildet. I boka gir forskerne en rekke eksempler på bruk av modellen slik

FAKTA



Boka om SINTEFs modell for risikoanalyse – CORAS (Illustrasjon: Springer-Verlag)

at det skal være lett for andre risikoanalytikere å ta den i bruk.

Les om boka her (deler er også tilgjengelig på nett).

Skrevet av: Norunn K. Torheim

Publisert: 18.06.2012
Sist oppdatert: 05.09.2012