Vi er det svakeste leddet i datasikkerheten

Vanlige folk vil være en større sikkerhetstrussel enn hackerangrep og sikkerhetshull også i fremtiden.

Steffen Pedersen Øberg
journalist

Tirsdag 05. mars 2013
kl. 05:00

Internettet og dets muligheter vokser i rasende hastighet, det stiller krav til utviklingen av sikkerhetssystemer.
(Bilde: Fra videoen Bildet av en tanke, Per Byhring, forskning.no)

De siste månedene har stadig nyoppdagede sikkerhetshull i programmeringsspråket Java skapt hodebry for brukere av nettbanker og andre tjenester verden over.

Men spam-eposter, Nigeria-brev og mail som later som om de kommer fra banken eller skattekontoret forsøker ikke bare å lure datamaskinen og søppel-epost-filteret ditt - de prøver å lure deg.

– Senest i dag fikk vi phishing-mail som utga seg for å være fra banker og kortleverandører og som ba oss registrere sensitive detaljer hos dem, sier Chunming Rong, professor ved institutt for data- og elektronikkteknikk ved Universitetet i Stavanger.

Han mener at selv om bygging av sikre systemer kommer i første rekke, hjelper supersikre datasystemer lite hvis menneskene ikke bruker dem riktig.

– Selv om vi har mekanisk sikkerhet, kan problemet ligge et helt annet sted. Det viktigste er å gjøre kunnskapen om hvor sårbare vi er på nett til allmenn kunnskap. Dette må formidles til vanlige brukere, fortsetter han.

Sunn fornuft fortsatt viktigst

Sunn folkeskikk og bevissthet er fortsatt forbrukernes viktigste forsvar mot nettkjeltringer.

– For den vanlige forbruker som tar grunnleggende forhåndsregler som gode passord, følger vanlige anbefalinger med henhold til sikkerhetsmur og antivirus, har en kritisk sans til mail og liknende, så er trusselen etter min mening liten.

Det forteller Ketil Stølen, sjefsforsker ved SINTEF IKT og professor ved instituttet for informatikk ved Universitetet i Oslo.

– Det betyr ikke at noen ikke kan skade deg via dine dataløsninger hvis de virkelig ønsker det og har de

nødvendige ressurser, men slik er det også for alt annet i samfunnet, fortsetter han, og legger til at vi i det daglige liv hele tiden gjør risikovurderinger og at løsningen er å bruke sunn fornuft enten det gjelder IT eller noe annet.


Sjefsforsker Ketil Stølen. (Foto: Sintef)

Flere utfordringer

Det er mer til datasikkerhet enn å stoppe hackerne fra å ta tingene dine. I et samfunn som i økende grad virtualiseres oppstår nye utfordringer og krav til sikring. Ett eksempel på en slik ny utfordring er det Stølen kaller gråsoneproblematikk.

– En stor del av sikkerhetsforskning inntil i dag har vært farget av en overdreven svart-hvit tenkning: enten er noe helt sikkert eller så er det usikkert. Med andre
ord, fokus har vært på absolutt sikkerhet i den grad det kan sies å eksistere, forklarer han.

- Les også: **Digital tillit**

– Vi som bedriver anvendt sikkerhetsforskning vet imidlertid at det er gråsonen mellom det sikre og det usikre som er det interessante. Hva vil det si at noe er sikkert nok, og hva vil det si at vi kan stole på noen når dette "noen" er et datasystem. Automatisert- og gjerne sanntidsstøtte for å håndtere gråsoneproblematikk er, som jeg ser det, en av de viktigste utfordringene i årene som kommer for forskningen innen datasikkerhet, sier Stølen.

Juridisk gap

Men også utenfor IT-verdenen finner en utfordringer til forbrukernes datasikkerhet. En helt annen problemstilling forskere og utviklere i økende grad tar stilling til er det Chunming Rong kaller *accountability*.


Professor Chunming Rong er en ledende ekspert innen "Cloud Computing" - programmering i nettskyer. Universitetet i Stavanger

– Det handler om at når bedrifter gjør en handling, eller tilbyr en tjeneste, må de kunne stå til ansvar for det, forklarer han.

Flere bedrifter som tilbyr tjenester på nettet bruker ikke sin egen infrastruktur. Et eksempel på dette er den skybaserte lagringstjenesten Dropbox, hvor brukerne kan laste opp data og lagre det i den digitale «skyen».

Dropbox sin infrastruktur tilhører egentlig Amazon. Et annet eksempel er nettbankene som bruker BankID som innloggingssystem. Felles for dem er at de tilbyr tjenester som egentlig er levert av underleverandører.

– Da kan man risikere at forbrukerens inntrykk ikke stemmer overens med bedriftens kontrakt, sier Rong.

Hvis det skjer noe med dataene dine hos en tjeneste som tilbyr lagringsplass, kan det vise seg at det ikke er tilbyderen selv som står ansvarlig, men en underleverandør. Dette skaper problemer når konsekvensene skal utredes.

– *Er det et gap mellom den teknologiske utviklingen og det juridiske?*

– Ja. Men nå har man advokater som jobber spesielt opp mot det å tolke det juridiske. Når en kontrakt er ferdig tegnet går de gjennom og sertifiserer det som står.

Skybaserte bedrifter

Rong forteller også at det er de skybaserte tjenestene som utgjør den største trusselen mot forbrukerne rent teknisk. Mens det før i hovedsak var private som brukte skybaserte tjenester begynner i dag bedriftene å benytte seg av tilbudene. Dette stiller sterkere krav til sikringen.

- Les også: **Sikkerheten kan forsvinne i skyene**

– Mer og mer data er tilgjengelig i skybaserte tjenester. Det er viktig at disse dataene er kryptert. Nå

har man ikke en god kontroll over hvem som kan komme inn å se og ta data som du har lagret. Per i dag er det bare et brukernavn og et passord som står mellom eventuelle kriminelle og dataene, forteller han.

Dynamisk trusselbilde

Vurderingen av skybaserte tjenester som den største trusselen skyldes at disse tjenestene er på full fart inn i våre dagligliv. Teknologien er ikke bare i vinden, den er også ny.

Farene som lurer på nettet forandrer seg i samsvar utviklingen. Og ettersom teknologien utvikler seg og skaper nye mål for hackerne, utvikler også sikkerheten seg.

Google skriver på sin blogg om avanserte algoritmer som kan oppdage mistenkelige forhold ved innlogging, selv om noen bruker riktig brukernavn og passord.

– Hvis en innlogging er vurdert som mistenkelig av en eller annen grunn – kanskje den kommer fra et land langt fra din siste innlogging – stiller vi noen enkle spørsmål om din konto. Det kan for eksempel være at vi spør etter telefonnummeret som hører til din konto, eller et sikkerhetsspørsmål, skriver de på bloggen.

Også nettbanken din benytter seg av flere steg for å sikre at riktig person logger seg inn. Selv om en tyv har fått fatt i passordet ditt, kommer han seg ingen vei uten kodebrikken og vice versa.

For at nettbanken din skal være i fare må kjeltringen altså stjele både det virtuelle passordet og den fysiske kodebrikken. At en eventuell skurk skal bruke så mye tid og ressurser på akkurat deg er lite sannsynlig. Ketil Stølen setter det i perspektiv:

– Det er helt klart at svaret avhenger av hvem og hva man er. Trusselen mot datasikkerhet for en enkelt forbruker er helt annerledes enn trusselen mot en bedrift som igjen er helt annerledes enn trusselen mot for eksempel en nasjon, sier han.