Nasjonal sikkerhetsmyndighet

Hovedpunkter fra NSMs årlige Rapport om sikkerhetstilstanden

Rapport om sikkerhetstilstanden er en årlig (sikkerhetsgradert) rapport som distribueres til en rekke offentlige myndigheter og en del private virksomheter.

Gjennom Rapport om sikkerhetstilstanden i 2007 beskriver NSM viktige sider av risikobildet og redegjør for sikkerhetstilstanden. Basert på risikobildet og sikkerhetstilstanden gir NSM anbefalinger som har til formål å bedre det forebyggende sikkerhetsarbeidet for de som er underlagt sikkerhetsloven, eiere av samfunnskritisk IKT-infrastruktur og andre. Dette dokumentet er en forkortet og ugradert versjon beregnet for alminnelig offentliggjøring.

Forord

Sikkerhet er et lederansvar på linje med alle andre forhold i en virksomhet. Erfaring fra tilsyn med etterlevelse av sikkerhetslovgivningen viser at sikkerheten som regel er god i virksomheter der arbeidet er solid lederforankret og gjennomføres på en systematisk måte. Der dette ikke er tilfelle, blir resultatet med hensyn til sikkerhet oftest noe tilfeldig og personavhengig. Systematisk bevisstgjøring av virksomhetsledelsen er helt nødvendig for å lykkes i sikkerhetsarbeidet.

Såkalte "nettsamfunn" er i rask utvikling på Internett. I den siste tiden har det blitt klart at slike samfunn også kan brukes til uønskede markedsføringsformål og at personvernet ikke er det beste. I verste fall kan tjenesten misbrukes av kriminelle elementer eller av fremmed etterretning.

Det tilbys i økende grad offentlig tilgjengelige tjenester som integrerer kart, satellitt- og luftfotografi med andre bilder og plantegninger. Denne teknologien er til stor hjelp ved samfunnsplanlegging blant annet for nødetatene. Imidlertid er det en risiko for at noe av den informasjonen som gjøres tilgjengelig kan være av sensitiv karakter. Utviklingen går her så raskt at den utfordrer samfunnets sikkerhetsbehov.

IKT-samfunnet krever tverrsektorielle og helhetsbaserte løsninger. Samvirke og samarbeid er nødvendig, men også samordning, standardisering og i noen tilfeller sentralisering. Særlig viktig er etablering av et helhetlig risikobilde og gode systemer for krisehåndtering.

Forebyggende sikkerhetstjeneste i henhold til sikkerhetsloven skal gi samfunnet en defensiv grunnsikring mot spionasje, sabotasje og terrorhandlinger. Summen av egensikringen i de enkelte virksomheter utgjør en viktig del av samfunnets samlede grunnsikring mot dette. Enhver virksomhet har et ansvar for å ha ulike sikkerhetstiltak for egenbeskyttelse mot etterretningsvirksomhet og mulige anslag mot virksomheten. PST fastsetter det nasjonale trusselnivået med hensyn til dette og utarbeider utfyllende trusselvurderinger. Det vises til PST for informasjon om dette.

1 Trusselbildet med hensyn til Internett-aktivitet

1.1 Trusler og trender

1.1.1 Botnet

Et *Botnet*[1] er et nettverk av infiserte datamaskiner som kontrolleres skjult via Internett. Disse infiserte maskinene fjernstyres og kan for eksempel gis kommandoer om å angripe andre maskiner som er tilkoblet Internett. Botnet er i dag det vanligste verktøyet for å gjennomføre et tjenestenektangrep. Et botnet utgjør en stor ressurs, med enorm kapasitet til å utføre distribuerte oppgaver. I 2007 har det vokst frem et stort botnet som har mekanismer som detekterer forsøk på kartlegging av maskiner i botnettet, og botnettet kan deretter automatisk kommandere deler av botnettet til å angripe vedkommende maskin. En slik selvforsvarsmekanisme har ikke tidligere blitt observert i et botnet. I tillegg til tjenestenektangrep brukes dette nettverket (kalt ”Storm”) blant annet til å sende ut store mengder e-post (spam). Dette er en av de økonomiske inntektskildene til bakmennene. De kan også skaffe seg inntekter ved å leie ut deler av nettverket, eller ved å ta på seg oppdrag om å bruke Storm som et offensivt våpen.

1.1.2 Trojanere

En *trojaner* er ondsinnet programvare som smugles inn i offer-maskinen under dekke av å være en ufarlig komponent, epost-sending, word-dokument, eller lignende. Programmene benyttes senere til å utføre skjulte handlinger på systemet de infiserer. Trojanere blir ofte benyttet til å stjele sensitiv informasjon. Målrettede trojanere rammer som regel en liten og klart definert målgruppe. De er designet for å stjele sensitiv informasjon. Antivirus- og brannmurprodukter gir begrenset beskyttelse mot trojanere. Samtidig har trojaneren som regel tilgang til alle ressurser som brukeren har rettigheter til.

1.1.3 SCADA-systemer

SCADA-systemer[2] er betegnelse på store datasystemer som benyttes for styring og prosesskontroll i stadig større deler av industrien. De binder sammen store, sentrale driftssentraler med de enkelte delene av de prosessene som skal styres.

Tradisjonelt har SCADA-systemene vært isolerte datasystemer, uten tilkopling til eksterne nettverk. Den eneste måten å utføre et anslag mot disse var ved fysisk tilgang. I de senere årene har imidlertid systemene blitt koblet sammen med bedriftenes øvrige datanettverk, samt direkte til Internett. Dette gjør systemene vesentlig mer sårbare, ved at det kan være mulig å ta kontroll over dem via nettverkene. Det finnes eksempler på at disse systemene er blitt utsatt for angrep og trusler fra aktører i Internettverdenen. Systemer som er tilknyttet kritisk infrastruktur har blitt eksponert for virus og hackerangrep. Det er ikke usannsynlig at det kan gjennomføres terrorangrep via Internett mot SCADA-systemer, eksempelvis i kombinasjon med fysiske angrep.

1.1.4 Undergrunnsøkonomi

Det er mange som tjener penger på ondsinnet programvare. Det finnes aktører som utvikler og selger programvare, og aktører som kjøper ferdigutviklet programvare for å benytte denne til økonomisk vinning. Utviklerne bak ondsinnet programvare utnytter gjerne resultater fra IT-sikkerhetsforskning på sårbarheter i applikasjoner og operativsystemer. Det er kjent at organiserte kriminelle grupperinger har

[1] BOTNET er sammensatt av ordene Robot og Nettverk.

[2] SCADA: Supervisory Control And Data Acquisition.

utnyttet ondsinnede programmer i storskalaoperasjoner. Spesialtilpasset programvare kan for eksempel benyttes til industrispionasje og for å svindle nettbanker.

Vellykkede løsninger som selges kommersielt er blant annet såkalte automatiserte pakker. Slike pakker benyttes ofte for å infisere et større antall maskiner. NorCERT har ved flere anledninger arbeidet med saker der disse pakkene har blitt benyttet til massespredning av ondsinnet kode. Slik programvare benyttes også til å effektivisere prosessen med å konstruere botnet, jf pkt 1.1.1 ovenfor.

Alle som begår Internettkriminalitet er avhengig av å benytte en tjenesteleverandør på lik linje med lovlige brukere. Det er et faktum at det internasjonalt finnes flere tjenesteleverandører som opererer på kant med loven eller som utnytter vag og utilstrekkelig lovgivning i enkelte land.

1.1.5 Politisk motiverte angrep over Internett

Politisk motiverte dataangrep blir vanligvis begått av grupper som protesterer mot nasjonale og/eller internasjonale politiske hendelser. Slike aktiviteter omtales ofte som "hacktivism".

Tjenestenektangrep benyttes for å lamme tilgangen til en tjeneste eller et nettverk og er så langt den typen angrep som har fått mest publisitet. Dette er også den angrepsformen som det er enklest å iverksette. Defacing er en form for elektronisk tagging av websider. I Norge forekommer det et par hundre tilfeller hver måned hvor angripere går inn og endrer innholdet på websider. Det aller meste av dette er gjort ved hjelp av helautomatiserte angrep og det er vanskelig å se noen gjennomgående politiske motiver bak disse.

Et eksempel fra nyere tid på tjenestenektangrep er et massivt angrep mot danske Jyllandsposten som kom i kjølevannet av publiseringen av Mohammed-karikaturene i 2006. Et annet eksempel er fra politiet i Sverige som ble hardt rammet av et tjenestenektangrep etter at de hadde stengt ned en tjeneste som bidro til spredning av opphavsrettslig beskyttet materiale.

1.1.6 Generelle trender i utviklingen av ondsinnet programvare

Kompleksiteten i ondsinnet programvare øker. Det finnes stadig flere teknikker for å gjøre arbeidet med analyse av angrepskode vanskeligere. De samme teknikkene vil samtidig ofte forhindre at koden plukkes opp av automatiske deteksjonssystemer, som for eksempel antivirus- og innbruddsdeteksjonssystemer. Utfordringen er så stor at selv sikkerhetsbevisste virksomheter vil kunne oppleve å bli utsatt for alvorlige dataangrep. Det er derfor viktig å fokusere på evne til skadehåndtering og skadebegrensing i arbeidet med å planlegge sikkerhet.

I 2007 ble det observert mange verktøypakker som enkelt kan legges ut via kompromitterte websider, og som automatisk infiserer besøkende klientmaskiner. Mye av dagens ondsinnede programvare kommer med funksjonalitet for å lete etter og stjele personopplysninger. Dette betyr at identitetstyveri foregår i stor skala ved hjelp av trojanere og botnet. De fleste av disse tyveriene forekommer uten at de fornærmede har noen anelse om at de har blitt utsatt for identitetstyveri.

1.2 NSMs egne observasjoner

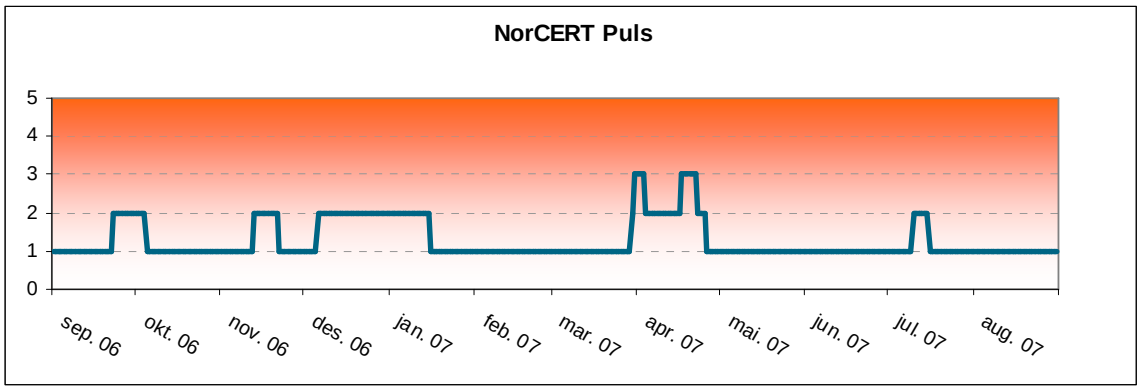
I tillegg til å sammenstille data fra åpne og lukkede kilder både nasjonalt og internasjonalt, samler NSM ved NorCERT også inn egne data gjennom nettverkssensorer. Dette er organisert gjennom varslingssystem for digital infrastruktur (VDI). Deltagerne i sensornettverket er representanter for kritisk digital infrastruktur i Norge og har utplassert sensorer i sine datanettverk for innsamling av informasjon.

1.2.1 NorCERT-puls i perioden september 2006 – september 2007

NorCERT-pulsen er delt opp i fem nivåer og er kort forklart i tabellen under.

Pulsnivå	Betydning
1	Ingen kjent fare for kritisk digital infrastruktur.
2	Moderat fare for kritisk digital infrastruktur.
3	Overhengende fare for vellykkede angrep rettet mot kritisk digital infrastruktur.
4	Stor fare for at store deler av kritisk digital infrastruktur vil bli satt ut av spill.
5	Store deler av kritisk digital infrastruktur er satt ut av spill.

Tabell 1 Kort forklaring av de forskjellige nivåene i NorCERT -pulsen.



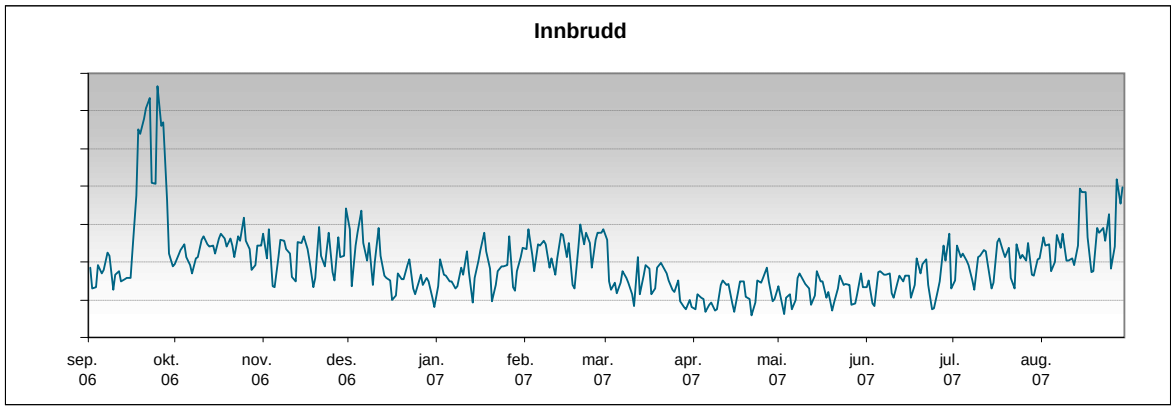
Figur 1 Grafen viser endring av NorCERT -pulsen i perioden september 2006 til september 2007.

I perioden fra september 2006 til september 2007 har det vært i alt seks pulsøkninger. De to pulsøkningene til nivå tre i mars – april kom som følge av en sårbarhet i behandlingen av Animated Cursor (.ANI) filer i Microsoft Windows og en ny alvorlig sårbarhet i Microsoft Windows tilknyttet DNS-tjenesten, hvor enkelte botnet implementerte søk og automatisk utnyttet denne sårbarheten.

1.2.2 Registrerte hendelser i sensornettverket

Den fremtredende nedgangen i helgene er en trend VDI har registrert så lenge sensorene har vært i drift, se figur 2. Når folk går fra jobb på fredag, stenger de ofte arbeidsmaskinen sin, og på denne måten blir det færre kompromitterte maskiner tilgjengelig på Internett.

Kartleggingsaktivitet representerer den desidert største delen av all aktivitet som observeres i VDI-systemet. Ut i fra de observasjonene som er gjort de siste 12 månedene kan vi ikke peke på noen spesielle trender.



Figur 2 Grafen viser antall innbruddshendelser per måned fra september 2006 til september 2007.

En av styrkene til VDI-systemet er å kunne oppdage *koordinerte* angrep mot kritisk digital infrastruktur i Norge. NorCERT definerer et koordinert angrep som en hendelse mot flere aktører fra en unik IP-

adresse. Teknisk betyr dette at koordinerte angrep blant annet oppdages når flere av VDI-sensorene trigger på aktivitet fra samme IP-adresse.

Mer informasjon og detaljerte trender fra VDI finnes i NorCERTs månedsrapporter som kan lastes ned fra vår hjemmeside.

2 Erfaringer fra tilsyn med sikkerhetsadministrasjon

Informasjonssikkerhet er et svært komplekst emne som krever forankring i ledelsessystemer. Denne forankringen kan bare oppnås ved at den enkelte virksomhet måles på dette som en suksessfaktor.

2.1 Sikkerhetsutdanning

Sikkerhetsleder har en viktig funksjon innen kontroll, råd, veiledning og kvalitetssikring. De virksomhetene som har plassert sikkerhetsleder nær ledelsen har erfart at bruken av sikkerhetsleder som bidragsyter til kvaltitesledelse har hatt stor nytte av dette. Sikkerhetsleder kan være en god bidragsyter i grenselandet mellom administrative dataverktøy, informasjonsforvaltning og saksbehandlingsrutiner.

Det er også registrert at den generelle opplæringen innen forebyggende sikkerhetstjeneste hovedsakelig gis til saksbehandlere som har dette som utøvende eller kontrollerende funksjoner. Lederes opplæring og kompetanse innen forebyggende sikkerhetstjeneste har vist seg i stor grad å være mangelfull. Resultatet har ofte blitt at sikkerhetspersonellets mulighet til å møte forståelse og prioritet har vært manglende. Virksomheter som har prioritert sikkerhetsopplæring av ledere har vist en langt bedre vilje og evne til å integrere forebyggende sikkerhetstjeneste med den øvrige aktiviteten i virksomheten.

2.2 Dokumentsikkerhet

Sentralisering av arkivtjenester kan innebære problemer i forhold til dokumentsikkerhet, da den lokale kompetansen om dokumentbehandling kan bli svekket. Tradisjonelt har dokumentsikkerhetsarbeidet blitt gjennomført i et samarbeid mellom sikkerhets- og arkivpersonellet ved den enkelte tjenestested. Med sentraliseringen av arkivpersonellet må sikkerhetsutdanningen lokalt styrkes for at sikkerhetspersonellet skal ha mulighet for å foreta kontrollene lokalt. Det kan se ut som om den nevnte måten å håndtere dokumenter på, har medført en systemfeil på sikkerhetsområdet.

2.3 Sikkerhetsgraderte anskaffelser

En av hovedoppgavene til NSM er å rapportere om sikkerhetstilstanden hos private leverandører til forvaltningen med leverandørklarering. Slike bedrifter spiller en viktig rolle for sikkerhetstilstanden av flere årsaker. For det første bidrar slike bedrifter til å levere produkter eller tjenester som er av betydning for vårt nasjonale sikkerhetsarbeid. For det andre er industrien viktig for å finne nye og smartere sikkerhetsløsninger, gjerne gjennom internasjonalt samarbeid. For det tredje er det viktig at bedriftene evner å beskytte den sikkerhetsgraderte informasjonen de besitter. For det fjerde kan offentlig forvaltning, etter NSMs syn, dra lærdom av hvordan flere bedrifter faktisk organiserer og administrerer sikkerhetsarbeidet.

NSMs tilsynserfaringer tilsier at sikkerhetstilstanden er gjennomgående godt ivaretatt hos de fleste klarerte leverandører. Generelt er det belegg for å si at leverandørene er sikkerhetsbevisste og motiverte for å drive forebyggende sikkerhetsarbeid, slik lovgivningen krever.

2.4 Risiko- og sårbarhetsanalyser (ROS)

Kun enkelte virksomheter har gjennomført ROS. Analysene har vært rettet mot deler av virksomheten og spesielt mot informasjonssystemer. Vedrørende disse systemene var oppmerksomheten rettet mer mot funksjonalitet og integritet enn skjerming av informasjonen. Selv om de grunnleggende krav til konfidensialitetssikring er gitt i regelverket, anser NSM det som viktig at alle elementene ivaretas i en helhetlig analyse. NSM er opptatt av at virksomheter jevnlig vurderer risikoen knyttet til terrorisme, sabotasje og spionasje i forhold til seg selv, og implementerer nødvendige sikkerhetstiltak.

Det er en klar sammenheng mellom overordnet virksomhets prioriteringer og sikkerhetstilstanden i underordnet virksomhet. Underordnede virksomheter har ofte hatt samme svakheter og mangler som en finner på overordnet nivå. Det finnes også gode eksempler på at gode tiltak i overordnet virksomhet gjenspeiles i gode tiltak i underordnet virksomhet. Blant de vellykkede tiltakene var bruk av ROS for å bedre rutiner og tiltak innen eget ansvarsområde. Dette var også beskrevet i overordnet virksomhets oppdrag til de aktuelle etatene. Dette er bra og eksempel til etterfølgelse.

3 Om sikkerhet ved graderte IKT-systemer og kommunikasjonssikkerhet

IKT-sikkerhet er et spesialisert fagfelt som stiller store krav til kompetansen hos personell både innenfor tilrettelegging, utforming og implementering av IKT-systemer. Denne kompetansen er problematisk for Staten å etablere. Statlige virksomheter opplever en stadig større profesjonalisering og spesialisering, noe som forutsetter at Staten er konkurransedyktig nok til å rekruttere og beholde spesialister, ikke minst innen teknologiske fag. Dette kan innebære at samfunnet ikke lenger har kompetansen til å foreslå, følge opp og kontrollere IKT-sikkerhetstiltak.

Antall søknader om sikkerhetsgodkjenning av informasjonssystemer er økende. I 2007 fikk NSM tilsendt over 200 søknader til behandling. Mange av sakene er omfattende og kompliserte og krever tverrfaglig håndtering i NSM. Saksbehandlingstiden varierer fra noen dager til flere år, avhengig av blant annet graderingsnivå, funksjonalitet, kompleksitet, teknologi, informasjonsutveksling med andre informasjonssystemer og kvaliteten på mottatt sikkerhetsdokumentasjon.

NSM har delegert sikkerhetsgodkjenning av enklere informasjonssystemer med lavt graderingsnivå til ledere av offentlige virksomheter. NSMs erfaring fra tilsyn viser imidlertid mangler ved praktisering av sikkerhetsgodkjenning av informasjonssystemer i virksomheter.

I dag utvikler ulike virksomheter ofte egne graderte informasjonssystemløsninger. NSM mener at større grad av gjenbruk av sikkerhetsgodkjente løsninger, innen både militær og sivil sektor, vil bidra til bedre sikkerhet. Gjenbruk vil bidra til bedre ressursutnyttelse for alle gjennom standardiserte grensesnitt og formater, samt mulighet for sikre, effektive og sentraliserte driftstjenester. Gjenbruk av prosedyrer og prosesser knyttet til aktiviteter som utvikling, drift og vedlikehold, hendelseshåndtering og gjenoppretting, samt godkjenning vil også gi en bedre ressursutnyttelse.

På midten av 90-tallet innførte EU normer for elektromagnetisk kompatibilitet og interferens (EMC/EMI) på elektronisk utstyr. NSM fant at det var vesentlig mindre Tempest-utfordringer[3] på utstyr levert med en EMC/EMI godkjenning. NSM ser nå imidlertid at denne trenden dessverre har snudd. Strålingsnivåer på dagens hyllevareutstyr viser en negativ tendens med hensyn til Tempest. Denne tendensen har sammenheng med blant annet innføringen av nye teknologier med høyere datahastigheter, trådløs teknologi, modulbasert sammensetning av systemer og mangel på tester av sammensatte systemer.

[3] TEMPEST: Utilsiktet stråling av kompromitterende informasjon fra elektronisk utstyr og systemer.

NSM finner at det er flere Tempestsårbarheter i IKT-systemer som bruker kommersielt hyllevareutstyr enn det som har vært tilfelle i en periode. Det er derfor behov for å utføre målinger på utstyret som skal brukes i systemer for sensitiv informasjon. NSM viderefører tilbudet om Tempestmålinger på hyllevareutstyr som skal brukes i systemer for sensitiv informasjon.

4 Sikkerhetskultur

Begrepet sikkerhetskultur er definert av NSM som *summen av de ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd.*

4.1 Sikkerhetsmessige aspekter ved nettsamfunn

Internett er et medium med et tilnærmet ubegrenset spredningspotensial av informasjon. Det er derfor et stort skadepotensial knyttet til spredning av sensitiv informasjon på nett. NSM er kjent med at mange aktører jobber aktivt med å samle inn sensitiv informasjon, for eksempel personopplysninger, virksomhetssensitiv informasjon osv. Hovedsakelig kan dette sees på som helt legalt. Likevel er ikke all innsamling av informasjonen ønskelig når det eksempelvis skjer fra trusselaktører som etterretnings- og terrororganisasjoner, kriminelle miljøer og hackermiljøer.

I det siste året har bruken av nettsamfunn økt blant den norske befolkning. NSM mener at dette ikke bare er positivt. Et nettsamfunn er et forholdsvis uformelt møtested som øker muligheten for at sikkerhetsgradert eller sensitiv informasjon utleveres. Ubevisst utleverer også brukerne personlig informasjon i en slik mengde og detaljgrad at informasjonen indirekte eller direkte kan utnyttes av mange trusselaktører.

Nettsamfunn er internettbaserte samlingssteder for enkeltpersoner som ønsker å kommunisere med andre mennesker. Nettsamfunn gir brukerne anledning til å kommunisere med andre brukere ved å utveksle personlig informasjon, meninger, nyheter, bilder, filer m.m. For å kunne bli bruker av de ulike nettsamfunn som tilbys på Internett, må den enkelte melde seg inn via en tilbyder. Tjenesten er i de fleste tilfeller gratis, og det finnes i dag mange ulike nettsamfunn for ulike målgrupper. Nettby er et norsk nettsamfunn med over 477 000 ”borgere”. Et annet norsk nettsamfunn er Blink med over 316 000 medlemmer. I begynnelsen av 2007 fikk det amerikanske nettsamfunnet Facebook en oppmerksomhet hos nordmenn som gjorde dette til det raskest økende nettsamfunnet i Norge. Ca 360 000 norske brukere er pr. i dag registrert som brukere. Facebook er det nettsamfunnet som gir brukeren størst mulighet til å utlevere personlig informasjon om seg selv. Den nye brukeren møter en rekke personlige spørsmål allerede i det man er i ferd med å registrere seg som bruker. I en slik situasjon settes det til dels store krav til brukerens bevissthet om hvor mye informasjon det kan være lurt å utlevere om seg selv.

De aller fleste nettsamfunn tilbyr den enkelte bruker muligheten til å begrense hvem som kan få tilgang til deres personlige informasjon. Mange velger allikevel ikke å benytte seg av denne muligheten. Det å begrense hvem som kan få tilgang til informasjon medfører også at brukeren ikke blir oppdaget av personer man gjerne ønsker kontakt med. Det har også forekommet hendelser hvor slike brukerdefinerte begrensninger ikke har fungert og andre brukere feilaktig har fått tilgang til andres brukerkontoer.

Nasjonal sikkerhetsmyndighet gjennomførte i mai 2007 en undersøkelse av hvem som hadde registrert seg som brukere og hva de utvekslet av informasjon om seg selv eller andre. NSM hadde oppmerksomhet rettet mot yrkesgrupper/brukere som med stor sannsynligvis behandlet sikkerhetsgradert informasjon. Funnene synliggjorde et behov for å bevisstgjøre virksomheter og enkeltpersoner om de sikkerhetsutfordringer som uaktsom bruk av nettsamfunn medførte. Den tilgjengelige informasjonsmengden åpnet for en kartlegging av både organisatorisk og personlig art hos virksomheter av stor betydning for samfunnskritiske funksjoner.

Personer som i det daglige arbeider med sikkerhetsgradert informasjon gjør seg synlige for trusselaktører når de i sin deltakelse i nettsamfunn oppgir informasjon om arbeidsgiver, stilling/posisjon og egne eller organisasjonens arbeidsoppgaver. Gjennom dette blir personer som tidligere har vært usynlige, synliggjort slik at de kan oppfattes som interessante for trusselaktører.

Digital utnyttelse er å bearbeide den tilgjengelige personlige informasjonen til å senke en persons sikkerhetsmessige bevissthet på en slik måte at det gjør det enkelt å gjennomføre dataangrep i form av f.eks. målrettede trojanere. Avsender er i stor grad avhengig av at mottakeren åpner et vedlegg i en tilsendt e-post eller følger en vedlagt link til et annet nettsted. Målet er å få mottakeren til å senke sitt forsvar ved å fremstille det slik at e-posten kommer fra en venn. Slik manipulering kan forholdsvis enkelt la seg gjøre ved å bruke informasjonen fra nettsamfunn.

Analog informasjonsutnyttelse er å benytte den tilgjengelige personlige informasjonen til å ta direkte kontakt. Den personlige informasjonen kan gjøre det enkelt for en profesjonell trusselaktør å tilnærme seg og knytte kontakt med en person. Potensielle menneskelige svakheter aktualiseres og forsterkes gjennom at vedkommende legger ut detaljert informasjon om seg selv. Slik informasjon kan i verste fall utnyttes til manipulering, press, trusler eller direkte vervingsforsøk.

Nettsamfunn stiller store krav til brukeren. Dersom virksomheter og deres ansatte ikke er seg bevisst verdien av informasjonen som legges ut på slike sider, øker risikoen for at sikkerhetsgradert informasjon eller forretningshemmeligheter blir offentliggjort. Den samme risikoen er til stede dersom virksomhetene og de ansatte ikke er bevisste i forhold til hvordan personlig informasjon kan utnyttes til indirekte eller direkte å kompromittere informasjon.

NSM har sett at en økt bevisstgjøring av sikkerhetsutfordringer ved deltakelse i nettsamfunn har ført til positive resultater. Flere virksomheter og ansatte ser ut til å ha tatt problematikken på alvor. NSM har observert at flere yrkesgrupper som tidligere hadde en høy grad av synlighet i nettsamfunn, nå er mindre synlige. Allikevel er det fortsatt grunn til å påpeke at virksomheter og personer som arbeider med sikkerhetsgradert informasjon må være bevisste på hvilke sikkerhetsmessige utfordringer nettsamfunn kan utgjøre.

4.2 Personellsikkerhetsmessige vurderinger av fremmede stater

De siste årenes utvikling har endret noen av forutsetningene for arbeidet med personellsikkerhet og for klarering. For det første har en stadig større del av befolkningen en kulturell bakgrunn fra land utenfor Norge og Vesten, og stadig flere innvandrere får norsk statsborgerskap. For det andre har etniske nordmenn tilbrakt stadig mer tid i andre stater, og ofte hatt mer langvarige opphold i forbindelse med studier og arbeid. Slike utviklingstrekk har ført til endringer i regelverket for personellsikkerhet.

Et viktig tiltak for å kunne ta høyde for regelendringene og samtidig ivareta Norges sikkerhetsmessige interesser er NSMs produksjon av Personellsikkerhetsmessige vurderinger av fremmede stater. Vurderingene av hver enkelt stat foretas spesielt med tanke på avholdelsen av en sikkerhetssamtale og skal inneholde tilstrekkelig med bakgrunnsopplysninger og analyse til å gjøre klareringsmyndighetene i stand til å planlegge en sikkerhetssamtale. Viktige momenter i en vurdering er blant annet landets sikkerhetsmessige betydning, kulturelle kjennetegn, lojalitetsstrukturer og statens rolle i samfunnet. I tillegg sikrer vurderingene at klareringsmyndighetene baserer seg på samme kunnskapsgrunnlag i personellsikkerhetsarbeidet. På denne måten står personellsikkerhetstjenesten bedre rustet til å møte de nye samfunnsutfordringene.

Med et lands sikkerhetsmessige betydning menes i hvilken grad landets styresett, forholdet til Norge og våre allierte, kriminalitetsbilde, etterretningsvirksomhet eller – interesser, økonomiske forhold og lignende, kan bidra til å påvirke vedkommende persons sikkerhetsmessige skikkethet. Når det gjelder vedkommendes tilknytning til hjemlandet, blir det i stor grad gjort de samme vurderingene som ved tilknytning til annen stat for norske statsborgere. Personkontrollen, vurdering av landets

sikkerhetsmessige betydning og selve sikkerhetssamtalen er ment å tilrettelegge for vurdering av en persons lojalitet, pålitelighet og sunne dømmekraft. Det er en helhetlig vurdering av disse tre kriteriene som er den reelle risikovurderingen av en persons sikkerhetsmessige skikkethet.

5 Offentlig tilgjengelig geografisk informasjon

5.1 Piktometri

I 2007 kom en ny fototjeneste med enda bedre oppløsning enn fotografiene i Google Earth og Aftenposten kart. Tjenestene går under navnet piktometri, og er kommersielt tilgjengelig i Norge fra tjenester som Gule sider og Microsoft Virtual Earth. Fotografiene har meget god oppløsning, ned til 12-20 cm, og det tas et stort antall fotografier inkludert skråfotografi.

Microsoft Virtual Earth er en konkurrerende tjeneste til Google Earth og Google Maps. Tjenesten er under oppbygging, men er godt utbygd blant annet i Microsofts ”hjemby”, Seattle i USA. Tjenesten består av kart, vertikalfotografier, skråfotografier, 3D-modeller samt kobling av informasjon inn i disse. Store deler av USA er lagt inn med piktometri-fotografier, selv om det kun er de største byene og attraksjonene som er lagt inn med 3D-funksjon. Dette gjelder også militære installasjoner.

Per i dag finnes det ikke tjenester hvor privatbrukere kan legge inn egen informasjon i piktometri-tjenester på sammen måte som man kan gjøre i Google Earth, men det er sannsynlig at dette vil komme. Da kan man se for seg at privatpersoner vil legge ut informasjon om hvor ulike trusselutsatte personer har kontor, med henvisning til konkrete vindusruter. Det kan også tenkes at det vil bli vist til og beskrevet sårbare punkter i kritisk infrastruktur, for eksempel konkrete transformatorer i det elektriske sentralnettet eller kritiske punkter i gassinfrastrukturen.

5.2 Mulig sensitiv informasjon på nettsider – plan- og bygningstegninger

IT-verktøy gjør det mulig å praktisere meroffentlighet ved å legge ut plan- og bygningstegninger på Internett i byggesaker og lignende. Dette er også gjort i enkelte norske kommuner. Det bidrar til å forenkle saksgang, og gir relevante brukere enklere og billigere tilgang. Samtidig kan det reises spørsmål ved om en slik praksis vil bidra til å øke verktøykassen til personer med ondsinnede hensikter. Det synes ikke nødvendig at plan- og bygningstegninger over sensitive bygninger ligger åpent tilgjengelig over Internett. Dette synes i liten grad å ha vært gjenstand for en sikkerhetsmessig verdivurdering.

6 Noen av NSMs anbefalinger

NSM viser til at sikkerhetstruende hendelser mot graderte IKT-systemer må rapporteres til NSM med en gang de er kjent. NSM anbefaler at virksomhetene[4] skaffer seg oversikt over hvor avhengig de er av data og nettverkstjenester. For å kunne beskytte seg mot omfattende tjenestenektangrep, må den enkelte virksomhet inngå avtaler med sine tjenesteleverandører om hvordan slike angrep skal forebygges og håndteres. Krav til sikkerhet, oppfølging ved angrep, deteksjons- og reaksjonsverktøy og metoder bør avtalefestes med leverandørene.

[4] I dette avsnittet definert ikke bare som virksomheter i henhold til sikkerhetslovens bestemmelser, men alle virksomheter med samfunnskritiske IKT-systemer

NSM anser at det vil være nyttig om offentlige og private virksomheter innenfor sektorer som for eksempel finans, energi og telekommunikasjon oppretter sektorvise CERT-funksjoner (Incident Response Teams). Definerte og etablerte grupper som har et ansvar ved en hendelse kan øve og forberede seg på effektiv håndtering. NSM kan bidra med råd og veiledning.

NSM anbefaler at *alle* virksomheter etablerer et tilpasset miljø for å håndtere IKT-sikkerhetshendelser i organisasjonen. Dagens IKT-trusler er så komplekse at det ikke er mulig å beskytte seg mot alle angrepsscenarier, virksomhetene bør være i stand til å håndtere sikkerhetshendelser som vil oppstå.

NSM anbefaler at virksomhetene bruker ressurser på opplæring av brukere. Svært mange angrep mot IKT-systemer retter seg mot klienter og sluttbrukere. Mange av disse angrepene forutsetter at brukeren lar seg lure til å akseptere en forespørsel. Målrettede angrep som er skreddersydd for å lure en bruker er det svært vanskelig å reagere på uten nødvendig opplæring. Tilstrekkelig opplæring av brukere har potensielt en stor sikkerhetsmessig gevinst i forhold til innsats og kostnader.

NSM anbefaler fortsatt at aktuelle virksomheter informerer NorCERT ved alvorlige IKT-hendelser, og at virksomheter med viktige samfunnsfunksjoner fører en aktiv dialog med NorCERT for å holde oversikt over trusler og angrep på Internett. Deling av informasjon om angrepsformer er viktig for å håndtere angrep og for å implementere forebyggende tiltak. NSM anbefaler fortsatt at virksomhetene med utgangspunkt i jevnlige risikoanalyser utformer beredskaps- og krisehåndteringsplaner for å forebygge og håndtere uønskede IKT-hendelser. Planverkene må øves for å gjøre organisasjonen forberedt på å håndtere en krise. Det er viktig at virksomhetene kjenner til sitt nærmeste CERT-kontaktpunkt, slik at ansvarlige myndigheter kan holdes oppdatert.

NSM anbefaler fortsatt at virksomhetene etablerer gode rutiner og prosedyrer for rask testing og utrulling av programvareoppdateringer. Det er viktig å innlemme både nettverkskomponenter og tjenesteprogramvare i disse rutinene, og ikke kun konsentrere seg om operativsystemer som det har vært mye oppmerksomhet på de siste årene

NSM anbefaler at alle virksomhetsledere har et bevisst forhold til innføring og bruk av ny teknologi som blant annet USB-minnepinner, mobiltelefoner, digitalkamera, PDAer etc., spesielt i forhold til graderte informasjonssystemer. For å unngå misbruk eller feil bruk av ovennevnte medier anbefales det at gode rutiner etableres, bekjentgjøres og følges opp.

NSM anbefaler alle virksomheter som har sikkerhetsgraderte informasjonssystemer om å prioritere arbeidet med IKT-sikkerhet. NSM understreker viktigheten av at dette arbeidet er forankret hos virksomhetens leder. Virksomhetens leder har et særskilt ansvar for å legge til rette for at intern sikkerhetsorganisasjon får opplæring i IKT-sikkerhetsarbeid generelt og sikkerhetsgodkjenning spesielt.

NSM anbefaler at virksomhetene foretar en verdivurdering av hva slags informasjon som er av en slik art at det bør eller skal beskyttes. Ut i fra en slik analyse vil virksomhetene også få en oversikt over hvem som behandler beskyttelsesverdig informasjon i organisasjonen. På den måten vil virksomhetene bedre se verdien av informasjonen og dermed forstå behovet for å innføre sikringstiltak.

NSM anbefaler også at virksomhetene ser på hva deres ansatte publiserer på nettsamfunn. Virksomhetene bør forsøke å skape en så god sikkerhetsmessig bevissthet som mulig hos sine ansatte. Den enkelte bør ikke være i tvil om hva som kan og ikke kan publiseres på Internett av arbeidsrelatert informasjon. Samtidig bør den enkelte bevisstgjøres i forhold til hvordan personlig informasjon kan utnyttes av andre. Flere virksomheter har laget egne instrukser som regulerer organisasjonens og de ansattes bruk av nettsamfunn som Facebook. NSM har utarbeidet et temahefte som kan bidra til å øke bevisstheten rundt deltakelse i nettsamfunn.