Høringsmerknader fra NorSIS

Det økende trusselbildet gjør at NorSIS mener loven bør åpne for at tilbydere i større grad kan pålegges å innføre sikkerhetstiltak. Truslene er mange, men vi ønsker å framheve noen trusler som i dag utgjør hoveddelen uønsket aktivitet i elektroniske kommunikasjonsnett.
En viktig faktor i det totale trusselbildet er den klare dreiningen vi har sett i løpet av de siste årene fra hobbyhackere til organisert kriminalitet i vinnings hensikt. Dette gjør at truslene vi ser i dag ikke lengre er bare plagsomme, men i stedet utgjør en direkte fare for den angrepne.

Spam

Mengden av spam har nå nådd slike mengder at den i mange tilfeller reduserer nytteverdien for privatpersoner og virksomheter av e-post dramatisk. Det er ikke unormalt at mer enn 80 % av innkommende e-post er spam. I tillegg medfører mange mottiltak også redusert nytteverdi av e-post. My av dette kan bedres ved at tilbydere av elektroniske kommunikasjonstjenester viser større ansvar for å redusere dette misbruket av nettverksressurser.
Problemet er ikke lengre bare et e-postproblem. Samme misbruk skjer også på andre meldingstjenester på Internett og på andre nettverk. NorSIS har erfart at samme form for uønskede masseutsendelser også skjer eller kan skje på SMS, MMS og ulike lyn-meldingstjenester.

Botnet

Ut fra offentlig tilgjengelige statistikker fra ulike kilder så øker trusselen botnet utgjør hele tiden. I Symantecs siste rapport fra september 2006 forteller de at de i første halvår 2006 i gjennomsnitt så 57 717 aktive botnet hver dag. Totalt observerte de 4 696 903 ulike botnet og identifiserte 6 337 botnet kontrollsentre i perioden. Tall fra andre kilder bare bekrefter at omfanget og problemet er stort og at det øker.
Botnet er hovedverktøyet for dagens organiserte IKT-kriminelle. De brukes til alt fra knekking av kryptonøkler, utsendelse av spam, etablere falske nettsteder, opprette nye botnet osv. osv. De fleste DDoS[1]-angrep kjøres i dag fra botnet. Et godt eksempel er angrepne tidligere i år på Jyllandsposten. Derfor er det viktig å sørge for at botnet er vanskeligst mulig å etablere og enklest mulig å oppdage og stoppe.

Malware

Malware er en samlebetegnelse på alle former for uønsket programvare som på ulike måter kan misbruke en datamaskin. Det innbefatter, men er ikke begrenset til, virus, spyware, trojanere, ormer og adware. Alt sammen er uønsket programvare som installeres uten brukerens samtykke eller ønske. Problemet er størst på Windows-plattformen, men er også økende på andre plattformer.
De ulike formene for malware brukes ofte som inngangsporten for å få innlemmet en maskin i et botnet. Derfor er det viktig å i størst mulig grad hindre spredning av malware.

Spoofing

De fleste angripere i dag prøver i størst mulig grad å skjule sine spor. En av den enkleste metodene i dag er å forfalske avsenderadressen eller såkalt spoofing. Dette er et problem som ikke er begrenset til IP-baserte nett. Det er demonstrert at tilsvarende

[1] DDoS – Distrubuted Denial of Service – Distribuert tjenestenektangrep

avsenderadresseforfalsking er mulig i telenett også. Metoden brukes også på lavere nettverkslag for å kunne misbruke for eksempel trådløse LAN.
De fleste tilbydere har allerede mekanismer i nettene sine som enkelt og rimelig kan hindre spoofing. Dessverre har de ikke aktivert disse mekanismene.

Kommentarer til ny § 2-3 i ekomloven

I forslaget i høringsunderlaget forslås denne endret fra:

§ 2-3. Krav til nett, tjeneste, tilhørende utstyr og installasjoner

Myndigheten kan stille krav til elektronisk kommunikasjonsnett, -tjeneste, tilhørende utstyr, installasjoner og bruk av standarder for å sikre samvirke mellom nett og tjeneste, kvalitet, effektiv utnyttelse av kapasitet i nett som nyttes av flere tilbydere, sikre liv og helse eller unngå skadelig interferens.

Myndigheten kan gi forskrifter om forholdene regulert i første ledd.

Til:

§ 2-3. Krav til nett, tjeneste, tilhørende utstyr og installasjoner

Myndigheten kan ***gi forskrift eller treffe enkeltvedtak om*** *krav til elektronisk kommunikasjonsnett, -tjeneste, tilhørende utstyr, installasjoner og bruk av standarder for å sikre samvirke mellom nett og tjeneste, kvalitet, effektiv utnyttelse av kapasitet i nett som nyttes av flere tilbydere, sikre liv og helse eller unngå skadelig interferens.* ***Herunder kan myndigheten kreve at tilbyder skal gjennomføre tiltak som begrenser mengden av spam.***

NorSIS er positive til at hjemmelen utvides til å treffe enkeltvedtak i tillegg til å gi forskrifter.

Vi er også positive til at hjemmelen i loven utvides til å kunne avkreve tilbydere tiltak for å redusere spam. NorSIS mener at denne hjemmelen til å avkreve tilbyderne mottiltak bør utvides og ikke bare omhandle et spesifikt problem. I eksemplene og forklaringene over så hav vi vist at hovedproblemene i dag omfatter mer enn spam og er heller ikke begrenset til bare IP-baserte nettverk.

Derfor mener vi at siste punktum i § 2-3 bør omformuleres slik at den kan gi hjemmel for tiltak mot spam, botnet, malware og spoofing. Vi har ikke et forslag til tekst, men slik teksten står i dag så dekker den kun et spesifikt problem og tar ikke høyde for fremtidige trusler. En mulighet er å omformulere til at tilbydere kan avkreves tiltak som gir en nødvendig basissikkerhet eller generalisere til at tilbydere kan avkreves tiltak mot skadelig eller omfattende misbruk av nettene. Det er viktig at dette gjøres teknologinøytralt.

Et viktig hjelpemiddel mot botnets er at riktige myndigheter får tilgang til såkalte netflowdata. Slike data gir ikke innsyn i innholdet av en datastrøm, men vil gjøre det mye enklere for for eksempel NorCERT å identifisere botnet og botnet-kontrollsentre. Dette er et tiltak som bør gjennomføres uavhengig av innføringen av EU-direktivet om lagring av elektroniske kommunikasjonsdata som et av flere tiltak for å demme opp for de før nevnte truslene.