Metoderapport SKUP 2000

«Sikker som nettbanken»

Dagbladets nyhetsredaksjon
Journalister: Kristian Sarastuen, Bjørn K. Bore og May Linn Gjerding

En artikkelserie om sikkerheten i nettbankene, kundens ansvar og bankenes ansvarsfraskrivelse.

Metoderapport SKUP 2000

«Sikker som nettbanken»

Journalister: Kristian Sarastuen, Bjørn K. Bore og May Linn Gjerding

En artikkelserie om sikkerheten i nettbankene, kundens ansvar og bankenes ansvarsfraskrivelse.

Publisert i Dagbladet i perioden 10.07.2000 – 17.07.2000

Dagbladets nyhetsredaksjon, ved nyhetsredaktør John Arne Markussen
PB 1184 sentrum
0107 Oslo

Kontaktperson: Kristian Sarastuen
Adresse: Fredensborgveien 35 b, 0177 Oslo
Tlf: 41 20 11 87

Vedlegg:
Artikkelserien (17 s.)
Kommentar- og debattinnlegg (4 s.)

Artiklene, og senere avsløringer, er tilgjengelige på Dagbladet.no. Adressen til samlesiden er http://www.dagbladet.no/kontekst/22261.html

Er nettbanken sikker?

De siste årene har norske banker brukt betydelige ressurser for å få sine kunder til å gå over til å bruke nettbaserte banktjenester. I nettbanken gjør kunden jobben sjøl, og begge parter skal spare både tid og penger. Tjenesten er like sikker som å gå i banken på vanlig måte – hevdes det. Nettbank er fremtiden, det må folk forstå. Så langt har over 600 000 nordmenn skjønt dette. Mange av disse bor på steder der nettbanken er så å si eneste alternativ. Spesielt etter at den lokale bankfilialen ble lagt ned.

I følge amanuensis ved BIs Institutt for Teknologiledelse, Ragnvald Sannes, sparer bankene milliarder av kroner på å dytte kundene over i de elektroniske bankene.
Internett-suksessen har fått så å si samtlige norske banker til å satse på nettbank. I 1999 kunne nordmenn velge mellom 134 ulike banktilbud på nettet.

1. juli trådte den nye finansavtaleloven i kraft. Samtidig meldte internasjonale medier om flere elektroniske innbrudd i engelske og tyske nettbanker. Ved flere anledninger skulle tyvene ha kommet seg unna med klingende e-mynt.

Vi valgte derfor å se på nærmere på det norske nettbanktilbudet. Dette var sommeren 2000 et etablert tilbud, flere av storbankene hadde hatt slike satsninger i flere år, og som nevnt, brukt av mange.

Vi ville se på følgende forhold:

- Er norske nettbanker sikre? Har det forekommet "innbrudd," er det mulig å bryte seg inn, og hvor stor er faren for det?
- Hva sier lovverket og kontraktene? Hvilket ansvar har kunden, hvilket ansvar har banken?
- Hvordan kan kunden sikre seg selv? Er noen banker sikrere enn andre, og hvilke forholdsregler bør nettbankbrukeren ta selv?

En kronologisk gjennomgang av arbeidet:

"Kunden har ansvaret"

Vi startet prosjektet med en gjennomgang av ansvarsforholdet mellom nettbanken og kunden. Hvem satt igjen med ansvaret dersom noen klarte å lure systemet?

Vi innhentet kontraktene for tegning av nettbank hos de største bankene. Resultatet var overraskende. En finlesing av disse viste at kunden selv har ansvaret for sikkerheten på sin egen PC. Bankene sammenlignet sikkerheten på den private PC med det ansvaret kundene har for å hindre uvedkommende i å få tak i koden til Visa-kort o.l.

I kontraktene ble det understreket at kunden måtte sørge for at PC-en var tilstrekkelig utrustet for å hindre uvedkommende å få tak i vitale opplysninger. DnB tilbød kunden et gratis oppdatert virusprogram, ellers bestod sikkerheten av de kodenøklene som fulgte med nettbankprogrammet.

Vi tok kontakt med Informasjonsdirektør Preben Sandborg Røe i Finansnæringens Hovedorganisasjon og informasjonssjef i DnB Jarl Veggan for å få en forklaring på dette. DnB hevdet at deres system var sikkert og at banken ikke kunne lastes for kundenes eventuelle uforsiktige bruk.

Røe i FH uttalte: "Det er ikke rimelig at bankene skal holdes ansvarlige for hva som skjer på private PC-er. Man må ikke forveksle en hjemme-PC med en bankfilial."

Hva så med sikkerheten?
Journalist Kristian Sarastuen kontaktet to kilder i det norske hackermiljøet. Sarastuen har hatt kontakt med disse personene over en toårs periode, og de har bidratt med fagkunnskap til flere saker. Begge er i 30-års alderen og har hver sin faste jobb innen dataprogrammering. De har tidligere vært aktive i ulike hackerprosjekter både nasjonalt og internasjonalt og har et stort kontaktnett.

Kontakten med dekknavnet "Ice" jobber "på fritiden" i en internasjonal elitegruppe av hackere fra fem ulike nasjoner, som mottar betaling for å teste datasikkerheten i større bedrifter. De tar også betaling for å bryte seg inn å stjele informasjon.

Begge disse kildene kunne fortelle at sikkerheten i norske nettbanker var dårlig. De listet opp en rekke ulike metoder, der en kunne ta seg inn i en nettbankkundes PC og dermed få tilgang

til personens konto. Imidlertid ville ingen av disse stå frem verken anonymt eller med fullt navn.

Vi kontaktet datasikkerhetsfirmaet Norman. Viseadministrerende direktør Jan Kristensen, kunne bekrefte hackernes påstander. Han hevdet at bankene i seg selv er godt rustet til å motstå et innbruddsforsøk fra en hacker. Det svake leddet er kundens egen PC. Kristensen hevdet at det ville være lekende lett for en dyktig hacker å skaffe seg tilgang til en nettbankkundes konto gjennom vedkommendes private PC.

Vi brukte tre dager på å dobbeltsjekke disse påstandene. Konklusjonen var entydig: Dataekspertene hevdet kundene var dårlig sikret, og at man når som helst kunne vente at kontoene deres ble tømt av hackere. Bankene hevdet at deres løsninger var sikre, men påpekte at det var kundens ansvar å besørge sikkerheten på egen PC.

Artikkel 1. stod på trykk som oppslag i Dagbladet 10.07.2000.

Sikkerhetshullene avsløres:

Journalist Kristian Sarastuen hadde bedt sine hacker-kilder å spre ryktet om at Dagbladet var interessert i personer som hadde oppdaget hull i nettbankenes sikkerhet. Vi ønsket å dokumentere dette ved å gjennomføre et kontrollert "elektronisk ran."

Etter oppslaget meldte flere personer seg gjennom vårt kontaktnett. En av disse, "Jon", ønsket å vise hvor enkelt han kunne knekke DnBs nettbank. Den etiske og juridiske siden ved å gjennomføre et slikt hackerangrep ble nøye diskutert og planlagt i Dagbladets redaksjon. I felleskap med nyhetsredaktør John Arne Markussen og sjef for nyhetsavdelingen Terje Myklevoll, ble det bestemt at journalist Sarastuen skulle få "Jon" til å gjennomføre stuntet, dersom kontoinnehaver var klar over hva som foregikk.

Begrunnelsen for beslutningen var at det er samfunnsmessig viktig å avsløre eventuelle sikkerhetshull i nettbanksystemet.

Journalist Kristian Sarastuen sjekket bakgrunnen til "Jon" før det ble bestemt å sette i gang forsøket. "Jon" er ansatt i et datafirma og har ansvar for datasikkerhet. Opplysningene stemte overens med den identiteten "Jon" oppgav.

Det var større problemer med å finne en person som ville stille sin DnB-konto til disposisjon for testforsøket. Personen som lot seg overtale var en venninne av Sarastuen. Hun deltok under løfte om full anonymitet, samt at hun kort tid etter ville si opp sin konto i DnB. Kundens anonymitet anser vi som en svakhet ved sikkerhets-testen. Vi ønsket å få en politiker til å delta i forsøket. Det fikk vi ikke til på kort tid, og vi valgte å prioritere tett oppfølging til problemstillingen.

Forsøket ble gjennomført 10.07. "Jon", som ønsket å være anonym i frykt for å miste jobben sin, sendte et lite spesialskrevet program på e-post til den utvalgte kunden. Programmet var skjult som et lite postkort og det installerte seg selv på harddisken da kunden åpnet det. Virusprogrammet på PC-en hennes reagerte ikke på e-posten. I følge "Jon" ville dataprogrammet kunne følge alle bevegelser mottageren gjorde på PC-en. Det "lyttet" på tastaturet og kunne registrere alle koder og passord som ble tastet inn. Resultatene ble sendt

tilbake til ”Jon” på en e-post, som ikke kunne spores på brukerens maskin. Programmet som ”Jon” brukte ligger fritt for nedlasting på internett. Programmet var endret slik at det ble lettere å passere virusprogrammer.

Dagbladet holdt kontakt med bankkunden per telefon og ba henne gå inn på sin konto i DnB nettbank. Kort tid etter at hun hadde logget seg inn på sin egen konto i nettbanken og overført et mindre beløp hun hadde utestående, fikk ”Jon” en e-post, der alle koder og passord stod beskrevet. Etter at bankkunden hadde logget seg av, brukte ”Jon” opplysningene til å skaffe seg adgang til kontoen hennes. Dagbladet hadde full oversikt over hva som stod på kontoen, og hvilke transaksjoner denne kunden hadde utført. Vi avsluttet forsøket med å overføre 100 kroner til en på forhånd avtalt konto i DnB.

”Jon” viste også Dagbladet en rekke konti i DnB han hadde fått tilgang til, etter å ha testet programmet. Han påstod at han ikke hadde tatt penger fra disse kontoene. Dagbladets team ba han slette disse kontiene fra sitt eget system, siden dette var ut over Dagbladets mandat, og uten tvil i strid med loven.

I følge ”Jon” fungerte det modifiserte dataprogrammet på samme måte som ”I Love You-viruset.” Det kopierte adresselisten på mottagerens PC og sendte programmet videre til alle som stod på denne. På denne måten ville programmet ha spredt seg til tusenvis av potensielle nettbankbrukere i løpet avkort tid. Hver gang en person gikk inn på sin nettbank, ville dataprogrammet plukke opp kodene og sende dem tilbake til ”Jon”.

Opplysningene fra ”Jon” ble grundig dobbeltsjekket. Dataingeniør Kristen Tande stod fram med navn og bekreftet metoden og skisserte flere mulige elektroniske innbrudd i nettbankene. Han beskrev i detalj sikkerhetshullene i Kredittkassens nettbank.

DnB ble konfrontert med Dagbladets test av sikkerheten i nettbanken. Informasjonssjef Thore Dyrdahl kommenterte at Dagbladets test i prinsippet kunne være ulovlig, men at banken på dette tidspunktet ikke ville forfølge dette videre. Ovenfor Dagbladets journalist gav han utrykk for at artikkelen kunne skade DnBs omdømme, men han kom ikke med noen form for trusler. Som en kommentar uttalte han. ”Vi tar ansvar i de tilfellene der kunden ikke har gjort noe direkte ulovlig eller grovt uaktsomt.”

Han opplyste også at banken ville endre ordlyden i kontrakten, slik at sikkerhetsansvaret mellom DnB og kunden ble klarere.

Tom Bolstad i Forbrukerrådet ble kontaktet for å utrede ansvarsforholdet mellom nettbanken og kundene i sikkerhetspørsmål. Han hevdet at kundene ville være beskyttet av finansavtaleloven som trådte i kraft 1. juli 2000.

Artikkel 2 stod på trykk 11.07.2000

Nettbank-testen:

Etter avsløringen av sikkerhetssvikt i enkelte nettbanker valgte vi så å ta en nøye gjennomgang av sikkerheten til de største aktørene i markedet. Er noen banker sikrere enn andre?

Siden krigen mellom sikkerhetseksperter og hackere blir tøffere, teknologien blir jo bare «bedre og bedre », valgte vi en teoretisk tilnærming når vi ville sammenligne bankenes sikkerhet. En systematisk gjennomgang av bankenes sikkerhetssystemer prøvd mot alle innbruddsforsøk kjent fra virkeligheten og alle kjente teoretiske muligheter for innbrudd i slike systemer ville gi den beste oversikt.

Med 134 nettbanker måtte utvalget begrenses. Vi valgte de største aktørene, i tillegg til Totenbanken, som bruker Fellesdata sitt nettbanksystem. Sistnevnte benyttes også av en rekke andre nettbanker.

All offentlig tilgjengelig informasjon om oppbygningen av disse nettbankene ble samlet inn. Kilder for dette var bankenes hjemmesider og informasjonsmateriell, søk i tekstarkiver, og kontakt med bankenes IT- og informasjonsavdelinger. Den direkte kontakten med bankene kunne være problematisk, siden de som kunne sakene ofte ikke hadde lov til å snakke, mens de som kunne snakke ofte hadde bare overfladisk kjennskap til området «Vår løsning er sikker»).

Deretter satte vi opp en liste over hvilke metoder for innbrudd i nettbanker som er a) kjent fra virkeligheten, og b) teoretisk mulige. Denne listen er satt opp på bakgrunn av omfattende litteraturstudier (faglitteratur, hackerbiografier, sikkerhetsforum på internett, arkivsøk osv.), omfattende samtaler med utviklere og konsulenter i internettbransjen, og ikke minst egen kunnskap til slike systemer. Bjørn Bore har i flere tidligere jobber arbeidet tett sammen med de første utviklerne av betalingssystemer på nett i Norge, og har selv utviklet flere nettjenester. Denne kunnskapen, og det omfattende kontaktnettet, kom selvfølgelig godt med.

Deretter ble hver nettbank i testen sjekket opp mot listen over kjente former for mulige angrep. Spørsmål og usikkerheter som oppsto underveis ble diskutert med bankene og med tidligere konsulterte sikkerhetseksperter. Vi brukte mye tid på dette arbeidet, og alle mulige former for angrep mot hver enkelt bank ble både diskutert med bankansatte, uavhengige eksperter og sikkerhetskonsulenter.

På grunnlag av dette ble så bankene rangert etter antall kjente svake punkter, hvor sterke skadebegrensende tiltak de hadde (størrelsesgrense på transaksjoner til utlandet o.l.), og i hvilken grad bankene hadde prioritert sikkerhet foran brukervennlighet/funksjonalitet i sine løsninger.

Ut i fra denne kunnskapen ble det også laget en kort liste for papir og en lengre for nett over hvordan nettbrukere kunne bedre sikkerheten i sin ende.

Sak 3 stod på trykk som oppslag 07.12.2000

Politikerne reagerer:

Dagbladets avsløringer om nettbankene medførte en strøm av reaksjoner på telefon, e-post og i form av leserbrev.

Arbeiderpartiets Ane Sofie Tømmerås, som var saksordfører for finansavtaleloven, ønsket å ta denne problemstillingen opp i justiskomitéen. Hun så det som viktig å sikre nettkundene det samme vernet som kortbrukerne. KrFs representant Finn Kristian Marthinsen ønsket også å ta

et initiativ for å få problemstillingen på dagsorden. Informasjonssjefene Tore Dyrdahl i DnB og Heidi Heltne ønsket også å rydde opp, slik at nettbrukerne kunne føle seg trygge.

DnB, som av opplagte grunner kom dårlig ut, reagerte på testen og kritiserte den for å ta mer hensyn til sikkerhet enn brukervennlighet. Banken slo allikevel fast at de tok ansvaret i tilfelle et innbrudd.

Sak 4 stod på trykk 14.07.2000

Dagbladet avslører omfanget av hacker-kontrollerte PCer:

Et viktig element for Dagbladets team var å kartlegge omfanget av datakriminaliteten rettet mot nettbanker. En ringerunde til informasjonssjefer og sikkerhetssjefer i de største bankene gav ikke noe resultat. Samtlige avviste at de hadde opplevd elektroniske innbruddsforsøk.

Det er tre mulige forklaringer på dette: a) Bankene har ikke opplevd noe elektronisk innbruddsforsøk i nettbankene. b) Bankene holder eventuelle innbrudd for seg selv. C) Innbrudd har forekommet uten at bankene har fått dette med seg.

Dagbladets team ble møtt av en anspent stemning blant bankpersonalet når vi ringte rundt. Kun informasjonssjefene fikk lov å uttale seg til pressen, ble det hevdet.

Direktør i Næringslivets Sikkerhetsråd, Helge J. Størkersen, kunne ovenfor Dagbladet bekrefte at bankene daglig var utsatt for hackerangrep. Dette var i hovedsak ufarlige angrep, men han uttalte til Dagbladets journalist at bankene ville holdt et eventuelt vellykket innbruddsforsøk for seg selv. ”De har alt å tape på å fortelle om det til media. Sikkerheten og tilliten er det de lever av.”

For å kunne gjennomføre det innbruddsforsøket som Dagbladet hadde avslørt, måtte en bankkundes PC være infisert av et hackerprogram av typen trojaner. Dette er et dataprogram som gjør hackeren i stand til å ta over kontrollen på den infiserte datamaskinen. Dagbladets team ønsket å kartlegge hvor mange PC-er som faktisk var infisert på denne måten. Metoden for å gjøre dette er et såkalt portskanningsprogram program.

Å starte et såkalt portskanningsprogram program, for å lokalisere infiserte datamaskiner, kan bli tolket som et forsøk på datahacking. Programmet kontakter maskiner koblet til nett for å se om en såkalt trojan har etablert seg. En god parallell til den virkelig verden er å ta i et dørhåndtak for å se om en dør er åpen.

Dagbladet kontaktet datasikkerhetsbedriften Norman og spurte om de var villige til å gjennomføre dette for avisen. Viseadministrerende direktør Jan Kristensen opplyste at bedriften ikke kunne ta på seg en jobb uten godkjenning fra eieren av nettverket, i hovedsak Telenor. Dagbladet kontaktet Telenor Nextel, men fikk et negativt svar. Dagbladets journalist ble truet med politianmeldelse dersom portskanning likevel ble gjennomført.
Telenor Nextel gjennomfører selv regelmessig portskanning, men resultatene av dette ville de ikke dele med Dagbladet. Opplysningene er heller ikke offentlig tilgjengelig på annen måte.

I et møte mellom journalist Kristian Sarastuen, leder for nyhetsavdelingen Terje Myklevoll og nyhetsredaktør John Arne Markussen, ble det bestemt at Dagbladet likevel skulle

gjennomføre portskanning. Retningslinjene var å telle antall infiserte maskiner, men ikke ta seg inn i noen av disse maskinene.

Konklusjonen var at dette var journalistisk nybrottsarbeid med hensikt å dokumentere en sikkerhetsrisiko i det norske samfunnet, og i henhold til intensjonene i redaktørplakaten.

Kristen Tande (se over) sa ja til å hjelpe Dagbladets team. Søkeprogrammet ble startet klokken 21 den 13.07.2000. Programmet var stilt inn på å finne maskiner åpnet av de ti mest kjente hacker-programmene. I virkeligheten er det hundrevis av slike programmer gratis tilgjengelig på internett. Da søket ble avsluttet klokken 24 hadde søkeprogrammet funnet 350 infiserte maskiner.

Samme kveld kontaktet journalist Sarastuen selskapet InfoStream, en av Norges største leverandører av nettjenester. Vakthavende dataingeniør opplyste at i Dagbladets søkeområde den kvelden var anslagsvis 2000 PC-er på nett. Ca. 17 prosent av PC-ene vi testet var med andre ord angrepet. Seniorkonsulent for datasikkerhet i Compaq, Peter Wahlman, opplyste at Dagbladets resultater av portskanning var i henhold til selskapets egne resultater.

Et forsiktig anslag over det totale antallet infiserte maskiner i Norge, ble utarbeidet på bakgrunn av Dagbladets resultat, tilsvarende søk gjort i Sverige og i samarbeid med sikkerhetseksperter hos Compaq og Norman. Konklusjonen er at minst 50 000 norske PC-er er åpnet av hackere. Trolig er tallet langt høyere.

Dagen etter ble Telenor Nextel kontaktet. Informasjonssjef Arne Cartridge opplyste at Dagbladet ville bli politianmeldt for portskanningen. Han innrømmet imidlertid at selskapet var klar over at hackerinfiserte datamaskiner var et økende problem.

Sak 5 stod på trykk i Dagbladet 17.07.2000

I tillegg til hovedsakene resulterte arbeidet i flere kommentar og debattinnlegg i Dagbladet, og noe overskuddsmateriale i form av andre artikler (noen er vedlagt).

Ressursbruk

Dagbladets artikkelserie spenner seg fra 10.07 til 17.07.

Sarastuen jobbet sammenhengende med dette stoffet fra 05.07 til 16.07. Ukjent antall overtidstimer. Bore begynte sitt arbeid med saken den 11.07 og jobbet sammenhengende med stoffet frem til 16.07. Ukjent antall overtidstimer. Gjerding jobbet med fakta og verifikasjon på den første artikkelen. Arbeidet fra 08.07 til og med 09.07.

Total tidsbruk er vanskelig å anslå, siden vi i slutten av perioden også jobbet med andre saker. Inkludert overtid blir minsteanslaget på fire regulære arbeidsuker.

Spesielle erfaringer
Saken om nettbankene var en av de første større sakene i Dagbladet med et tett samarbeid mellom nyhetsredaksjonen og nettutgaven. Vi valgte en slik samkjøring delvis fordi Bore er ansatt i nettredaksjonen, men også fordi det var helt klare journalistiske fordeler med det.

Nettutgaven ble brukt for å øke tipstilfanget, mulige tipsere er jo etter all sannsynlighet tunge nettbrukere. En samkjøring papir/nett ga oss også muligheten til å publisere stoff det rett og slett ikke var plass til i papirutgaven. Enkelte av sakene ble også kjørt først i nettutgaven, og ga oss muligheten til å få ut umiddelbare reaksjoner på sakene (eksempelvis «- Vi tar ansvaret» 12. juli).

Dagbladets team opplevde det som vanskelig å gjøre etiske vurderinger, når handlingene utført på vegne av oss eller gjennom en indirekte oppfordring, ligger i en juridisk gråsone. Vi ble blant annet truet med politianmeldelse av Telenor. I ettertid har vi ikke hørt noen ting og vi er også helt sikre på at vi holdt oss innenfor norsk lov og at handlingene var nødvendig for å avdekke sterkt kritikkverdige forhold i banknæringen.

Et annet problem er at de fleste kildene har noe å selge, enten produkter eller kompetanse. Det var få uavhengige og kompetente kilder. Dette medførte naturlig nok stor ressursbruk på faktaverifisering og kildekritikk. Vi oppdaget også hvor viktig det er i saker som handler om informasjonsteknologi å ha en grunnleggende og grundig forståelse av teknologien.

Konsekvenser

- Dagbladet kjenner til at minst to storbanker, DnB og Kreditkassen, endret ordlyden i sine standard kontrakter for nettbankkunder. Bankene har hevdet at kontraktene ble endret som en følge av den nye finansavtaleloven, men faktum er at kontraktene ikke var endret før 11.07, nesten to uker etter at loven var trådt i kraft. Forbrukerombudet forhandler nå med banknæringa om ordlyden i disse kontraktene. Forhandlingene ventes sluttført høsten 2001. Dagbladet vil følge saken videre.

- Dagbladet kjenner til at det ble utført en omfattende gjennomgang av sikkerhetssystemene i de store nettbankene, etter avsløringene. ”Dere vet ikke hvor mye arbeid dere har kostet oss.” (Ansatt i IT-avdeling i storbank). Flere banker, blant annet Skandiabanken, har vurdert å endre sine løsninger og ta i bruk sikkerhetssystemer anbefalt i Dagbladets test. Vi regner med å gjenta testen.

- Dagbladet avdekket at bankkunder har en svakere beskyttelse i lovverket enn kortkunder. Saksordfører for finansavtaleloven, Ane Sofie Tømmerås, varslet en gjennomgang av lovverket, for å likestille nettkundene med kortkundene. Barne- og familieminister, Karita Bekkemellem Orheim, skrev på kommentarplass i Dagbladet at en slik gjennomgang kunne bli aktuell. Vi vil følge opp denne saken.

- Avsløringene førte til nye avsløringer om sikkerhetshull i nettbankene. Mest alvorlig var hullet i Sparebanken NOR, der kontopplysningene til samtlige kunder lå tilgjengelig på nettet, for alle som hadde passord i banken. Saken stod på trykk 30. august.

Oslo 18/1 2001

Kristian Sarastuen Bjørn K. Bore May Linn Gjerding