

## Snarvei til bedre sikkerhet

*“Javisst har vi sikkerheten under kontroll.” Situasjonen har forandret seg radikalt de siste tre årene. Oppmerksomheten rundt sikkerhet har flyttet seg helt opp på styrerommet i store og mellomstore virksomheter. Med oppmerksomhet følger tiltak.*

Mens mellomstore og store virksomheter og betydelige deler av forvaltningen har fått sikkerheten under kontroll, er situasjonen langt fra like ryddig i ‘underskogen’: Småbedrifter i alle slags bransjer, skoler, ideelle organisasjoner – og større virksomheter som i utgangspunktet befinner seg langt fra teknologien. For de fleste av disse er IT et verktøy på linje med andre produksjonsmidler – de mangler IT-kompetanse og innsikt på samme naturlige måte som et bilbud-firma mangler mekanikere. I motsetning til hva tilfellet er for budfirmaet, er det imidlertid langt mellom kompetente servicestasjoner og verksteder på IT-siden – spesielt når vi kommer inn på sikkerhet.

### Liten fortropp, stor baktropp

At denne situasjonen sakte, men sikkert forandrer seg, endrer ikke det faktum at tusenvis av virksomheter står på relativt bar bakke med hensyn til IT-sikkerhet: De får levert sine systemer og nettverk, et Internett-abonnement og en ruter – og antar at leverandøren er kompetent nok til å besørge det som skal til for å fungere. Sikkerhet har de ikke noe forhold til – før virusangrep, innbrudd eller tap av data er et faktum.

Denne gruppen er mest utsatt, men den er ikke alene om å fortsatt henge etter på sikkerhetssiden. Tallrike virksomheter med egen driftskompetanse og betydelig IT-erfaring, har utsatt og utsatt en overmoden opprydding på sikkerhetsfronten: Det blir for lite tid, for tynt med ressurser og for mange branner som skal slukkes i det daglige. Ute av syne, ute av sinn – og sikkerheten får ligge, gjerne til katastrofen er et faktum. Da kommer boomerangen tilbake med voldsom kraft, og sørger for at tid og penger spart gjennom å skyve problemene foran seg, blir for smuler å regne.

Det bisarre i situasjonen er at grunnleggende sikkerhet koster lite. Verktøy og mekanismer er på plass allerede, men benyttes ikke – fordi ingen har tatt seg tid til verken å bringe trusselbildene på det rene eller å skaffe oversikt over hvordan de bør håndteres. I denne artikkelen diskuterer vi hvordan forholdet bør angripes, hvilke elementer som er viktigst for å komme fra liten sikkerhet til et fundament som tilsvarer låste dører og stengte vinduer. Avslutningsvis ser vi på naturlige veier videre – den største utfordringen er også i denne sammenhengen å komme i gang. Når grunnmuren står der, er det lettere å ta fatt på reisverket.

## Myter og misforståelser

Ikke minst når vi diskuterer grunnleggende sikkerhet, møter vi hyppig følgende tre 'sannheter' eller antagelser knyttet til arbeidet som må gjøres:

- ✓ **Sikkerhet er vanskelig** – det krever bred og grundig kunnskap på en rekke områder.
- ✓ **Sikkerhet er kostbart** – vi har ikke råd til å investere titusenvis av kroner i brannmurer og innbruddsalarmer.<sup>12</sup>
- ✓ **Sikkerhet er svært tidkrevende** – vi har ikke den tiden som kreves for å etablere god sikkerhet.

Alle tre er korrekte dersom målet er å etablere full – maksimal – sikkerhet. Et slikt nivå er det imidlertid få som har råd til og enda færre som har behov for. Riktig sikkerhet for de fleste virksomheter er på et noe lavere nivå – som fortsatt krever ressurser, men i en annen størrelsesorden. **Det viktigste poenget er imidlertid at for etablering av grunnleggende sikkerhet er alle tre påstandene ovenfor uriktige.**

### Ingen røk uten ild

Påstandene har med andre ord sin opprinnelse i høyst reelle forhold: Sikkerhet kan være både komplisert, tidkrevende, kompetansekrevene og kostbart. IT-sikkerhet kommer ikke i noen særstilling i så måte. Det som har forandret seg de siste årene, er for det første tilgjengeligheten av frie verktøy og dermed mulighetene vi har til å beskytte oss, og for det andre truslene vi står overfor.

I Mellvik-Rapporten nr. 86 (august 2001) presenterte vi en samling slike verktøy, som hver på sin måte kan bidra til å heve sikkerhetsnivået dramatisk.<sup>13</sup> Internettet er et veritabelt skattkammer i så henseende, med tusenvis av verktøy som i mange tilfeller konkurrerer fordelaktig med kommersielle alternativer, både funksjonelt og på andre måter. De er imidlertid uten verdi før vi har investert tid i å finne dem, lære dem å kjenne, og deretter installert, testet og satt dem i drift.

Tiden som må investeres er omtrent den samme, uansett om vi har med kommersielle eller frie verktøy å gjøre, og det er ingen tvil: Den er betydelig. Utvelgelse, installasjon og drift av verktøy for IT-sikkerhet er med andre ord både kompetanse- og tidkrevende, slik påstandene ovenfor postulerer – et nedslående faktum inntil vi kommer til den erkjennelse at etablering av grunnleggende sikkerhet ikke forutsetter slike verktøy.

### Hvor finnes verktøyene?

Viktige nettsteder med oversikter over tilgjengelige sikringsverktøy:

- <ftp://coast.cd.purdue.edu/pub/tools>
- <ftp://ftp.porcupine.org/pub/security/>
- [http://cert.org/other\\_sources/tool\\_sources.html](http://cert.org/other_sources/tool_sources.html)
- <http://www.atstake.com/research/tools>

## Med blanke ark

Vi skal se at beskjeden innsats kan gi store resultater, uten å hente inn verktøy verken fra Internettet eller leverandører. Faktum er at om vi tar for oss veien fra ingen IT-sikkerhet til god – eller fundamental –

<sup>12</sup> Apropos innbruddsalarmer og innbruddsdeteksjon: I neste utgave av Mellvik-Rapporten (se baksiden) begynner vi en serie i tre deler som diskuterer nettopp dette området – som er både undervurdert og misforstått i markedet.

<sup>13</sup> Se også artikkelen "Kontrollér sikkerheten gratis" i Mellvik-Rapporten nr. 7 (august 2000).

IT-sikkerhet, kommer vi anslagsvis 80% av veien til målet med svært enkle midler.

All sikkerhet er relativ – i forhold til trusler, risiko og eksponering. Åpne dører, det vil si ingen sikring, virker som en magnet på 'tilfeldig forbipasserende snoker'. Dørene skal imidlertid ikke mer enn lukkes for å sende halvparten av dem videre til neste objekt. Med lås, alarmer og andre tiltak hever vi nivået ytterligere, men med stadig mindre effekt i forhold til investeringene.

### Historisk sløvhhet

Den viktigste årsaken til at vi i 2002 kan karakterisere situasjonen innen IT-sikkerhet generelt som utilfredsstillende, er historisk: Både leverandører og marked har hatt fokus på funksjonalitet og brukervennlighet, mens sikkerheten i beste fall har kommet i andre eller tredje rekke.<sup>14</sup> Selv for produkter som leveres i dag, er det regelen snarere enn unntaket at sikkerhetsmekanismene er slått av fra leverandørens side, og må eksplisitt aktiviseres for å ha noen effekt.

Dette er i seg selv alvorlig, og forverres ytterligere av det faktum at systemer typisk leveres med all verdens nettverkstjenester aktive. At nettverket står åpent er ille, og når systemene i tillegg står med alle dører på vidt gap, er det ikke underlig at innbrudd og vandalisme florerer.

Når nøden er størst, er imidlertid hjelpen nærmest, og det er her vi kommer tilbake til mytene ovenfor: Vi har verktøyene vi trenger for å komme i gang – på systemer, rutere, klienter og svitsjer. Utfordringen knyttet til etablering av grunnleggende sikkerhet er å investere et minimum av tid for å forstå hvordan de skal brukes, aktiviseres og holdes ved like. Dette fordrer et minimum av innsikt og interesse, og en del tid – som er vel anvendt. Det er temmelig meningsløst at vi låser våre dører og vinduer med den største selvfølgelighet, mens vi lar mot-orveien passere gjennom våre livsnødvendige IT-systemer.

En enkel strategi for etablering av grunnleggende sikkerhet består av fem hoveddeler:

- ✓ Sikring av nettverket – i første omgang aksessrutere som forbinder det interne nettverket med verden utenfor. I andre omgang – og gitt at nettverket er omfattende nok til å bestå av flere segmenter sammenknyttet med svitsjer eller rutere – er det ønskelig å foreta en partisjonering, som gir et styrket dybdeforsvar.<sup>15</sup>
- ✓ Sikring av tjenere: Fjerning av unyttige og/eller utsatte nettverkstjenester, trafikkfiltrering, bedre autentisering, kontroll av brukerregistreringer, etc.

<sup>14</sup> Bill Gates' ferske utspill som setter sikkerheten i høysetet hos Microsoft, er et glimrende eksempel – se egen kommentar på side 29.

<sup>15</sup> Se "Partisjonering: Effektiv nettverksikkerhet" i Mellvik-Rapporten nr. 77.

- ✓ Sikring av klienter – mange av de samme trinnene som for tjenerne: Fjerne tjenester og brukere, etablere trafikk-filtrering og så videre.
- ✓ Vedlikehold av programvare: Finnes det oppdateringer av operativsystemer og/eller andre programvarekomponenter som er av sikkerhetsmessig betydning, er det viktig å få dem på plass snarest.
- ✓ Mer pålitelig autentisering: En så enkel sak som passord representerer fortsatt et sikkerhetsmessig hull av dimensjoner, spesielt i små organisasjoner: Der brukerne mangler elementær innsikt i sin egen rolle og betydning for sikkerheten, er det få som forstår viktigheten av å ha passord i det hele tatt. Praksisen blir deretter.

### Passord, passord, passord

På veien mot 100% sikkerhet, som ikke betyr absolutt sikkerhet, men optimal sikring i forhold til risiko og behov, representerer passord hele 50%. Et bedre eksempel på at liten tue kan velte stort lass, finnes knapt. Likeledes illustrerer dette hvor lite som egentlig skal til for å bevege seg fra ingen til betydelig sikkerhet:

- ✓ **Motivasjon:** Når brukerne forstår sin rolle, sitt ansvar og risiko-momentene, er mye vunnet. Dersom de samtidig får forståelsen av hva som er gode og dårlige passord, og hvordan de selv kan lage gode passord som er enkle å huske, har vi etablert grunnleggende sikkerhetsbevissthet. Den positive innstillingen som følger av en slik bevisstgjøring, må vedlikeholdes gjennom jevnlig påminnelser – med eksempler på hva vi har vunnet, spart oss for, og hvordan det har gått med andre som har vært mindre flinke. Slike historier koster ingen ting, de kommer jevnlig tikkende inn via pressen.
- ✓ **Verktøy:** Uansett hvilke plattformer vi benytter, er de i dag utrustet med verktøy og mekanismer som hjelper oss å kvalitetssikre passordene. Sørg for å ta dem i bruk og at brukerne forstår hvorfor de er der: Minimum lengde, sammensetning, varighet, gjentakelser etc.

#### Enkle regler for gode passord

- Passord skal aldri skrives ned, lagres i klartekst, deles med andre eller lagres i applikasjoner.
- Bruk ikke samme passord i ulike sammenhenger, for eksempel hjemme og på jobben.
- Gode passord er minst 8 tegn lange, inneholder tall og spesialtegn, store og små bokstaver, skiftes jevnlig (kvartalsvis er bra) og gjenbrukes aldri.
- Lag enkle huskereglene for passordene – første-bokstaver i en setning er en god metode: "Min Honda har 4 hjul og er Blå": MHh4hoeB, "Jeg besteg Besseggen i 97!": 9jbBSGni7!. Programmer som foreslår gode passord er tilgjengelige for de fleste plattformer.
- Bruk kontrollprogrammer som kontrollerer passordene, innbrytere gjør det!

- ✓ **Kontroll:** Som en ytterligere forsikring mot dårlige passord, er kontrollprogrammer til stor nytte. En slik ekstra kontroll hører imidlertid naturlig hjemme i andre fase av sikringsjobben: Den kan utsettes, men ikke glemmes.

### Filtrering

Alt moderne nettverksutstyr har filtreringsmekanismer innebygget, og har – i motsetning til hva situasjonen var for 3-5 år siden – tilstrekkelig kapasitet til å utføre slik filtrering uten merkbare konsekvenser for ytelsen. Når Internett-forbindelser etableres, er

det vanlig – men ingen selvfølge, at leverandøren undersøker behovene og definerer et filter i henhold til dette. Selv der dette blir gjort, er det imidlertid sjelden filteret er godt nok: For å unngå klager om tjenester som ikke fungerer, vil leverandørene gjerne legge inn åpninger for hva de tror kan bli brukt i stedet for å dekke kun det konstaterte behovet. Dessuten er det et faktum at behovene forandrer seg.

Derfor er det nødvendig å vedlikeholde slike filtre jevnlig. Vi begynner med å finne ut hvordan situasjonen ser ut i dag og å kartlegge behovet. Det er bedre å stenge for mange hull og å åpne dem i henhold til behov, enn å tro at de trengs og la dem stå åpne.

Alle utstyrsleverandører har sin egen måte å representere slike filtre på, og kompleksiteten kan være for stor til at det er nyttig å bruke tid til oppbygging av ekspertise på området. En raskere vei til målet er å kjøpe den kompetansen som skal til – fra leverandøren eller fra en selvstendig part.

Filtrering er ikke det samme som en brannmur, men grensen mellom dem er glidende. I forbindelse med etablering av grunnleggende sikkerhet, er målet å utnytte de filtreringsfunksjonene som allerede finnes. En 'ekte' brannmur kommer inn når vi skal videre – fra en 80% til en 100%-løsning.

### Sikring av tjenere

Sikring av tjenere handler først og fremst om å rydde opp – fjerne tjenester og programmer som ikke brukes, brukere som ikke er aktive, og å rydde opp i konfigurasjonsfiler. I tillegg til å ha enorm betydning for sikkerheten, gir dette uten unntak også en effektiviseringsgevinst: Aktive tjenester spiser ressurser, selv om de aldri brukes, spesielt på Windows-plattformer.

Hvordan dette gjøres, kommer an på plattformen. Windows NT og 2k har en 'services-manager' som kontrollerer hvilke tjenester som skal startes og hvordan. I Unix og Linux ligger tekstbaserte konfigurasjonsfiler til grunn, som kan endres direkte eller via grafiske verktøy.

For driftsansvarlige – med eller uten erfaring innen sikring – er dette kjente operasjoner som knapt representerer noen utfordring verken kompetansemessig eller praktisk. Helt uten bakgrunn eller hjelpemidler er det imidlertid ikke nødvendig å starte. I tillegg til den flora av sikringsverktøy vi nevnte innledningsvis, finnes det også dokumentasjon, veiledninger og oppskrifter som adresserer nettopp disse oppgavene.

**NFS** – Network File System (Unix/Linux)

**SMB** – Server Message Block (Microsoft LAN Manager)

**SMTP** – Simple Mail Transfer Protocol

**SNMP** – Simple Network Management Protocol

**FTP** – File Transfer Protocol

**RPC** – Remote Procedure Call

**TFTP** – Trivial File Transfer Protocol

**HTTP** – Hyper Text Transfer Protocol

#### Praktisk sikring av tjenere

Sikring av tjenere går i første rekke ut på å fjerne tjenester som ikke brukes, dernest å blokkere trafikk som er uønsket. I denne sammenheng er første gruppe av størst interesse, og fremgangsmåten – uansett operativsystem – blir som følger:

- Bestem eller finn ut hva som er tjenerens oppgave(r). Færre oppgaver per tjener er bedre – det gir oversikt, robusthet og enkelhet. Spesielt tjenere som er synlige utenfra (fra Internettet) er kritiske i så måte. En Web-tjener skal være kun det, ingen ting annet.
- En del typiske tjenester som dukker opp i den forbindelse er SMTP (epost-tjener), SNMP (klient for styringsverktøy – normalt dårlig sikret og meget utsatt), DNS (navnetjener), FTP (tjener for filoverføringer), SMB/Samba (tjener for Microsoft fildeling/deling av printere), LPD (print-tjener), RRAS (ruting og fjernaksess i W2k), telnet (innlogging via nettverket), SQL Server (tjenesten avhenger av leverandør), NFS (Unix fildeling), Web-tjener, telefaks- og telefoni-tjenester.
- Slå av eller fjern disse tjenestene der de ikke brukes. Dette gir ikke bare bedre sikkerhet, men også bedre ytelse.
- De mest risikable tjenestene er (i denne rekkefølgen) DISCARD, CHARGEN [IP-tjenester laget for testing, perfekte for såkalte Denial of Service angrep], RPC, SNMP, SMTP, NFS, Finger, TFTP, HTTP, Telnet. De fleste av dem kan blokkeres uten videre for de fleste tjenere. De to førstnevnte skal også blokkeres i rutere og annet sammenkoblingsutstyr.
- På Windows-maskiner som ikke skal dele verken filer eller utskriftstjenester, fjernes disse.
- Ytterligere detaljer samt anvisninger på hvordan sikringen skal utføres i praksis, finnes i litteraturhenvisningene på neste side.

Videre finnes det utallige bøker som diskuterer praktisk sikring av systemer og nettverk for alle tenkelige plattformer og utstyrstyper.

I denne jungelen av kunnskapskilder – med generelt høy kvalitet, anbefaler vi følgende for å komme raskt og effektivt til målet:

- ✓ Organisasjonen SANS Institute – [www.sans.org](http://www.sans.org), er den viktigste kilden. Vi har tatt frem denne organisasjonen ved en rekke anledninger her i Mellvik-Rapporten, som tilbyr det ypperste av opplæring, publikasjoner og fritt tilgjengelig materiale via Internettet.
- ✓ Blant plattformspesifikke veiledninger med fokus på grunnleggende sikkerhet hos SANS Institute, vil vi spesielt trekke frem følgende:
  - Securing Windows 2000 Server* [[rr.sans.org/win2000/sec\\_server.php](http://rr.sans.org/win2000/sec_server.php)]
  - A Simple and Effective Path to Improving NT Security* [[rr.sans.org/win/path.php](http://rr.sans.org/win/path.php)]
  - Securing Linux Installations* [[rr.sans.org/linux/sec\\_install.php](http://rr.sans.org/linux/sec_install.php)]
  - Securing HP-UX 11* [[rr.sans.org/unix/HP-UX11.php](http://rr.sans.org/unix/HP-UX11.php)]
  - Securing Solaris* [[rr.sans.org/unix/sec\\_solaris.php](http://rr.sans.org/unix/sec_solaris.php)]
- ✓ Sist, men ikke minst har SANS utarbeidet hefter med såkalte 'step-by-step' veiledninger for sikring av de meste populære plattformene: NT, Windows 2000, Linux og Solaris. Heftene er på ca. 100 sider, koster ca. USD 50 per stk. og er vel verdt investeringen. De er også tilgjengelige i PDF-format til en noe høyere pris, avhengig av antall brukere.
- ✓ For Linux-miljøer er [www.linuxsecurity.com](http://www.linuxsecurity.com) et oppkomme av gode ideer og praktiske råd med hensyn til såvel grunnleggende som avansert sikkerhet.
- ✓ Flere pekere – for alle plattformer – er lagt ut på vår Web-tjener, se side 35 for detaljer.

### **Sikring av klienter**

Sikring av klienter er like viktig som bevisstgjøring av brukerne: Feilaktig eller mangelfullt konfigurerte klienter har et like stort potensiale for misbruk som tilsvarende tjenere.

Metodene er omtrent de samme som for tjenere – med det unntak at Windows-plattformer før NT 4.0, dvs. 9X, ME og 3.x, ikke lar seg sikre. At de også har færre tjenester tilgjengelige for andre brukere på nettverket hjelper, men det er like fullt et faktum at disse plattformene ikke er forenlige med god sikkerhet – med mindre de utelukkende brukes som grunnlag for Windows-terminaler. For klienter kan vi dermed gjøre følgende observasjoner:

- ✓ Oppgrader eldre Windows-plattformer til W2k [Windows XP er fortsatt en relativ nykommer i sikkerhetsmessig forstand].
- ✓ Bruk av Terminal Server løsninger gir bedre kontroll over sikkerheten, og mindre avhengighet av klientplattformens sikring.

- ✓ Klientene sikres etter samme mal som tjenere, med vekt på eliminering av unødige tjenester og programvare.
- ✓ For Windows-systemer er det viktig å sørge for at *Registry* for det første ikke er tilgjengelig fra nettverket, og for det andre er satt til optimale verdier sett fra et sikkerhets-synspunkt. Referansedokumentene ovenfor gjennomgår hvordan dette gjøres.

## Oppsummering

Vi kan oppsummere den effektive veien fra minimal IT-sikkerhet til et godt fundament – til 80%-løsningen – i følgende punkter:

- ✓ Bevisstgjøring av brukerne: De skal forstå hvorfor sikkerhet er viktig, hvorfor deres passord er av betydning for virksomheten og sin egen rolle i totalbildet.
- ✓ Kontroll og bytte av passord for alle brukere, fjerning av inaktive brukere.
- ✓ Aktivisering av mekanismer som sørger for gode passord som byttes regelmessig.
- ✓ Filtrering av trafikk fra eksterne nettverk. Kun tjenester og systemer som skal være tilgjengelige eksternt, skal være synlige. All annen trafikk filtreres.
- ✓ Sikring av tjenere: Fjerne tjenester som ikke benyttes, plassere interne tjenester der de hører hjemme, aktivisere aksess-kontroll til viktige ressurser, sørge for at administrasjonskonti kun er tilgjengelige for de som trenger slik tilgang.
- ✓ Sikring av klienter: Også her fjernes tjenester som ikke benyttes, eliminere usikre plattformer.
- ✓ Kontroll av programvare-versjoner:

## Veien videre

Dette er snarveien – den rimelige, raske og effektive veien fra en høyst risikabel åpenhet til 80% sikkerhet. Et formidabelt fremskritt uansett synsvinkel. Men er det godt nok? Kan vi nå lene oss tilbake og hevde at sikkerheten er ivaretatt?

Situasjonen kan beskrives med følgende analogi: Vi har en bil, og har nå lært oss hvordan vi skal ta ut nøkkelen og vri om låsen når den forlates. Mens fremskrittet er stort, vet de fleste av oss av erfaring at dette kun er tilstrekkelig dersom vi befinner oss på et avsidesliggende sted der få eller ingen ferdes. I en Internett-verden finnes ikke slike steder. Våre virtuelle naboer befinner seg fysisk i Kina, India, Russland og Strømstad. Tilgjengeligheten er uavhengig av geografi, og kun til en viss grad begrenset av båndbredde.

Med andre ord er det naturlig – og nødvendig – å betrakte den grunnmuren vi har bygget som nettopp det: Fundamentet for videre bygging. Vi må videre, trinn for trinn, til vi når et nivå som står i riktig forhold til de verdiene som skal beskyttes. Hvor dette nivået er, vil vi i mange tilfeller ikke vite før vi er kommet et stykke på vei: Vi møter en smerte-

grense som representerer balansepunktet mellom medisin og sykdom, mellom trusler og verdier. På veien dit skal vi blant annet innom følgende områder:

- ✓ Brannmurer og viruskontroll
- ✓ Passordknekkere for løpende kontroll av brukernes passord
- ✓ Verktøy for løpende kontroll av nettverks- og systemsikkerheten
- ✓ Nettverkspartisjonering
- ✓ Innbruddsdeteksjonssystemer
- ✓ Sikring av fjernaksess-brukere (VPN, personlige brannmurer)
- ✓ Policy, retningslinjer og standarder – for organisasjonen, for den enkelte, for verktøy, for bærbare systemer, for hjemmebrukere

Uansett hvilke teknologiske mekanismer og verktøy vi setter i sving, og helt uavhengig av hva de koster, er det vårt fundament som avgjør om de har noen verdi. Den første 'femti-prosenten' vil alltid være den samme: Brukerne, deres holdninger og deres passord – eller tilsvarende autentiseringsmekanismer. ■