

Gratis sikkerhet

Det heter seg at ingen ting er gratis. De fleste av oss har erfart at så er tilfelle – med enkelte unntak. Dessuten – unntakene som bekrefter regelen er subjektive: Det én av oss vil kalle gratis er ikke nødvendigvis gratis for den neste. Spesielt når vi kommer inn på verdien av tid, blir det fort sprik mellom oppfatningene.

Ikke gratis, kanskje billig?

Tid er penger. Produkter som ikke koster noe, eller som er spesielt rimelige, har pådratt seg en kostnad idet vi begynner å bruke tid på dem. Dersom samsvaret mellom oppgave/problem og produkt er godt og kvaliteten er god, kan det være noe å spare i forhold til et alternativ som koster penger, med mindre terskelen for å ta produktet i bruk er så høy at vinningen går opp i spinningen.

IT-sektoren utmerker seg i forhold til andre bransjer på en rekke områder, også med hensyn til tilgangen på gratis-produkter: Programvare innen alle tenkelige kategorier er fritt tilgjengelige via Internettet, på CD-plater som deles ut i øst og vest, i magasiner og bøker, og via andre kanaler. Kvalitet og nytteverdi spenner like vidt som anvendelsesområdene – fra gullkorn til søppel, fra operativsystemer til spill.

Fokuseringen på dette fenomenet har tiltatt voldsomt de siste årene, i parallell med at Linux har gått sin seiersgang over store deler av verden. Som vi har diskutert tidligere i Mellvik-Rapporten, er Linux blitt selve symbolet på fri programvare – fortjent eller ufortjent. Fokuseringen har blant annet avdekket at de frie produktene ofte holder høy kvalitet, i enkelte tilfeller like bra eller bedre enn kommersielle alternativer. At dette bestrides på det sterkeste av leverandørene som blir truffet, er ikke bare naturlig, men også en understrekning av at konkurransesituasjonen er reell.

Ved siden av å konkurrere med kommersiell programvare, dekker de frie produktene segmenter og områder som ikke adresseres på annen måte. Sikkerhet er interessant nok et eksempel her: Til tross for stor oppmerksomhet fra marked og leverandører, er det fortsatt et faktum at god sikring og overvåking fordrer bruk av fri programvare. Faktisk er det slik at en rekke av de mest prominente kommersielle produktene i segmentet, har sin opprinnelse som nettopp frie verktøy (OSS, *Open Source Software*).

'Fritt' og 'gratis' blir imidlertid fort kostbart dersom vi skal bruke tid på å lete oss frem til de beste produktene og de som stemmer overens med våre behov. En rekke bøker, magasiner og nettsteder er til god hjelp i så henseende – og yter betydningsfulle bidrag både når vi er på søken og når ett eller flere verktøy skal testes eller settes i drift. Dessuten – og like viktig: Fri programvare har tradisjonelt hatt ord på seg for å være vanskelig å bruke – laget av eksperter for eksperter. Denne karakteristikken er ikke lenger dekkende. Fri programvare har gjen-

nomgått en veritabel ansiktsløfting på brukergrensesnitt-siden de siste årene, og kvalifiserer oftere til gode karakterer enn det motsatte i dag. Spesielt populært er det blitt å gi verktøyene Web-grensesnitt, hvilket er positivt uansett synsvinkel, i tillegg til å være relativt enkelt for utviklerne å håndtere.

Om vi begrenser oss til området sikkerhet, er situasjonen at brukerne, dvs. system- og sikkerhetsansvarlige, har behov for opplæring i konfigurering og bruk, uansett hvor verktøyet kommer fra. Om vi postulerer at brukerterskelen (brukergrensesnittet), egenskapene, dokumentasjonen eller tilgangen på opplæring er den samme for kommersielle og frie produkter, blir det innlysende at de frie alternativene må vurderes nøye. Diskusjonen om hvorvidt et slikt postulat stemmer med virkeligheten, vil aldri legge seg, men det er interessant å legge merke til at det som regel er detaljer og enkelttilfeller som havner i fokus.

Bredde og dybde

Sikring av systemer og nettverk er en omfattende affære der en rekke programmer, mekanismer og utstyr skal spille sammen og utgjøre det vi ofte kaller et forsvarsverk. Selv om det er mulig, er det optimalt kun for små og teknisk kompetente miljøer å besørge hele sikkerheten via frie verktøy. For eksempel er det mulig for en oppegående systemansvarlig å konfigurere og drive en Linux-basert brannmur – gjerne på en avdanket PC – som ikke står tilbake for kommersielle alternativer på noe punkt, og dessuten koster minimalt.

I diskusjonen nedenfor har vi plukket ut en håndfull områder som er godt dekket av frie, selvstendige verktøy. Å ta dem i bruk er i de fleste tilfeller overkommelig med hensyn til tid og omfang, og det er lett å se deres effekt og nytteverdi. Videre er smitte-effekten vanligvis stor: Positive erfaringer med ett eller noen få verktøy frister til å ta i bruk flere. For system- og sikkerhetsansvarlige som ønsker å utvikle seg videre på området, er erfaringene og kunnskapene som bringes til torgs i prosessen, stimulerende nok til å gi mer smak.

Den naturlige prosedyren vil i mange tilfeller være:

- ✓ Å ta i bruk utvalgte frie verktøy for å bygge opp erfaring med systemer, nettverk og omgivelser.
- ✓ Bygge opp erfaring med verktøyenes egenskaper, muligheter, sterke og svake sider – et faglig fundament for senere evaluering av andre verktøy, frie eller kommersielle.
- ✓ Frie verktøy gir raskt resultater og er gode kortsiktige løsninger.
- ✓ For langsiktige løsninger er det viktig å gå grundig til verks, analysere behovene, sammenligne verktøy og velge kvalifisert.

Boken "Linux System Security" er et viktig referanseverk i forbindelse med sikring av Linux-systemer og etablering av Linux-baserte brannmurer. [Av Scott Mann, Ellen Mitchell, Prentice Hall 2000, ISBN 0-13-015807-0].

Kategorier og verktøy

Vi tar for oss følgende områder/kategorier:

- ✓ **Ekstern kontroll:** Port-skanning og hullsøking – se introduksjon og detaljer om utvalgte verktøy i artikkelen “Test nettverket – gratis” i Mellvik-Rapporten nr. 75.
- ✓ **Beskyttelse:** Personlige brannmurer – ‘trafikkkontrollører’ og filtre for enkeltstående maskiner og små nettverk, et tema vi diskuterte i detalj i artikkelen “Skal det være en personlig brannmur” i Mellvik-Rapporten nr. 75.⁷
- ✓ **Overvåking:** Nettsniffere – som lytter på – og analyserer – nettverkstrafikken
- ✓ **Intern kontroll:** Verktøy for systemadministratorer – passordkontroll, styring av privilegier, logging av aktiviteter mm.

Med unntak av brannmurer kan de fleste verktøy ha like stor verdi for angripere som for forsvarere. De er like gode i offensiv som i defensiv sammenheng, et faktum enkelte har vanskelig for å forsones seg med. I Forsvaret er sammenhengene imidlertid en selvfølge: Kanoner er like viktige for forsvarsrollen som for angriperrollen. At et verktøy brukes av Crackere er med andre ord intet argument mot verken kvalitet eller egnet i en forsvarsrolle – snarere tvert imot.

Tabell 1 Oversikt over verktøy-kategorier og aktuelle, frie produkter.

Kategori	Navn	Funksjon	Plattformer ^a	Referanse
Ekstern kontroll	Nessus		Unix, Linux	www.nessus.org
	SAINT	Portskanning, søking etter kjente svakheter og hull, signatur-skanning	Unix, Linux	www.wwdsi.com
	SARA		Unix, Linux	www.www-arc.com
	Nmap	Portskanning	Unix, Linux, NT	www.insecure.org
	Strobe	Portskanning	Unix, Linux, NT	ciac.lnl.gov
Beskyttelse	ZoneAlarm	Brannmur for individuelle PCer	Windows	www.zonelabs.com
	BlackIce Defender			www.networklce.com
	TCP Wrapper	Kontroll av inngående forbindelser, aksept/avvisning iht. definert policy	Unix, Linux	Inkludert i de fleste Linux- og Unix-systemer
	Port Sentry	Tilpasser forsvaret løpende iht. data fra TCP Wrapper	Unix, Linux	www.psionic.com
Overvåking	Logcheck	Løpende kontroll av loggfiler, med automatisk håndtering av definerte hendelser	Unix, Linux	
	tcpdump, ipwatch, snoop, netwatch	Verktøy for tapping av nettverkstrafikk	Medfølger hhv. Linux/BSD Unix, AIX, Solaris, NT/W2k	
Intern kontroll	Tripwire	Kontrollerer og varsler illegale aktiviteter på systemer, rutere, web-sider mm.	Unix, Linux, NT, W2k	www.tripwire.com

a. Merk at plattformene et verktøy kjører på ikke sier noe om hvilke plattformer verktøyet kan teste. De fleste skanneverktøy kan dirigeres til å søke etter svakheter knyttet til alle populære operativsystemer. Videre er enkelte verktøy delt i en klient og en tjenerdel. Plattformspesifikasjonen gjelder da for tjener-delen.

⁷ På web-siden for Mellvik-Rapporten nr. 75 viser vi en tabelloppstilling av et utvalg kommersielle verktøy for personlige brannmurer.

Av de fire gruppene i listen ovenfor ser vi at én – beskyttelse – er passiv, mens de andre er kontrollerende og potensielt proaktive. Distinksjonen er vesentlig: Alle trenger beskyttelse, og beskyttelsestiltak hører hjemme i enhver sammenheng – også på private hjemme-maskiner og nettverk på 'gutterommet'. Det betyr at vi må stille spesielle krav for denne kategorien med hensyn til usynlighet og enkelhet i installasjon og drift.

Den andre gruppen er verktøy for drifts- og sikkerhetsansvarlige – hvis bruksverdi er avhengig av plattform og hvor i nettverket det plasseres. Det optimale er naturligvis i mange tilfeller en bærbar maskin som kan flyttes etter behov. Dessuten er det et faktum at Linux er en ideell OS-plattform for et slikt system: Praktisk talt samtlige frie verktøy er laget for eller støtter Linux, og er enklest å installere på denne plattformen. Det betyr ikke at andre plattformer er utelukket: Som vi skal se nedenfor, er en rekke av verktøyene tilgjengelige på flere plattformer.

Ekstern kontroll

Gruppen 'ekstern kontroll' er den største i denne sammenheng – med god grunn: Det er her ethvert angrep begynner – med å kartlegge svakheter og hull, samle informasjon om nettverk og systemer, og etablere et bilde av topologien. Første gangs bruk av slike kontrollverktøy (som ofte kalles 'skannere' eller 'portskannere', til tross for at de fleste kan betydelig mer enn bare å 'skanne porter') er uten unntak en overraskelse for brukeren: De færreste har i forkant det fjerneste begrep om hvor mye nyttig informasjon som kan samles på denne måten – raskt, effektivt og i noen tilfeller uten at offeret har noen mulighet til å merke undersøkelsene. Dessuten vil førstegangsbrukere gjerne oppdage ting ved eget nettverk de ikke har vært klar over – ukjente systemer, segmenter, rutere, modem og så videre, viten som er kritisk for sikkerheten.

Et slikt verktøy blir derfor lett 'vanedannende': Enhver sikkerhetsansvarlig med respekt for seg selv og oppgaven, vil ønske å foreta regelmessige kontroller av sikkerheten med slike verktøy – i takt med at nye svakheter oppdages og hull tettes.

Tilsvarende gjelder på angripersiden. Begge sider arbeider kontinuerlig med oppdateringer og forbedringer, kikker naturligvis hverandre i kortene, og benytter i stor grad de samme verktøyene. Åpenhet omkring svakheter, feilrettinger og tilgjengelige verktøy blir betraktet som en nødvendighet av de fleste sikkerhetsekspertene: Kunnskap og viten er makt, og *security by obscurity* hører historien til. Cracker-verktøy og -metoder blir gjerne forsøkt hemmeligholdt, men med liten suksess: Verktøy kan ikke brukes uten å synes, og når nye hull eller metoder oppdages, tar det ikke mange dagene før de blir offentlig kjent i alle fall.

Et kappløp med tiden

I og med at nye produkter, revisjoner, oppdateringer og systemer kontinuerlig strømmer på markedet – med tilhørende sikkerhetshull og

svakheter, blir dette et kontinuerlig kappløp: Hvem finner svakheterne først og hvordan kan de utnyttes eller tettes? Det ideelle scenario der produkter er 100% pålitelige, fri for huller og helt sikre, kan aldri bli virkelighet. Utfordringen blir å automatisere mest mulig av kontrolljobben: Verktøyene må oppdateres kontinuerlig, og få har tid eller ressurser til å gjøre dette manuelt. Dermed blir en viktig kvalifikasjon for verktøyene at de helt eller delvis kan kjøres og oppdateres uten tilsyn.

I kjølvannet av slike behov dukker det dessuten opp en annen problemstilling: Hvem stoler vi på? Er de løpende oppdateringene pålitelige, eller risikerer vi å åpne systemer og nettverk i stedet for å sikre dem? Kan verkøylene vi skaffer og setter vår lit til, inneholde trojanske hester? Muligheten er definitivt til stede: Vi har sett eksempler på at kommersielle leverandører uvitende har sendt ut infiserte produkter – med dramatiske konsekvenser. Her står vi overfor en ny bunke utfordringer som kun delvis er løst i dag. Vi nøyer oss med å konstatere at verktøyene som diskuteres nedenfor, utvikles og vedlikeholdes av kilder vi har all grunn til å stole på.

Nessus

Nessus (se også Mellvik-Rapporten nr. 75 og 77) blir betraktet som ledende i dette segmentet. Med opprinnelse og hjemsted i Frankrike, og teknologisk utspring i Nmap (se nedenfor), har Nessus klatret til topps gjennom en kombinasjon av fleksibilitet, funksjonalitet og tilgjengelighet (brukergrensesnitt). Som regelen er for frie verktøy, er Linux det enkleste utgangspunktet: Ferdig kompilert og pakket kan Nessus installeres i løpet av få minutter. Solaris tar noe lenger tid mens andre Unix-plattformer er krevende – om enn langt fra umulige.

Nessus har en modul-arkitektur som gjør det enkelt å utvikle og installere nye funksjoner i det eksisterende verktøyet. Dette har stimulert utviklere i øst og vest til å glemme sine hjemmesnekrede favorittverktøy, og i stedet utvikle for Nessus. Snøballen ruller, og resultatet er over 600 moduler som i tillegg til den grunnleggende portskanningen, kontrollerer områder som CGI-hull (Web-servere), brannmurer (feilkonfigurasjoner, kjente hull og svakheter, etc.), NIS, SMTP (epost-tjener), SNMP (tjenester for nettadministrasjon), Windows, RPC (bl.a. NFS), filtjenester (SMB) – og mange andre. Videre er arkitekturen distribuert, slik at systemet kan installeres på én maskin og brukes fra hvor som helst i nettverket – via sikrede protokoller og pålitelig autentisering.

I tillegg til et velutviklet brukergrensesnitt (som ikke er Web-basert), har Nessus en HTML-basert rapportmodul som genererer et hierarki av rapporter. Formatet er både lett tilgjengelig og tidsbesparende – med kort vei og få klikk til områder som er interessante. Mens tjeneren bør være en Linux-maskin, finnes det klienter i Java (for nettlesere) og Windows, slik at den praktiske bruken er plattformuavhengig.

Den viktigste innvendingen mot Nessus berører ikke produktet i seg selv, men fagområdet: Det tar tid å bli en effektiv bruker – fordi varia-

NIS – Network Information Service

RPC – Remote Procedure Call

NFS – Network File System

SMB – Server Message Block
(Microsoft fil- og print-tjenester)

SMTP – Simple Mail Transfer
Protocol

SNMP – Simple Network
Management Protocol

Kort om Nessus:

Effektivt, omfattende og lærerikt, ikke for nybegynnere, men for ansvarlige som har tid og interesser for å forstå hva de driver med.

Nessus fordrer en Linux- eller Unix-plattform å kjøre på. Rene Windows-miljøer bør se på ISS, Internet Security Scanner, som er et kommersielt produkt (www.iss.net), og kan lastes ned gratis for uttesting.

sjonene og dermed valgmulighetene er så mange, og fordi det tar lang tid å bygge opp tilstrekkelig innsikt til å forstå konsekvensen av å velge en modul inn eller ut: Hva er forskjellen på *SYN scan*, *FIN scan* og *NULL scan*, og når skal vi velge hvilken av dem? Omfattende – om ikke alltid like velorganisert – dokumentasjon hjelper, men forandrer ikke det faktum at dette tar tid.

SAINT

SAINT (*Security Administrator's Integrated Network Tool*) er et direkte avkom etter SATAN (*System Administrator's Tool for Analyzing Networks*). SATAN fikk voldsom oppmerksomhet på midten av 90-tallet, og skapte opphetet debatt om offensive kontra defensive verktøy. Forfatterne,⁸ som begge har bidratt med flere viktige sikkerhetsverktøy i løpet av de siste ti-årene, hevdet med styrke at for å komme på offensiven i forhold til Crackere, er det nødvendig å ha minst like gode våpen. Ved å demonstrere for all verden den selvfølgelighet at våpen fungerer like godt offensivt som defensivt, avslørte de på sett og vis at keiseren var naken: En selvfølgelighet ingen hadde tatt sjansen på å nevne i klartekst.

Etter at tumultene hadde lagt seg, dannet SATAN skole for videreutviklingen av kontrollerende verktøy, også på den måten at nettleseren ble brukergrensesnitt. Videreutviklingen har gjennomgått flere generasjoner, delt seg, og gått i flere retninger. SAINT er den mest kjente av dem, og er blitt halvkommersiell på veien: Produktet videreutvikles av selskapet World Wide Digital Security, Inc. (www.wwdsi.com), som selger to tilleggsprodukter – en rapportgenerator og en automatisk oppdateringstjeneste. Nye versjoner av SAINT blir først tilgjengelige for betalende kunder av disse produktene, mens eldre utgaver (noen måneder gamle), er fritt tilgjengelige. I og for seg en snedig måte å generere inntekter fra fri programvare på, og vi skal la den etiske diskusjonen ligge.

SAINT er mindre omfattende enn Nessus, og enklere å bruke. Videre kommer oppdateringene meget hurtig: I skrivende stund har Code Red viruset vært ute i en uke, og SAINT er forlengst oppdatert til å kontrollere om hullet finnes. Dessuten har SAINT vist seg svært effektivt til gjennomtrengings-test av brannmurer – et spesielt viktig område på grunn av misforståelsene som preger eksistensen av slikt utstyr. 9 av 10 synes fortsatt å mene at dersom de har en brannmur, er sikkerheten god. Som vi diskuterte i Mellvik-Rapporten nr. 37 og 57,⁹ er virkeligheten den stikk motsatte. De fleste brannmurer koster mye og gir beskjeden sikkerhet, ikke fordi produktene er dårlige, men fordi de brukes feil.

Om SAINT er bedre enn Nessus – eller motsatt, kommer an på øynene som ser og ikke minst behovene. Det er plass for begge – og flere – i markedet, og de drar hverandre fremover som konkurrenter skal. I og

⁸ Wietse Venema og Dan Farmer

⁹ Begge utgavene er tilgjengelige ON LINE på vår Web-tjeneste, se side 35.

med at begge er lett tilgjengelige og godt dokumenterte, er mulighetene gode for å gjøre seg opp egne meninger.

SARA

SARA (*Security Administrator's Research Assistant*) er en annen avleget av SATAN. Fellestrekkene med SAINT er dermed mange – på en rekke områder er det vanskelig å skille dem fra hverandre både med hensyn til funksjonalitet og resultater. SARA er fritt tilgjengelig i tradisjonell forstand, og synes å ha oppstått som en reaksjon på at SAINT ble stadig tettere knyttet til kommersielle tilleggsprodukter. Hovedansvarlig for utviklingen er samme person, som hoppet fra World Wide Digital Security, Inc. til Advanced Research Corp. i 1999.

Valget mellom SAINT og SARA blir dermed primært et valg mellom idealisme og 'rettroenhet' på SARA-siden, og betalbare tilleggsverktøy hos SAINT.

Rene portskannere

Blant en flora av rene portskannere på markedet, er Strobe og Nmap de mest interessante. **Strobe** – fra Lawrence Livermore National Laboratories i California – var det første automatiserte verktøyet i sitt slag på markedet, og har på sett og vis utspilt sin rolle. På grunn av nettopp enkelheten, lever det imidlertid videre, og brukes som *back end* av en rekke andre verktøy.

Nmap er en videreutvikling av Strobe, og langt mer sofistikert – og komplisert. Den benyttes av blant annet Nessus, og videreutvikles løpende.

Det faktum at de enkle verktøyene lever videre sammen med sine langt mer avanserte og kompliserte slektninger, demonstrerer viktigheten av enkelhet og variasjon: Det er ikke alltid maksimal funksjonalitet og bredde er hva vi trenger. Sammen med flere dusin slektninger, demonstrerer de fem nevnte variantene behovet for variasjon – verktøy som er tilpasset oppgavene, i stedet for universelle *swiss army knife* produkter som kan gjøre litt av det meste, men ingen ting godt.

Personlige brannmurer

For to år siden ble begrepet 'personlig brannmur' betraktet som en spøk av de fleste. I dag er det i høyeste grad alvor, og en produktgruppe som omfattes med stor og voksende interesse i markedet. Alle systemer tegner grunnleggende beskyttelse – på samme måte som alle bilder og hus har lås – og etterhvert alarmsystemer. Vi innretter oss etter den virkeligheten vi lever i, og tar de kostnadene som følger med på kjøpet.

'Personlig brannmur' er egentlig en villedende betegnelse, med opprinnelse fra 'personlig datamaskin', som har satt seg fast i mangel på et bedre alternativ. 'Maskin-spesifikk beskyttelse' er hva vi egentlig mener – mekanismer som kontrollerer inn- og utgående trafikk til ett spesifikt system, og sørger for blokkeringer og filtrering i henhold til en definert policy.

Interessert i sikringsverktøy?

Nettstedet www.insecure.org/tools.html er riktig sted å begynne.

Slike verktøy representerer en interessant trend i markedet. Sammen med voksende mobilitet, mer komplekse nettverk og stor dynamikk, utpeker individuell beskyttelse seg som den mest pålitelige form for systemsikring, kanskje sågar den eneste. Sammen med ende-til-ende kryptering (VPN) utpeker personlige brannmurer seg som et i fremtiden allesteds nærværende produkt på alle slags systemer, fra PDAer til tjenere – en utvikling vi skal komme tilbake til ved en senere anledning her i Mellvik-Rapporten.

Den største utfordringen knyttet til produktgruppen er at brukerne er uinteresserte – eller negative: De ønsker lettvinthet, tilgjengelighet og effektivitet. En brannmur – og de fleste andre sikringstiltak – gir det motsatte. I praksis betyr det at produktene må være om ikke usynlige, så i alle fall utilgjengelige for brukeren. Styring og kontroll må ligge hos de som har ansvaret for nettverket, og betraktes som en del av dette – en aksessmekanisme. I profesjonell sammenheng lar dette seg gjøre, mens det for personlige brukere (hjemmebrukere med eget utstyr) er et større lerret å bleke. Her må ISPene på banen med tjenester som på et eller annet tidspunkt blir obligatoriske.¹⁰

Med et slikt latent potensiale er det ikke å undres over at produkttilfanget vokser jevnt. Like fullt er de 'gamle' fortsatt eldst: Såkalte *TCP-wrappere*, programmer som evaluerer hver eneste inngående eller utgående forbindelse i henhold til en regelsamling. Enkelhet satt i system på en uslåelig måte, og 'oppfinneren' er ingen ringere enn den samme Wietse Venema som også sto bak SATAN. En rekke varianter finnes for ulike plattformer, med forskjellige påbygninger. Et populært eksempel er **Port Sentry**, som overvåker loggfilene fra en *wrapper*, og rapporterer om forsøk på portskanning og andre irregulære aktiviteter. Den kan også foreta automatiske oppdateringer av konfigurasjonsfilene til *wrapper*-programmet, og for eksempel blokkere all trafikk fra kilder som foretar skanning.

Svakhetene ved en slik *wrapper* er at den for det første kun virker for TCP, og kun for etableringen av forbindelser. Trafikken går deretter ukontrollert. Dessuten kontrolleres ikke RPC-baserte tjenester, som må håndteres separat – et forhold som stort sett kun berører tjenere.

Logcheck er et annet verktøy fra samme kilde, som løpende holder øye med systemets loggfiler (tilsvarende *event log* på NT/W2k), og sender epost eller utfører kommandoer dersom den oppdager noe som i henhold til konfigurasjonen er mistenkelig.

PC-baserte produkter

I artikkelen om personlige brannmurer i Mellvik-Rapporten nr. 75, presenterte vi en oversikt over en del slike produkter. Oversikten er gjengitt som referansemateriale på web-siden med tilleggsinformasjon til denne utgaven (se detaljer på side 35). I denne samlingen utmerker

¹⁰ Det kan diskuteres hvorvidt slike mekanismer bør plasseres hos Internett-leverandøren i stedet for hos brukeren. En sentral plassering tar imidlertid ikke høyde for brukerens mobilitet, og legger dessuten siste stykket frem til brukeren åpent for angrep eller avlytting.

Konsolideringen fortsetter

Konsolideringen i sikkerhetssektoren fortsetter – en naturlig og stort sett positiv utvikling. Aktører som har rukket å bli store, kjøper seg vekst og bredde ved å overta mindre leverandører med nisjesuksesser eller som har vist potensiale.

ISS, Internet Security Systems, er blitt en betydningsfull aktør i segmentet, og overtok nylig NetworkICE, selskapet bak BlackICE Defender.

En mindre attraktiv, men tilsynelatende uunngåelig konsekvens av konsolideringen er at frie verktøy blir heller halvkommerisielle. Sett fra en sikkerhetsmessig synsvinkel, er imidlertid det viktigste poenget at verktøyene blir vedlikeholdt og videreutviklet.

Overvåking

Andre 'nettverkssniffere'

Flere dusin frie nettverkssniffere med ulike karakteristika er tilgjengelige på Internettet, og to av dem er spesielt verd å nevne i denne sammenheng:

- **Dsniff** er en samling verktøy som søker etter interessant informasjon på nettverket og har mekanismer for å reversere den trafikk-isolasjon som introduseres av svitsjer (naughty.monkey.org/~dugsong/dsniff).
- **Ethereal** er for alle praktiske formål NTs Netwatch for Unix og Linux, en sniffer med vindusbasert brukergrensesnitt (ethereal.zing.org).

ett produkt seg spesielt: ZoneAlarm fra selskapet ZoneLabs er riktignok kommersielt, men kan lastes ned og brukes gratis så lenge bruken er personlig eller ikke-kommerisiell, et ypperlig utgangspunkt for å skaffe praktiske erfaringer. Produktet er å finne i segmentets toppklasse, noe en serie utmerkelse fra ulike fagtidsskrifter forteller sitt om.

ZoneAlarm er hva en vanlig bruker vil kalle en pest og plage før den er ferdig konfigurert: All inngående og utgående trafikk kontrolleres og varsles, og brukeren – eller noen andre – må etablere godkjenninger for hver enkelt applikasjon som skal ha kontakt med nettverket utenfor. Denne grundigheten er imidlertid gull verd, et vesentlig bidrag til sikkerheten.

BlackICE Defender er et annet produkt i samme klasse – med tallrike fellestrekk. Den er imidlertid ikke gratis for noen, og yter intet bidrag i kategorien 'gratis sikkerhet'. Om de hundrelappene produktet koster per lisens, er signifikante eller en pølse i slaktetiden, er en annen sak.

Løpende overvåking av systemer og nettverk betyr å holde øye med pågående aktiviteter i sann tid. Igjen kan bruken være offensiv eller defensiv: En Cracker vil ha stor glede av å tappe trafikken på et lokalnett, og kan i løpet av kort tid samle all informasjon som trengs for å rulle ut vellykkede angrep eller usynlige innbrudd. Derfor er det viktig å holde både inntrengere og medarbeidere unna muligheter for slik overvåking: Ingen andre enn de som skal beskytte systemer og nettverk, har bruk for denne informasjonen. I og med at dette er vanskelig i praksis – fordi enhver avansert bruker med det riktige utstyret kan 'tappe' store deler av nettverket, går trenden i retning av å kryptere all trafikk – også den interne. Ytelse og båndbredde har vært til hinder for dette så langt, men er i ferd med å bli borte takket være effektive og billige krypterings-brikker og fallende båndbreddepriser.

Overgangen til svitsjede nettverk har også bidratt til en bedre situasjon gjennom å forkorte veiene trafikken traverserer. Bedringen betyr at terskelen er hevet, men ikke at sikkerheten er blitt god, og argumentene for generell bruk av kryptering er fortsatt like sterke.

De fleste generelle systemer – og en rekke rutere, brannmurer og andre konnektivetsprodukter – leveres med mer eller mindre sofistikerte verktøy for tapping av nettverket. Den mest kjente er **tcpdump**, som er standardutstyr på Linux-systemer og tilgjengelig for de fleste andre plattformer. Tilsvarende verktøy under Solaris er **snoop**, mens AIX har **iptrace** og Win NT/2k har **netwatch**.

Samtlige er relativt krevende i bruk, med Microsofts Netwatch som hederlig unntak. System-, nettverks- og sikkerhetsansvarlige bør ha erfaring med dem, slik at de raskt kan settes inn når behovet oppstår. Videre kan slike verktøy benyttes til kontinuerlig overvåking, sammen med søkemekanismer som kan trigge på spesielle mønstre, adresser, tjenester, data eller kombinasjoner.

Intern kontroll

crack –
www.users.dircon.co.uk/~crypto

L0phtcrack –
www.l0pht.com/l0phtcrack
L0phtcrack et kommersielt produkt.

John the Ripper –
www.openwall.com/john

Tripwire – www.tripwire.com

LIDS – *Linux Intrusion Detection System*, www.turbolinux.com/lids

I denne sammenhengen er vi spesielt opptatt av to sider knyttet til den løpende interne kontrollen: For det første at sikkerhetsnivået som er etablert, blir opprettholdt, og for det andre at vi umiddelbart oppdager det dersom noe galt er fatt. Første punktet betyr løpende kontroll og oppfølging av brukerne: Hvem har tilgang til hva, er passordene gode nok, blir de skiftet tilstrekkelig ofte – i henhold til policy og så videre. Verktøy og mekanismer for slik oppfølging følger med de fleste systemer, og bør benyttes. Videre finnes det en rekke passordknekkingsprogrammer – for eksempel **crack** og **John the Ripper** for Linux/Unix og **L0phtCrack** for NT/W2k – som gir nyttige bidrag til kontroll ved å avsløre brukere som saboterer sikkerheten gjennom opplagte passord.

Å oppdage at vi har hatt ubudne gjester er en langt større utfordring enn det kan se ut til ved første øyekast. De fleste av oss husker James Bond og hans hårstrå på dørkarmen, og våre IT-systemer krever langt mer sofistikerte verktøy. IDS – *Intrusion Detection Systems* – er en sjanger i seg selv, med verktøyet Tripwire som idémessig og i noen tilfeller praktisk opphav.

En rekke kommersielle verktøy i denne kategorien har dukket opp de siste årene. Selv Tripwire er blitt kommersielt – og er anerkjent som ledende i segmentet. Den opprinnelige OSS-baserte utgaven av produktet er fortsatt tilgjengelig, men er utgått på dato. En nyere utgave av det kommersielle produktet er også fritt tilgjengelig – omtrent etter samme mønster som SAINT ovenfor.

Intrusion Detection blir et stadig viktigere element i våre sikringsystemer, og blir tema for en egen artikkel i Mellvik-Rapporten i nær fremtid.

Oppsummering

Mens hundretalls av sikringsverktøy er tilgjengelige gratis, er det naivt å tro at vi kan etablere tilfredsstillende sikkerhet uten kostnader. Samtidig er det også et faktum at god sikkerhet ikke trenger å være kostbart, og ei heller uforholdsmessig tidkrevende. Erfaring er den mest verdifulle ressursen i denne sammenheng. Praktisk bruk av de verktøyene vi har gjennomgått her – og andre i samme kategorier, gir slik erfaring: Hva virker under hvilke omstendigheter, og hva passer i vårt miljø? Behov og omgivelser er forskjellige og fordrer ulike tiltak for å etablere nødvendig sikkerhetsnivå.

Vi kan kjøpe eller på annen måte skaffe til veie all verdens sikringsverktøy og -tiltak, men de blir raskt verdiløse om de ikke følges opp av en ansvarlig person, gruppe eller leverandør med nettopp sikring og sikkerhet som hovedoppgave. Det betyr ikke at vi alle trenger vår egen sikkerhetseksperter, men at vi må innse egen begrensning dersom vi ikke har eller kan skaffe nødvendig ekspertise.

Kunnskap er makt, og å vite hva som trengs og hvordan det kan skaffes, er sunn fornuft. Å la humla suse og skylde på manglende ressurser eller tilgang på ekspertise, er ikke bare uansvarlig. Det burde kvalifisere til umiddelbar omplassering – eller permanent 'utplassering'. ■