

Har du testet sikkerheten?

“Yes. Vi har god sikkerhet. Brannmur og filtrering, virus-kontroll, NAT og VPN. Vi vurderer IDS-systemer, men det har ingen hast. WLAN? Ganske bra – med autentisering og MAC-filtrering, men uten kryptering. Det ble for komplisert. Jotakk, det står ganske bra til på sikkerhetsfronten.”

Sikkerhet på prøve

Sitatet er hentet fra en samtale med en norsk IT-leder på forsommeren, og representativt for hva vi får høre når sikkerhet kommer på banen. Og dersom alt stemmer, synes situasjonen å være under rimelig kontroll – muligens med unntak av det trådløse nettverket. I den forbindelse kan vi ikke unngå å undres – hva er egentlig problemet? Samtlige produkter på markedet har jo enten middels gode eller gode krypteringsmekanismer innebygget.

WPA – Wi-Fi Protected Access
WEP – Wired Equivalent Privacy

“Vi har en del W98-klienter. De kan ikke kjøre WPA. Og WEP er vel og bra, men det blir for komplisert å distribuere nøklene manuelt.” Med andre ord – sikkerheten får lide til fordel for enkelhet, en akk så alminnelig situasjon. Uakseptabelt er det i alle fall. Uten kryptering kan hvem som helst lytte til trafikken og skaffe seg den informasjon som skal til for å få tilgang til nettverket. At bruken av VPN representerer en ny barriere som i de fleste tilfeller er vanskelig å bryte igjennom, er naturligvis viktig, men den beskytter ikke mot misbruk av ressursene.

Eksemplet setter fingeren på et forhold som fortsatt ofte dukker opp ved siden av lettvintheten: Misforståelsene. At autentisering gir sikkerhet i seg selv. Autentisering er nødvendig, og gir identifikasjon av bruker mot tjeneste og motsatt – med en eller annen grad av pålitelighet, men gir ingen beskyttelse mot innsyn eller tapping (transportsikring). Og WLAN er fortsatt – høsten 2004 – et svakt punkt i mange nettverk, et forhold vi skal komme tilbake til i Mellvik-Rapporten senere i høst. Aldri har det vært enklere og billigere å etablere god WLAN-sikkerhet. Det som skal til er interesse og aksept for nødvendigheten av slik sikring.

Truende dynamikk

Selv i organisasjoner som tydelig tar sikkerhet på alvor og har foretatt betydelige investeringer i sikring de siste årene, dukker det ofte opp store hull, typisk forårsaket av nettopp misforståelser og lettvinthet. Som vi var inne på i forrige utgaves lederartikkel (“Sikkerhet på ville veier”), er brannmurer faretruende ofte en kostbar måte å forsinke nettverkstrafikken på. Tradisjonelt ‘kringvern’ – som brannmurer er en del av – er både viktig og nødvendig, men lite verdt på egen hånd. Den legendariske amerikanske general George S. Patton (1885-1945) skal ha uttalt at *“fixed fortifications are monuments to the stupidity of Man”*, og setter fingeren på det ømme punktet.

Dynamikken som preger vår IT-hverdag er den viktigste og oftest oversette årsaken til denne situasjonen. Mens vi etablerer og vedlikeholder

brannmurer, antivirus-systemer, mekanismer for automatisk oppdatering av programvare (*patching*) og innbruddsdeteksjons-systemer, tester våre motstandere nye mekanismer for å gjemme virus, ormer og usynlige overvåkingsprogrammer i tilsynelatende uskyldige datastrømmer. Statistikkene viser at de lykkes. Like fullt lever store deler av verden videre i den villfarelse at de har god sikkerhet når de statiske sikrings-tiltakene er gjennomført.

Bråvåkningen kommer når innbruddet eller virusutbruddet er et faktum. Da viser det seg gjerne at én eller flere av forutsetningene som ligger til grunn for det eksisterende forsvar, har forandret seg: Nye brukere, nye versjoner, flere VPN-produkter, flere partnere eller kunder som har tilgang til utvalgte interne data – og så videre. Et av hovedproblemene med tradisjonell forsvarstenking er at den tar utgangspunkt i stabile og kjente grenser. I IT-sammenheng finnes en slik virkelighet kun i historien. Det finnes ikke lenger klare skillelinjer mellom hva som er eksternt og internt. Hjemmekontorer, mobile brukere, partner/kunde-programmer, fusjoner og oppkjøp, nye teknologier, omlegging av infrastruktur – og så videre. Våre mekanismer og metoder – og ikke minst måten å tenke på – må videreutvikles i takt med dette.

Kunnskap er fortsatt makt, uvitenhet er en trussel

En slik tilpasning til virkeligheten er ikke gjort i en håndvending. Vi har ved tidligere korsveier gjennomgått en rekke viktige sider og problemstillinger som fortsatt er relevante i utviklingen av en sikkerhetsarkitektur. Vårt fokus denne gang er på kunnskap – om oss selv, vår egen situasjon og hvor vi står. Hvordan kan det ha seg at eksterne parter ('hackere') som fatter interesse for vår organisasjon og vårt nettverk, vet mer om våre svakheter enn vi selv? I enkelte tilfeller har de sågar bedre og mer oppdatert oversikt over våre interne systemer enn driftsgruppen selv besitter. "De har tid til å gjøre det, det har ikke vi", er forklaringen vi får servert.

Vi tviler ikke på at så er tilfelle, men verken situasjonen eller unnskyldningen blir mer akseptabel av den grunn. Dette handler om ansvar, prioritering og å velge de riktige tiltakene. Satt på spissen kan vi si at en organisasjon som ikke har tid eller råd til å sikre sin daglige drift, knapt har livets rett.

Kunnskap er makt – mer enn noen gang. En forutsetning for god sikkerhet er at vi selv vet det som er verdt å vite om egen infrastruktur, også svakheter, og at det er vanskelig eller umulig for andre å skaffe til veie slik informasjon. Slik kunnskap får vi ikke ved å analysere skisser av sikringsarkitektur og mekanismer, men ved å teste sikkerheten – utsette den for prøver som emulerer den virkelige infrastrukturen eksponeres for til daglig.

Tyver og innbrudd, bukken og havresekken

Da må det vel være en glimrende idé å hyre inn en ekte innbryter til å gjøre testingen, forsøke å bryte seg inn? Det er både forbausende og

foruroligende at en slik tanke dukker opp. Det gjør den imidlertid, og pressen har laget positive oppslag om organisasjoner som har gjort nettopp det. Hvorfor leier ikke en gullsmed like godt en innbruddstyv til å vokte sitt gull?

Det kan riktignok være effektivt forsvar å trykke fienden til sitt bryst, men antagelsen om at en allianse med én eller flere innbrytere vil gi god IT-sikkerhet, er ikke bare en total misforståelse, men også naivt. Dette har ikke bare med tillit å gjøre, men også med oppfatning av kompetanse og innsikt. At en person har klart å trenge gjennom tilsynelatende solide forsvarsverker, sier fint lite om vedkommendes kompetanse. Personen kan være flink til å spore opp verktøy og dyktig i bruken av dem, men har sjelden innsikt i hvordan et effektivt forsvar bør bygges opp. Siden den egentlige kompetansen er ukjent, gir det dessuten liten grunn til å sove godt om natten at en slik person eller en gruppe ikke er i stand til å trenge igjennom vårt forsvar. Der den ene feiler, kan den neste lykkes, og vi er like langt.

Det vi ikke vet, har vi vondt av, og i denne sammenhengen er kun det beste godt nok: Faglig forsvarlige tester av alle tenkelige sider av sikkerhet og forsvar. Når vi har akseptert at det aldri finnes noen 100% sikkerhet, og samtidig ser at 'alle tenkelige sider' slett ikke er noen uoverkommelig mengde, har vi et godt utgangspunkt for å komme til neste nivå.

Finn svakhetene – før andre gjør det

I tillegg til de sikringstiltak som allerede er på plass, må vi inn med prosedyrer for hyppig, gjerne uregelmessig, testing av sikkerheten.⁶ Enkelte IT-ansvarlige mener riktignok at de får testet sikkerheten hver eneste dag, og får det de trenger av kunnskap fra analyse av loggfiler. Mens slike analyser ikke er bortkastet, hører de fortsatt hjemme i kategorien 'se i sladrespeilet' sikkerhet: Vi vet ikke om skuta holder før stormen er over. Organisasjoner flest kan ikke leve med en slik utrygghet – som ei heller er ansvarlig.

Artikler om testing av sikkerheten i tidligere utgaver av Mellvik-Rapporten:

- "Test sikkerheten – gratis" i nr. 75.
- "NMAP og Nessus: Sikkerhetskontroll, par excellence" i nr. 77.
- "Lite sikkerhet uten Nessus" i nr. 80.
- "Gratis sikkerhet" i nr. 86 (aug. 2001)

Testing av egen sikkerhet kan betraktes som en driftsoppgave, og kan angripes deretter – gjennom outsourcing eller ved å bygge opp egen kompetanse og tilsvarende arsenal av verktøy. Dersom en ekstern partner med tilstrekkelig kompetanse, tillit og akseptable betingelser forøvrig finnes, er det liten tvil om at dette er veien å gå – av de samme årsaker som outsourcing i sin alminnelighet. I motsatt fall – eller dersom organisasjonen selv besitter høy sikkerhetskompetanse og har ambisjoner om å videreutvikle denne, er det riktig å ta tak i kontrolloppgaven selv – eventuelt med starthjelp fra eksterne eksperter.

En flora av verktøy

Vi har i tidligere utgaver av Mellvik-Rapporten (se ramme på foregående side) diskutert både metoder og verktøy for testing av nettverks- og systemsikkerheten – med fokus på fritt tilgjengelige (Open Source)

⁶ Her er det viktig at tidspunktene velges tilfeldig, slik at det ikke blir rutine i å lukke hull som normalt står åpne fordi det er praktisk.

verktøy. Slike verktøy, med Nessus [www.nessus.org] i spissen, utgjør fortsatt selve fundamentet for et grundig testoppsett. Som så ofte er tilfelle med Open Source verktøy, har imidlertid Nessus en relativt høy terskel.⁷ Mens vi kan velge å oppfatte dette som en fordel, ettersom det neppe er hensiktsmessig at sikkerhetskontroll utføres av personer som ikke vet hva de gjør, har markedet tydelig vært av en annen oppfatning. I løpet av de 3-4 siste årene har det dukket opp et betydelig antall slike verktøy, de fleste rettet mot Windows som plattform og mot Windows-miljøer – av naturlige årsaker.

Uavhengig av vår prinsipielle oppfatning, er det et faktum at en rekke av disse verktøyene er både solide, omfattende og – som ventet – relativt lett tilgjengelige. De beste og mest kostbare variantene koster flere hundre tusen kroner (for eksempel Fundstone FS1000, www.fundstone.com), og har formidabel kapasitet med hensyn til korrelasjon av ulike trusler – typisk det svakeste området for andre produkter. Videre er mulighetene for rapportgenerering og ikke minst plattformdekning høyst variable parametre.

Uansett hva vi velger, bør følgende krav vies oppmerksomhet – utover selvsagte parametre som fleksibel angivelse av nett, subnett, porter, type scanning, grundighet etc.:

- ✓ Søke etter og rapportere kjente svakheter i de OS-plattformene vi benytter, fortrinnsvis med referanse til hvor mer informasjon om den enkelte svakhet kan finnes (i offentlige databaser eller leverandører).
- ✓ Gi forståelige anvisninger for hvordan de mest alminnelige svakhetene kan rettes, evt. med pekere til detaljer.
- ✓ Arkivering av data, slik at forandringer i forhold til tidligere kjøring lett kan identifiseres og analyseres.
- ✓ Enkel og forståelig konfigurasjon.
- ✓ Automatisk (klokkestyrt) kjøring.
- ✓ Fleksibel rapportgenerering.

De viktigste verktøyene i dette relativt smale segmentet – i tillegg til Fundstone og Nessus som vi allerede har nevnt, er følgende (se tilleggssiden på www.mellvik.no for ytterligere informasjon om verktøyene og aktive pekere til leverandørenes web-sider, detaljer på side 35):

- ✓ MegaPing (Magneto Software)
- ✓ Retina Network Security Scanner (eEye Digital Security)
- ✓ SAINT 5 (en kommersiell videreutvikling av det kjente Open Source-verktøyet SAINT) (SAINT Corp.)
- ✓ NetIQ Security Analyzer 5.0 (NetIQ Corp.)
- ✓ GFI LANguard Network Security Scanner 3.3 (GFI Software)

⁷ Samtidig skal det i rettferdighetens navn nevnes at Nessus har utviklet seg vesentlig i positiv retning de siste 3 årene, også med hensyn til brukervennlighet og ikke minst 'installasjonsvennlighet'.

- ✓ NMAP med tilhørende brukergrensesnitt NMapFE (Open Source)⁸
- ✓ MBSA – Microsoft Baseline Security Analyzer (v 1.1.1) (Microsoft, gratis)

De to sistnevnte hører hjemme i en kategori for seg selv, ettersom de ikke analyserer nettverk, men maskiner/systemer. MBSA er av beskjedne verdi for annet enn små Windows nettverk.

Må vi, så må vi ...

1000-kroners spørsmålet til slutt er: Kan vi klare oss uten? Det kommer naturligvis an på hvilken risikoprofil vi kan leve med. Hovedpoenget er at på grunn av dynamikken i hverdagen blir gårsdagens sannheter ofte dagens løgner, og kun aktiv testing kan avsløre om vi fortsatt har et akseptabelt sikkerhetsnivå. Hvilket nivå dette er, er en annen historie, som blant annet påvirker hvilket verktøy og hvilken hyppighet som er riktig for vår situasjon.

Mange av oss har for vane å kjenne på døra etter at vi har låst den. Er vår IT-infrastruktur viktig nok til å fortjene tilsvarende oppmerksomhet? ■

⁸ Selve søkemotoren i NMAP er en del av flere andre produkter, inklusive Nessus og Retina Network Security Scanner.