

Sikkerhet og Windows 2000

Dette er fjerde og nest siste artikkel i serien om W2k og sikkerhet som startet i Mellvik-Rapporten nr. 86.

Mens Windows 2000 har en lang rekke forbedringer og viktige/nyttige verktøy for sikring, er det også et faktum at systemet er fullt av svakheter og hull – som regelen dessverre er for våre dagers komplekse programvare-systemer. En rekke Web-steder overvåker denne situasjonen og inneholder oppdaterte oversikter over feil, mangler, hull og deres status. Ett av dem er www.labmice.net/articles/win2000securiityholes.htm.

Routing and Remote Access Service (RRAS)

L2TP – Layer 2 Tunneling Protocol

PPTP – Point-to-Point Tunneling Protocol

RIP – Routing Information Protocol

OSPF – Open Shortest Path First (rutingprotokoll)

POTS – Plain Old Telephone Service, gammeldags analog telefoni på godt norsk

Vi fortsetter vår fokusering på Windows 2000 og sikkerhet med en gjennomgang av funksjoner og tjenester for ruting og fjernaksess – på mange måter et odde par i og med at de funksjonelt sett har lite med hverandre å gjøre.

Vi finner tallrike slike eksempler i Windows generelt og Windows 2000 spesielt: Tjenester som er koblet sammen uten nødvendigvis å ha annet med hverandre å gjøre enn at de deler enkelte ressurser. Telefoni-tjenesten er ett eksempel – den kan ikke stoppes uten at vi også stopper *Remote Connection Manager*. Dermed blir en del av nettverks-funksjonaliteten som de fleste er avhengige av, også borte. Videre kan web-tjeneren ikke stoppes uten at også FTP-tjenesten forsvinner. Disse tette koblingene reduserer fleksibiliteten og mulighetene for å sikre et system: Et viktig prinsipp i forbindelse med all sikring er at tjenester som ikke brukes eller som ikke er nødvendige, skal stoppes. Det er ikke alltid mulig i Windows 2000. At ubrukte tjenester også forbruker ressurser er en annen sak, som isolert sett kan være viktig nok, og som automatisk blir det dersom programmene 'lekker' hukommelse.⁷

Fjernaksess og VPN er to sider av samme sak. Vi har i gjennomgangen av IPSec diskutert denne komponentens viktighet i den forbindelse, og blant annet sett at deler av IPSec-implementasjonen er klientsiden av VPN-ligningen. RRAS representerer tjenersiden: Den tar imot innkommende forbindelser – fra individuelle brukere eller eksterne nettverk, og etablerer krypterte kanaler via L2TP/IPSec eller PPTPv2.

RRAS-modulen kan imidlertid langt mer enn å være en VPN-tjener:

- ✓ Pakkeruting – for TCP/IP, IPX og AppleTalk mellom to eller flere fysiske, virtuelle eller oppringte grensesnitt.
- ✓ Støtter rutingprotokollene RIPv2 og OSPF for automatisk oppdatering av rutingtabeller.
- ✓ Kan sørge for både portbasert og adressebasert NAT, *Network Address Translation*.⁸
- ✓ Kan opptre som tjener eller klient for ISDN, POTS (modem) eller VPN-forbindelser.
- ✓ Håndterer automatisk (trafikkstyrt) opp- og nedkobling av ISDN- og POTS-forbindelser.

7 Å 'lekke' hukommelse betyr at et program inneholder feil som gjør at det legger beslag på stadig mer hukommelse over tid. Til slutt vil ressursen være oppbrukt, og systemet må omstartes for å komme i gang igjen. Slike problemer var spesielt plagsomme i Windows NT, men er langt fra fraværende i W2k.

8 Det er igjen verdt å minne om at NAT og IPSec ikke lar seg kombineres, av årsaker vi diskuterte i forrige utgave (Mellvik-Rapporten nr. 88 side 25).

Mer om RRAS

Vår gjennomgang tar for seg enkelte deler av RRAS som er spesielt interessante i sikkerhetssammenheng. Informasjon om RRAS i hele sin bredde er å finne i hjelpefilene som følger systemet, i det såkalte *Resource Kit*, som kjøpes separat fra Microsoft, og ikke minst i boken "*Windows Routing and Remote Access*" av K. Charles (New Riders Publishing, 2000).

IETF – Internet Engineering Task Force

- ✓ Kan ivareta statisk pakkefiltrering per grensesnitt, fysiske og virtuelle.
- ✓ Kan fungere som NetBIOS-portner mellom ulike transport-protokoller, for eksempel mellom IPX og TCP/IP.

RRAS ivaretar typiske tjenerfunksjoner, og er ikke med i arbeidsstasjonsutgaven av Windows 2000 (Professional).

Sikkerhetsfunksjonene og egenskapene vi diskuterer nedenfor, er grunnleggende elementer i RRAS, og er tilgjengelige uansett hvilken aksessmekanisme som velges (oppringt, VPN). Likeledes er observasjonene relevante for VPN-forbindelser basert på IPSec/L2TP og for oppringte forbindelser med PPTP.

Tunneller, IPSec og RRAS

Under gjennomgangen av IPSec påpekte vi blant annet at støtten for såkalt tunnel-modus er marginal, såvidt tilstrekkelig til å tilfredsstille minstekravene i standarden. I praksis er denne tunnel-støtten lite anvendelig, og Microsoft har presentert relevante argumenter for å gjøre et slikt valg (se Mellvik-Rapporten nr. 87 side 24).

Forholdet er at IPSec har en rekke sider som ikke harmonerer med behovene i mange fjernaksess-situasjoner av i dag. Dette kan på den ene siden karakteriseres som svakheter, men er områder IPSec aldri hadde ambisjoner om å dekke. IPSec ble laget for sikring av nettverk-til-nettverk forbindelser.

Arbeid er i gang i Internettets standardiseringsorgan IETF for å rette opp i forholdet, og komme frem til en IPSec-variant som er i harmoni med behovene (se www.ietf.org/html.charters/ipsra.html). Det vil imidlertid ta flere år før en ny standard er tilgjengelig i praksis. I mellomtiden er de viktigste funksjonene dekket av RRAS:

- ✓ Dynamisk allokering av IP-adresser til fjern-klienter via VPN.
- ✓ Dynamisk administrasjon av rutingtabeller på VPN-tjener og/eller klient i tilknytning til at forbindelser blir koblet opp og ned⁹.
- ✓ IPSec kan autentisere rutere og maskiner, men ikke brukere. Å administrere/kontrollere rettigheter og andre egenskaper i forbindelse med opp/nedkobling blir dermed vanskelig. RRAS (sammen med L2TP) sørger for pålitelig brukerautentisering, og løser på den måten problemet.
- ✓ Muligheter for detaljert aktivitetslogging og tilhørende kontroll.
- ✓ IPSec støtter kun IP (TCP/IP), mens RRAS gjør det mulig å kjøre både IPX og AppleTalk i krypterte tunneller.

Disse og flere egenskaper blir gjennomgått i detalj i neste avsnitt.

⁹ Her ligger et av argumentene for å koble sammen ruting og fjernaksess i én og samme pakke.

Egenskaper og funksjoner

Mens RRAS først og fremst er en kommunikasjonsmodul, reflekterer dens innhold også det faktum at tiden er ute for rene kommunikasjonsløsninger: Uten sikkerhet, ingen kommunikasjon. For oss som skal bruke løsningen, er det viktig å være klar over disse egenskapene – det er første trinn på veien mot å ta dem i bruk.

Vi begynner med en gjennomgang av funksjonaliteten, mens råd og erfaringer i forbindelse med praktisk bruk kommer i neste utgave:

- ✓ **Aksesskontroll:** Hvorvidt en bruker har anledning til fjernpålogging bestemmes i første omgang av hvordan kontoen er definert på tjenermaskinen – eller i Active Directory: Fjernaksess kan allerede her være blokkert eller tillatt. I neste omgang konsulteres systemets *remote access policy*, der en rekke parametre kan være med på å bestemme om en gitt bruker slipper inn på systemet eller ikke – blant annet gruppetilhørighet, protokoll, tid på døgnet og egenskaper knyttet til forbindelsen. Når en regel trigges, kan den sørge for å håndheve riktige parametre for forbindelsen, for eksempel autentiserings- og krypterings-opsjoner, aksessprivilegier og tidskonstanter for automatisk nedkobling.
- ✓ **RADIUS-støtte:** RRAS kan opptre som klient overfor en RADIUS-tjener, som tar ansvaret for bruker-autentisering ved oppkobling. Dette forenkler integrasjonen med eksisterende løsninger der RADIUS er en dominerende standard. I miljøer med mange RRAS-tjenere er RADIUS som regel en nødvendighet.
- ✓ **Internet Authentication Service (IAS):** W2k har sin egen RADIUS-tjener innebygget og tett koblet til RRAS. Konfigurasjon av IAS er praktisk talt identisk med tilsvarende for RRAS: Har vi forstått den ene, følger den andre med på kjøpet.
- ✓ **Pakkefilter:** RRAS inneholder sitt eget statiske pakkefilter, omtrent tilsvarende det vi finner i de fleste rutere. Filteret kan knyttes til både fysiske og logiske (virtuelle) grensesnitt, inklusive oppringte forbindelser. Parametre som kan inngå i filterets regler er retning (inn/ut), protokoll, sender/mottaker-adresse, sender/mottaker-port og fragmenteringsstatus. Filtreringsreglene kan knyttes til bruker i stedet for grensesnitt, og håndheves via *RRAS policy*.
- ✓ **Gjensidig autentisering:** RRAS støtter mekanismene EAP-TLS og MS-CHAPv2 for toveis (gjensidig) autentisering. Uten å gå i detaljer kan vi konstatere at begge gir høy grad av pålitelighet. Observasjonen er spesielt viktig fordi forrige utgave av Microsofts CHAP-variant var mislykket.
- ✓ **Støtte for Smart-kort og digitale sertifikater:** Autentiseringsmekanismen EAP-TLS kan benytte såkalte X509v3-sertifikater som lagres på Smart-kort. Dette er den sterkeste (sikreste) autentiseringsmetoden for oppringte og VPN-bru-

RADIUS – Remote Authentication Dial-In User Service, se Mellvik-Rapporten nr. 56 ("Mens vi venter på Single Logon: RADIUS").

EAP – Extensible Authentication Protocol

MS-CHAP – Microsoft(s versjon av) Challenge Handshake Authentication Protocol, v2 betyr 'versjon 2'

TLS – Transport Layer Security, praktisk talt identisk med **SSL**, Secure Socket Layer

kere i RRAS, og kan via *policy* gjøres obligatorisk for fjernbrukere. Kombinasjonen applauderes av sikkerhetsekspertene, som mener egenskapen er grunn god nok i seg selv til å bytte fra eldre Windows-varianter til W2k.

- ✓ **Kryptering:** RRAS støtter kryptering via IPSec eller MPPE (*Microsoft Point-to-Point Encryption*). Vi kommer tilbake til dette i forbindelse med VPN i neste utgave.
- ✓ **Uttestenging:** RRAS kan sørge for automatisk blokkering av fjernaksess for brukere som etter gjentagne forsøk ikke oppgir riktig passord. Blokkeringen gjelder kun fjernaksess, og har ingen ting med lignende mekanismer for direkte (lokal) aksess å gjøre.
- ✓ **Logging:** RRAS gir gode muligheter for detaljert logging av alle slags aktiviteter knyttet til fjernaksess. Loggingen kan sendes til det sentrale logg-systemet (*Event Viewer*) og/eller til tekstfiler.
- ✓ **Tilbakeringing:** Via *policy* kan brukere tvinges til å kun benytte forhåndsregistrerte telefonnummere. Umiddelbart etter innloggingen får de beskjed om å koble seg fra, og systemet vil ringe tilbake på det forhåndsallokerte nummeret. Mekanismen er kjent fra ISDN-rutere og modemtjenere, og reduserer sjansene for at innbrytere skal kunne prøve seg fra tilfeldige tilkoblingspunkter. For legitime brukere er det fortsatt mulig å sette over det oppgitte telefonnummeret, og derigjennom øke fleksibiliteten – og risikoen.
- ✓ **Faste nummer:** En annen variant er å kreve at brukeren ringer fra ett eller flere registrerte nummere. Effekten er den samme som for tilbakeringing, men muligheten for å 'lure' systemet er større – dog avhengig av det lokale telefonsystemet.

Medaljens bakside

Alle disse egenskapene vil – enkeltvis eller i kombinasjon – bidra til å styrke sikkerheten. Å kjenne til dem er første trinn på veien til å ta dem i bruk – i et omfang og på en måte som passer til behov og forhold forøvrig.

I all sin positive tilstedeværelse, har også RRAS sine svake sider, som hører med til helhetsbildet, og som det er viktig å være oppmerksom på. De viktigste er:

- ✓ RRAS er programvare – på samme måte som IPSec-implementasjonen vi har diskutert tidligere. Dette har uunngåelige ytelsesmessige konsekvenser, og skalerer dårlig i forhold til spesialisert hardware. Akseleratorer hjelper, og det er mulig å komme et stykke på vei med intelligente nettverkskort (med IPSec-støtte) og spesialgrensesnitt for oppringte forbindelser.¹⁰ Slike hybride løsninger blir imidlertid sjelden kosteffektive, spesielt når driftsproblematikk tas med i beregningen.

- ✓ RRAS er et komplisert stykke programvare, og brukergrensesnittet for konfigurasjon er ikke blant de mest vellykkede. Det betyr i praksis at feilsøking og -retting blir vanskelig og tidkrevende – et forhold vi også kommer inn på i neste utgave. En rekke såkalte Q-artikler i Microsofts kunnskapsbase er knyttet til nettopp RAS og RRAS, og utdyper en del mindre opplagte forhold. For eksempel injiserer RRAS nye regler i IPSec – automatisk og i det stille – når forbindelser etableres via L2TP. Det skal søkes lenge og grundig i *on line* dokumentasjon for å finne noe om dette, mens effektene blir umiddelbart synlige på systemet. Uker og måneder med feilsøking kastes lett bort på grunn av slike finurligheter.

Installasjon, verktøy

RRAS er installert og klar til bruk på et W2k tjener-system. I tillegg til det grafiske drifts/konfigurasjons-verktøyet, finnes det et kommandolinjeverktøy [netsh.exe] som kan brukes til å styre alle sider av RRAS-systemet. Som tilfellet er for IPSec, gir kommandolinje-verktøyet en langt mer nøyaktig og detaljert kontroll over systemet, og vil uten tvil være ekspertenes preferanse.

Videre finner vi en håndfull nyttige verktøy i tilknytning til det såkalte *Resource Kit*, som må anskaffes separat fra Microsoft og som er vel verdt investeringen: En gullgruve av verktøy og informasjon som et profesjonelt miljø ikke bør være foruten. Et voksende antall av verktøyene kan lastes ned fra Internettet, men de viktigste er fortsatt kun å finne på ressurs-CDen. RRAS-verktøyene hører – dessverre – til denne gruppen.

Nyttige RRAS-verktøy som er å finne på **Windows 2000 Resource Kit CD**:

- RASSVRMON.EXE
- RASUSERS.EXE
- IASPARSE.EXE
- RASLIST.EXE
- TRACEENABLE.EXE

Sistnevnte er også tilgjengelig via Internettet.

Neste utgave

I neste utgave avslutter vi denne artikkelserien med en presentasjon av viktige VPN-spesifikke forhold og en gjennomgang av praktiske råd knyttet til RRAS: *Best Practices*. ■

¹⁰ Digi Inc. er den best kjente leverandør av slike 'konsentrator-kort' for PC-plattformen, se www.digi.com.