

Sikkerhet og Windows 2000

Dette er tredje artikkel i en serie som startet i Mellvik-Rapporten nr. 86.

Det hagler med pepper over Microsoft i disse dager: Sikkerheten og påliteligheten svikter under et voksende press fra virus, trojanske hester og andre former for nettverksbaserte angrep, og avslører en situasjon de fleste av oss var kjent med fra før: At produktene er altfor kompliserte og 'integreerte' til å kunne gi den sikkerhet og pålitelighet markedet trenger – et faktum vi kom inn på i forrige artikkel.

Virus, pålitelighet og Windows

Til tross for denne erkjennelsen, fortsetter Windows generelt og Windows 2000 spesielt sin fremgang i markedet. Med andre ord er det nærliggende å konkludere med at svakhetene ikke kan være alvorlige nok til å skremme kundene. Eller er det alternativene som mangler?

Vi skal ikke ta fatt i den generelle diskusjonen, men holde oss til Windows 2000 – som også får så ørene flagrer. "Windows 2000 krever en sjekklister på 3.000 punkter for å sikres tilfredsstillende" blir det hevdet i Computerworld 28/9/01. Sammenhengen er en diskusjon mellom sikkerhetseksperter etter siste ukers virusangrep, og påstanden er

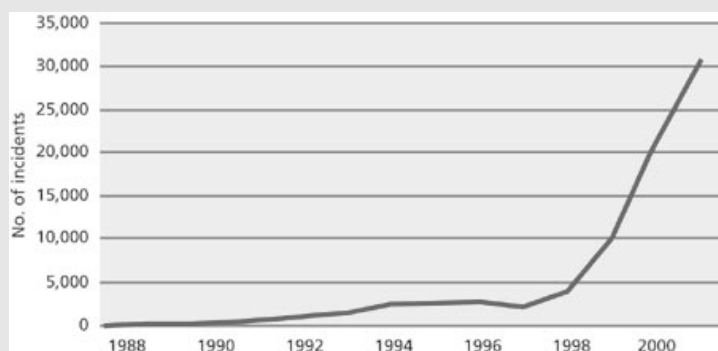
isolert sett riktig. På den ene siden er W2k – som vi har påpekt tidligere i denne serien, Microsofts første operativsystem med gjennomtenkte og funksjonelle sikringsmekanismer: Arkitekturen, mekanismene og verktøyene er der og fungerer. At de ikke er optimale er en annen sak – få systemer på markedet kan få en slik betegnelse når de betraktes fra en sikkerhetsmessig synsvinkel. 3.000 parametre som kan justeres, og som i betydelig grad påvirker hverandre, forteller sitt om kompleksiteten i systemet generelt og sikringsmekanismerne spesielt, og forutsetter en effektiv overbygning for å kunne brukes.

Med hensyn til hva som skal til for å etablere en rimelig grad av sikkerhet, er situasjonen noe enklere enn den fremstilles. Kun i ekstreme tilfeller er det nødvendig eller ønskelig å berøre alle eller de fleste av

Sikkerhet, forsikring og motivasjon

Sikkerhet og sikringstiltak er et nødvendig onde – de er kostbare, tidkrevende og ofte hemmende for brukerne. Dessuten er de positive resultatene sjelden synlige. Fellestrekkene med forsikring er med andre ord tallrike: Vi betaler premier og investerer i tiltak som reduserer premiene, men ser forhåpentlig aldri resultatene – utover bedre nattesøvn og større trygghet for ansatte, kunder og myndigheter.

Med økende fokus på IT-sikkerhet i media og generelt, er veien til investeringsmidlene blitt enklere og kortere. Dette er den eneste positive effekten vi kan se av de siste års utvikling: Veksten i IT-relaterte innbrudd, skadeverk, virus og andre varianter vokser voldsomt, som diagrammet fra CERT (CENTER FOR INTERNET SECURITY, CARNEGIE MELLON UNIVERSITY) illustrerer. Utviklingen med hensyn til finansielle tap som følge av slike aktiviteter følger etter: Amerikanske CSI, COMPUTER SECURITY INSTITUTE, forteller at innrapporterte tap (i USA) for første halvår 2001 beløp seg til USD 377,8 mill. fordelt på 186 rapporter. Tallene for hele 2000 var 249 rapporter og en samlet sum på USD 265,6 mill.



3.000 enkelt-punkter. Spesielt dersom Active Directory tas i bruk og kompatibilitet med NT fjernes, blir oppgaven overkommelig.

At sikringsmekanismene finnes, er imidlertid ikke det samme som at de er pålitelige. Systemer har feil, verktøy har feil, implementasjoner er feil, arkitekturer er kompliserte og uoversiktlige. Mekanismene i W2k gir god sikkerhet i forhold til sine tidligere slektninger, og kan – når konfigurasjonen er optimal og kjente hull tettet – gi adekvat sikkerhet for alminnelige formål.

Denne erkjennelsen er det viktig å ha med i betraktninger knyttet til sikkerhet: Å gå gjennom en sjekkliste – kort eller lang – for W2k, gir beskjeden sikkerhet på egen hånd, men skal være ett av elementene i en større sammenheng, som summert gir en tilfredsstillende sikkerhet for organisasjonen. Uansett om systemene er basert på W2k, Solaris, Linux eller noe annet, er sikringen av dem en del av dybdeforsvaret, ikke et selvstendig tiltak. Hvilken rolle systemene spiller i organisasjonen, er avgjørende for hvor grundig vi går til verks og hvilke tiltak og mekanismer vi velger å benytte.

Når vi i forrige artikkel fokuserte på IPSec og de mulighetene for sikring som ligger i Microsofts (egentlig Ciscos) implementasjon, er årsaken at W2k-systemer ofte er å finne i kanten av nettverket – som tjenere for fjernaksess, eller som universaltjenere i tusenvis av små og mellomstore organisasjoner. I slike sammenhenger og omgivelser representerer IPSec-implementasjonen et viktig og effektivt sikringsverktøy som ikke kan ignoreres.

IPSec fortsetter

Gjennomgangen i forrige artikkel presenterte implementasjonen av IPSec, og konstaterte at den har en lang rekke egenskaper som på den ene siden er lite kjent, og på den andre siden både effektive og lett tilgjengelige. I gjennomgangen nedenfor avslutter vi diskusjonen med en oppsummering av verktøyets mangslungne sider, og noen praktiske råd med hensyn til hvordan det kan tas i bruk i en organisasjon: Hvilke valg som er å anbefale under gitte omstendigheter.¹

Gjennomgangen nedenfor er av åpenbare årsaker relativt teknisk av natur, og refererer hyppig til uttrykk og begreper som er unike for W2k. For sikkerhets- og driftsansvarlige som omgås W2k daglig, hører disse uttrykkene til dagligtalen.

Kryptering, autentisering

- ✓ 3DES er den sikreste og mest ressurskrevende krypteringsalgoritmen, og bør benyttes der sikkerhet mot innsyn er spesielt viktig. Forgjengeren DES er OK der behovet for sikring er mer beskjeden, og hensyn til ytelse og kompatibilitet har

DES – *Digital Encryption Standard*, etablert tidlig på 80-tallet, benytter 56-bits krypteringsnøkler. Betraktes ikke lenger som 'god sikring'.

3DES – *Triple DES*, modernisert utgave av DES-standard som er blant de sikreste standard-algortimene på markedet i dag.

¹ Organisasjonen SANS, som vi hyppig har referert til i forbindelse med sikkerhet, har lagt ned en stor jobb for å utvikle kunnskap om sikring av Windows 2000. Blant annet har SANS utviklet et praktisk arbeidshefte med navnet "Securing Windows 2000 step by step", som er av uvurderlig verdi for profesjonelle sikkerhets- og driftsansvarlige. Utvalget av områder som prioriteres i denne artikkelen er påvirket av erfaringer SANS har samlet inn fra tusenvis av organisasjoner i USA og resten av verden.

høy prioritet. Mens DES er langt bedre enn ingen kryptering, er det viktig å være klar over at algoritmen er relativt lett å knekke med dagens utstyr. Bruk av 3DES forutsetter at den såkalte *High Encryption Pack* installeres.

- ✓ For integritets-sikring er SHA1-algoritmen bedre enn den mer kjente MD5, mens sistnevnte gir best interoperabilitet med andre produkter og plattformer. Dessuten er implementasjonen av SHA1 i W2k svak, med den følge at den praktiske forskjellen mellom de to alternativene er beskjeden. Derfor anbefales MD5.
- ✓ W2k tilbyr et valg mellom to såkalte Diffie-Hellman grupper, som avgjør størrelsen på enkelte krypteringsnøkler. 1024 bits er alternativet som anbefales, fordi den ytelsesmessige forskjellen mellom 768 og 1024 er minimal.
- ✓ Når to systemer skal kommunisere, forhandler de seg gjerne frem til et minste felles multiplum av parametre. I mange tilfeller betyr det at et system som er satt opp til å bruke 3DES-kryptering, ender opp med å bruke DES i stedet. Dette er ikke nødvendigvis akseptabelt, og kan unngås ved å spesifisere at kun 3DES blir godtatt. Kommunikasjon med parter som kun støtter DES, vil da bli blokkert.
- ✓ Å benytte autentisering via nøkler som er utvekslet i forkant (*presshared keys*), er ikke tilrådelig, og kun akseptabelt midlertidig i forbindelse med test-systemer og -oppsett.
- ✓ Kerberos²-implementasjonen i W2k er, som vi har vært inne på tidligere, verken feilfri eller helt kompatibel med andre plattformer. Ikke desto mindre gir Kerberos-autentisering et betydelig bidrag til sikkerheten.
- ✓ Når god sikkerhet er påkrevet og Kerberos ikke er tilgjengelig, bør autentisering via digitale sertifikater benyttes – for eksempel i forbindelse med fjernaksess via VPN.

Nøkler, levetid og PFS

PFS – *Perfect Forward Security* – er en mekanisme som sikrer at automatisk genererte krypteringsnøkler aldri kan brukes om igjen. Dette kan høres ut som en selvfølge, men er tvert imot alminnelig. Å generere slike nøkler tar tid og ressurser, og det er en alminnelig effektivisering å ta vare på noen eller alle grunnelementene en nøkkel genereres fra. Dermed kan nye nøkler raskt genereres – med den ulempe at de er 'beslektet' med en som tidligere er benyttet, hvilket svekker sikkerheten et hakk.

I oppsettet av IPSec kan vi velge om PFS skal benyttes eller ikke. Mekanismen gir alltid bedre sikring, og har en pris i form av ressursforbruk.

- ✓ Innstillingene for krypteringsnøklenes levetid bør generelt være som de leveres. Standardverdiene representerer fornuf-

² Se Mellvik-Rapporten nr. 16.

tige valg for de fleste omgivelser. Å forkorte levetiden for nøkler gir ikke i seg selv bedre sikkerhet, men reduserer mengden data som kompromitteres dersom koden skulle bli knekket. Når sikkerheten er spesielt kritisk, er det mer effektivt å bytte til 3DES-kryptering og PFS enn å redusere nøkkelens levetid. Dessuten er endringer i levetiden negativt for kompatibiliteten mellom ulike IPSec-implementasjoner.

- ✓ Når sikkerhet er spesielt kritisk, bør *Master Key Perfect Forward Security* benyttes. Den ytelsesmessige kostnaden er betydelig, fordi 'hovednøkkelen' ikke kan byttes uten at avledede 'sesjonsnøkler' også regenereres.
- ✓ Med mindre effektivitet er viktigere enn sikkerhet, er det hensiktsmessig å benytte *Session Key Perfect Forward Security*.
- ✓ Et godt kompromiss mellom sikkerhet og effektivitet er å velge *Session Key PFS* inn, og *Master Key PFS* ut.

Regler og enkelhet

Ulike egenskaper i IPSec aktiviseres gjennom regler og grupper av regler, typisk via dialogbokser der vi krysser av våre valg og preferanser. Vi påpekte i forrige artikkel at systemets kommandolinje-verktøy er både mer pålitelige og gir bedre oppløsning i valgene enn de vindusbaserte variantene. På grunn av tidspress og andre forhold, vil imidlertid de vindusbaserte verktøyene være fullstendig dominante i praksis.

Reglene som styrer IPSec i Windows 2000, kalles *Policy Objects*, policyobjekter. De konfigureres og aktiviseres via dialogbokser som i de fleste tilfeller har fornuftige startverdier for alminnelige miljøer. Ikke desto mindre er det viktig å forstå hva uttrykk og begreper betyr, og hvilken effekt de har. W2k's hjelpesystem gjør en rimelig jobb med hensyn til beskrivelse, men gir liten innsikt i konsekvensene av de ulike valgene. Dette er motivasjonen bak vår relativt detaljerte gjennomgang her: Liten tue kan velte stort lass. Første punkt nedenfor er et godt eksempel:

- ✓ Vær ekstremt forsiktig med valgene '*Accept unsecured communication, but always respond using IPSec*' og '*Allow unsecured communication with non-IPSec-aware computers*'. Fritt oversatt betyr dette at vi ønsker å være sikre når det er mulig, men det er akseptabelt med null sikkerhet. Å aktivisere disse vil med andre ord bety å nullstille alle andre IPSec-baserte sikringstiltak.
- ✓ I filtre og enkelte andre sammenhenger kan vi i innstillingsbildet velge mellom *My IP Address*, *Any*, *Subnets* eller en spesifikk IP-adresse. Her er det hensiktsmessig å unngå spesifikke IP-adresser for å ta vare på både automatikk og sikkerhet. Unntaket er systemer som har flere nettverks-grensesnitt, og som typisk krever ulike regler for hvert av dem. På et slikt (*multihomed*) system, vil bruk av *My IP Address* føre til at definerte filter-regler blir anvendt likt på alle grensesnitt. Det er sjelden ønskelig.

- ✓ Filter-regler kan og bør i de fleste tilfeller speiles, det vil si at samme regel skal gjelde for inngående og utgående trafikk til og fra en gitt adresse eller et nettverk. Å benytte den muligheten verktøyene gir for aktivering av 'speilregler', gir et enklere regelverk, god standardisering og bedre sikkerhet.
- ✓ Systemer som leverer infrastrukturtjenester som DHCP, DNS, WINS, SNMP, RRAS og domene-kontrollere, må behandles med spesiell omhu. Å aktivisere IPSec-filtre her er det samme som å blokkere aksess fra klienter som ikke kjører IPSec. Det hører til sjeldenhetene at alle klienter er sikret på denne måten. At slik sikring er en god idé når ressursene forøvrig strekker til, er en annen sak.
- ✓ Filter-regler og tilhørende prosedyrer bør lagres i Active Directory, slik at de kan inngå i en hvilken som helst policy. Gjenbruk betyr forenkling. Med god planlegging, testing og riktig navngiving blir det lett å benytte det samme regelsettet i hele organisasjonen. Grundig dokumentasjon som alltid er oppdatert for hver enkelt regel, er like kritisk. Videre er det i de fleste tilfeller bedre å lage nye regler enn å flikke på eksisterende. På den måten unngår vi utilsiktede følgeskader av at regler er benyttet andre steder enn 'antatt'.

Gruppe-policy

Grupper er et tøyelig begrep i W2k, som blant annet avhenger av hvordan systemet er konfigurert. Samtidig er grupper og gruppetilhørighet selve nøkkelen til å utnytte mulighetene som finnes til å håndheve aksessrestriksjoner – for brukernes tilgang til filer, systemer og andre ressurser. Igjen er det god planlegging som skal til for å lykkes, ved siden av at den eller de som planlegger, må ha god innsikt i hvilke muligheter som finnes, og hva de ulike alternativene betyr i praksis. Kurser og opplæring er nyttig, men praktiske øvelser gir de beste resultatene: Øvelse gjør mester – og gir innsikt.

En gruppe kan dekke én person eller et helt domene, og alle nivåene imellom. Grunnregelen for tilordning av grupperegler er at de aldri skal gjelde på domene-nivå, men holdes til OU (*Organizational Unit* – avdeling eller enhet) eller lavere. Unntaket som bekrefter regelen er at en overordnet 'Respond Only Rule' bør etableres på domene-nivå, for å fange opp tilfeller der en OU mangler IPSec-policy.

- ✓ Det er en god idé å lage gruppe-policy objekter (GPO) som kun inneholder IPSec-regler, og deretter sørge for tett skrivebeskyttelse for objektene, slik at de ikke kan endres av andre – ei heller systemadministratorer. Flere kokker gir mer søl, også blant eksperter. For å sikre at beskyttelsen blir varig, er det lurt å sørge for logging av alle forsøk på modifikasjon. En slik grad av paranoia rettferdiggjøres av kompleksiteten i og viktigheten av IPSec-objektene: Her etableres – eller ødelegges – sikkerheten på systemet. For kritiske systemer har dette smitteeffekter til hele nettverket og organisasjonen.

- ✓ Når et GPO som inneholder IPSec-regler skal slettes, må koblinger til aktive filtre først frigjøres. Deretter må endringen få tid til å spre seg gjennom systemet, eller vi kan forsere en slik spredning eksplisitt.

VPN, tunneller

VPN står for de fleste som hovedområdet for IPSec, en oppfatning vi har behørig satt til veggs i disse to artiklene: VPN er ett av en håndfull anvendelsesområder, alle med høy nytteverdi i sikkerhetsmessig sammenheng.

Vi konstaterte i forrige artikkel at støtte for IPSecs tunnel-modus er marginal i Windows 2000: Tilstrekkelig til å være innenfor standardens minimumsgrenser, men heller ikke mer. I praksis betyr det at L2TP benyttes for tunneller, hvilket neppe burde forårsake komplikasjoner.

Tvert imot sørger bruken av L2TP for å fjerne komplikasjoner knyttet til IPSecs tunnel-modus, for eksempel i forbindelse med rutingprotokoller som OSPF og RIP.

Ytelse og hardware-støtte

Nettverksgrensesnitt med innebygget støtte for IPSec ('hardware-akseleratorer') er effektive, relativt billige og bør brukes der det lar seg gjøre. Uten slik støtte er det ikke uvanlig at IPSec med 3DES/SHA1 legger beslag på 90% av CPU-kapasiteten på et typisk system. Effektivt båndbreddeutnyttelse kan falle fra 100 Mbps til ca. 40 Mbps eller lavere, avhengig av systemets CPU- og hukommelsesressurser. Nettverkskort med IPSec-støtte er tilgjengelige på markedet for rundt NOK 1.000.

Merk at slike akseleratorer kun tar hånd om kryptering av utgående trafikk. Den innkommende trafikken må fortsatt dekrypteres av systemet selv. Derfor er det en god idé å evaluere tilgjengelige CPU-ressurser uansett, med tanke på oppgradering av hastighet eller eventuelt flere prosessorer. Målinger foretatt av Intel viser at med selskapets PRO/100S nettverkskort, som har IPSec-støtte, i et system med 500 MHz Celeron prosessor og 128 MB hukommelse, var CPU-belastningen 73% ved en kontinuerlig IPSec-overføring.

Dette er tall til ettertanke, ikke minst fordi nettopp dette nettverkskortet er anerkjent for sin effektive IPSec-håndtering. Det er en nyttig påminnelse om at sikkerhet alltid har en ytelsesmessig kostnad som – selv med våre dagers prosessorer – er signifikant.

Derfor går det aldri av moten å tenke effektivitet: Vi krypterer ikke 'i utrensmål'. Forbindelser som allerede er sikret på andre måter, for eksempel med SSL eller TLS (epost, Web-transaksjoner osv.), er det meningsløst å sende gjennom IPSec.

OSPF – *Open Shortest Path First*
(rutingprotokoll)

RIP – *Routing Information Protocol*

L2TP – *Layer 2 Tunneling Protocol*

SSL – *Secure Socket Layer*

TLS – *Transport Level Security*, egentlig det samme som SSL, med enkelte påplusninger fra IETF, *Internet Engineering Task Force*.

IPSec og NAT

NAT, *Network Address Translation*, er svært populært i forbindelse med småkontorer og hjemmekontorer (se Mellvik-Rapporten nr. 59). NAT forandrer adresse- og port-feltene i pakkene, slik at et helt nettverk kan forbindes til Internettet og kun bruke én enkelt offisiell adresse. Dette er nyttig og effektivt på mange måter, ikke minst sikkerhetsmessig, men kan ikke benyttes sammen med IPSec: Når datastrømmen er behandlet av IPSec, kan ingen ting forandres, ei heller adressene. Den samme problemstillingen gjelder for alle slags proxyer – for filoverføringer, Web-trafikk og så videre.

Løsningen er å sørge for at IPSec, NAT-oversettelse og proxy-funksjoner håndteres av samme boks som forbinder det interne nettverket til Internettet. Vi forsaker sikkerhet ende til ende, i og med at trafikken dekrypteres ved kanten av det interne nettverket, og må ha et forhold til hvilke konsekvenser dette kan ha. For et lite nettverk uten andre forbindelser utad, er dette ofte akseptabelt.

Neste utgave

Seriens fjerde artikkel tar for seg fjernaksess-tjenestene i Windows 2000 sett fra et sikkerhets-perspektiv. På samme måte som tilfellet er med IPSec, har RRAS – *Routing and Remote Access Service* – langt mer å by på enn navnet indikerer. Blant disse egenskapene finner vi også mekanismer som tar vare på svakheter i IPSec-implementasjonen. ■