

Sikkerhet og Windows 2000

Windows 2000 og sikkerhet er et tema som berører svært mange av oss. I artikkelserien som begynner i denne utgaven, setter vi fokus på hva Microsoft har gjort for å bidra til større sikkerhet, hvordan tiltakene virker og ikke minst hvordan de kan utnyttes i praksis.

Stødig vekst for W2k

Ekspertene strides fortsatt om hvorvidt Windows 2000 fortjener betegnelsen 'moderne operativsystem', og om Active Directory er en katastrofe eller en velsignelse. I mellomtiden finner systemet veien inn i et jevnt voksende antall miljøer verden over – ikke med den hastighet Microsoft hadde håpet, men med god fremdrift.

Diskusjonen om metoder og betegnelser blir dermed primært av politisk eller akademisk verdi. En IT-gruppe, -avdeling, -leder eller -ansvarlig har langt mer praktiske problemstillinger å ta vare på: Å sørge for at organisasjonen får profesjonelle IT-tjenester av høy kvalitet til riktig pris, herunder besørge at sikkerheten blir ivaretatt – på egen hånd eller sammen med en sikkerhets-gruppe. I denne virkeligheten er det liten plass til faglige eller akademiske diskusjoner som ikke direkte berører dagens situasjon eller planer for fremtiden.

Windows 2000 er en del av denne virkeligheten, i tallrike organisasjoner en særdeles viktig del: Avhengigheten av IT-systemene er total, og Win2k er en av pilarene de er bygget på – i mange tilfeller sågar den eneste. Det betyr – blant annet – at nettopp disse systemene er naturlige angrepspunkter for interne eller eksterne 'inntrengere', og derfor krever spesiell oppmerksomhet med hensyn til sikkerhet og sikring.

Et dårlig renommé

Tidligere utgaver av systemet – under NT-navnet – har med god grunn vært beryktet for slett sikkerhet og tallrike hull. Derfor har Microsoft gjort en ekstra innsats på sikkerhetsfronten i forbindelse med utviklingen av W2k. For første gang kan et operativsystem fra Microsoft karakteriseres som gjennomtenkt sett fra en sikkerhetsmessig synsvinkel. Den amerikanske Windows- og sikkerhets-eksperten Eugene Schultz sier det slik: "W2k er et dramatisk fremskritt i forhold til NT på de fleste områder, og spesielt på sikkerhetsfronten. Dette gjelder hull, svakheter, mekanismer og ikke minst verktøy."

Forholdet – som er viden kjent – burde føre til at salget av Windows NT 4.0 stoppet momentant, og at W2k klatret raskt oppover på statistikene. Så har imidlertid ikke skjedd: Tall for første kvartal 2001 viser at NT 4.0 fortsatt ligger foran W2k på salgsstatistikken. Forspranget krymper, men langt fra så raskt som både Microsoft og de av oss som er opptatt av sikkerhet, kunne ønske. Situasjonen demonstrerer nok en gang at den påstått voldsomme forandringshastigheten i IT-bransjen først og fremst er å finne hos journalister og entusiaster. Næringsliv og forvaltning er avhengige av stabilitet og pålitelighet, mens forandringer, oppgraderinger og oppdateringer er forstyrrelser. Dessuten er det et faktum at W2k er et langt mer komplekst system enn forgjengeren. Denne kompleksiteten skremmer – med god grunn. Det faktum at den etablerte påliteligheten – i form av Windows NT 4.0 –

også betyr dårlig sikkerhet, merkes ikke før ulykken er ute, og representerer et beskjedent incentiv til å forsere utskiftingen for de fleste miljøer. Microsofts stadige forandringer av lisensbetingelser, avtaler og priser drar i samme retning.

Arkitektur kontra virkelighet

Det året Windows 2000 har vært i alminnelig drift, har nok en gang demonstrert at mens arkitektur er én ting, er implementasjon noe annet. Om arkitekturen er aldri så bra, har vi ingen garanti for at systemet er bygget og satt sammen slik arkitektene hadde forestilt seg. God sikkerhet er et resultat av en solid og gjennomtenkt arkitektur, implementert av fagfolk som for det første forstår arkitekturen, og for det andre kan utøve håndverk av høy kvalitet. Spesielt på siste punkt svikter det – hos de fleste programvareleverandører. Ikke bare er programmererne mangelfullt opplært og uerfarne. I tillegg har selskapene altfor dårlige regler og rutiner for hvordan programmeringen skal utføres – og testes (*engineering practices*). Å bli fort ferdig er viktigere enn å levere god kvalitet hos de fleste. Resultatet er – blant annet – ustabile systemer som er fulle av sikkerhetshull.

Derfor er strømmen av sikkerhetsbulletiner – fra Microsoft og andre – stor, for W2k, IIS, Outlook, Internet Explorer og så videre. Vår oppgave som system- og sikkerhetsansvarlige er å holde øye med denne utviklingen og sørge for at vi i minst mulig grad blir eksponert for konsekvensene. At vi ikke kan forlange erstatning eller fri hjelp til feilretting

fra leverandøren, er en historisk unik situasjon som vi har diskutert tidligere her i Mellvik-Rapporten, og som skal få ligge i denne omgang.

Vi begynner vår artikkelserie med en gjennomgang av hovedelementene i det vi kan kalle W2k's sikkerhetsarkitektur. De påfølgende artiklene har en mer praktisk orientering, med presentasjoner av hvordan arkitektur og verktøy kan utnyttes, og hvordan svakheter og hull kan tettes.

Windows 2000 finnes i fire ulike varianter, alle bygget over samme lest, men med ulik 'vekt- og styrkefordeling' og forskjellig 'standardutstyr'. Vår diskusjon er konsentrert om W2k Advanced Server, og er like relevant for Data Center Server. Arbeidsstasjonsvarianten

Microsoft går sine egne veier

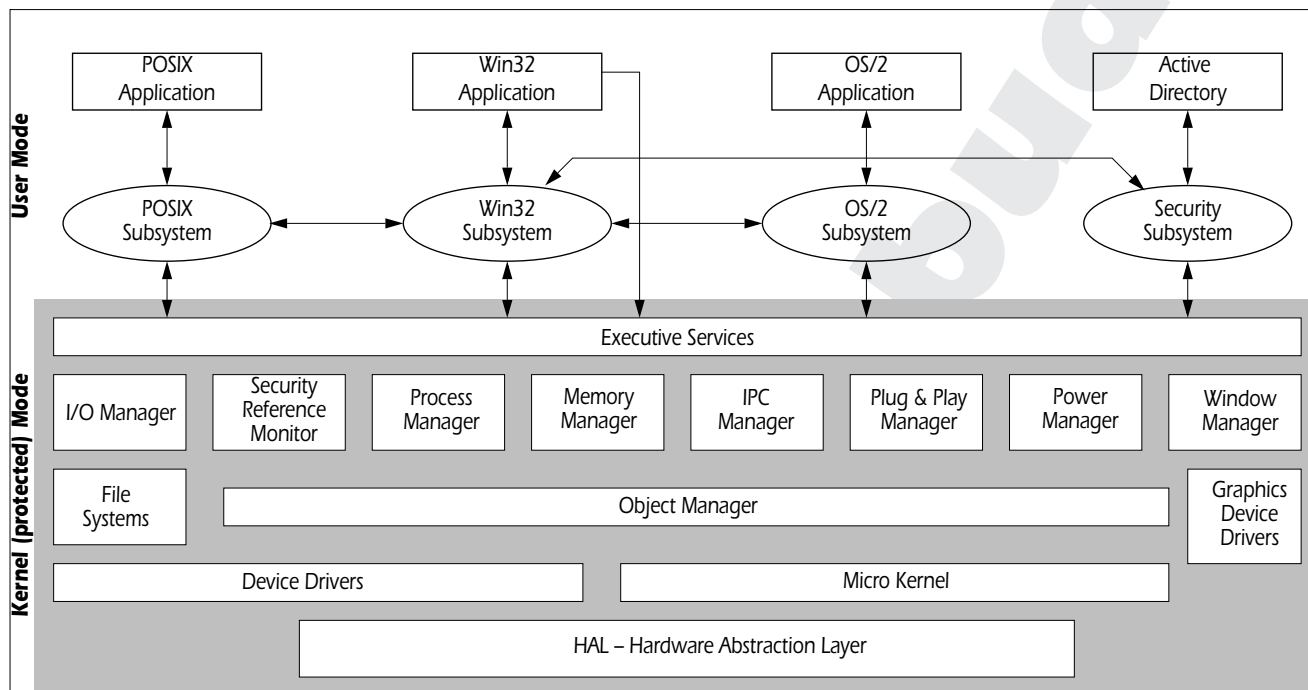
Microsofts velkjente "embrace and extend" policy er gyldig også på sikkerhetsområdet. Den går i korthet ut på at selskapet omfavner etablerte standarder, for deretter å utvide dem til å dekke egne spesifikke behov. Microsofts utgave av standardene blir dermed ikke lenger kompatible med den egentlige standarden, kun med seg selv. Strategien er velkjent i et historisk perspektiv, og virker kun for aktører som er fullstendig dominante i markedet og derigjennom kan tillate seg å velge bort muligheter til samspill med andre via standarder.

Microsoft har på denne måten 'sjanghaiet' en lang rekke standarder de siste ti årene. Argumentet for forandringene er uten unntak at 'standarden var for snever, utvidelser var nødvendige for å kunne implementere våre avanserte løsninger'. Mens det alltid kan argumenteres for utvidelser og tillegg, er poenget med standarder å skape kompatibilitet, ikke å dekke alle tenkelige situasjoner. Kompatibilitet og samspill betyr forsakelser – vi får ikke i pose og i sekk.

I tilknytning til Windows 2000 og sikkerhet, er følgende standarder og utvidelser spesielt relevante:

- DNS, navnetjenesten i Internettet, er utvidet i W2000 og integrert med katalogtjenesten Active Directory. Mens systemet gjerne kan kjøres sammen med en standard DNS-tjeneste i nettverket, eliminerer et slikt valg muligheten til å utnytte den universelle katalogtjenesten Active Directory tilbyr: Adresser, maskinnavn, lisenser, hardwareinformasjon, generelle inventarlistor, brukere, privilegier, linjer, kapasiteter og så videre. Det er mulig, men ekstremt krevende å holde Active Directory manuelt oppdatert med statisk DNS-informasjon. Med dynamisk adressetildeling (DHCP) blir det umulig. Dermed blir det nødvendig å benytte den utvidede DNS-tjenesten som er inkludert i W2k, men som i sin tur ikke er kompatibel med systemer som ikke kjører Windows.
- Kerberos 5 benyttes i forbindelse med autentisering av brukere – et positivt valg for sikkerheten, og utvidelsene i forhold til standarden er beskjedne. De er imidlertid store nok til å forårsake inkompatibiliteter i forhold til andre produkter som implementerer standarden. Verre er det at implementasjonen er plaget av hull som legger autentiseringssystemet åpent for angrep (se <http://ic.unicamp.br/~ra941613/w2k>). Det finnes ingen enkel vei rundt denne svakheten. Løsningen er å bruke andre autentiseringssystemer, via Smartkort og tilhørende støttetjenester som er inkludert i W2k eller tredjeparts produkter.

og den grunnleggende tjener-utgaven mangler noen av verktøyene og tjenestene som blir diskutert, men deler den underliggende sikkerhetsarkitekturen.



Figur 1 Arkitekturen i Windows 2000 ligner til forveksling på tilsvarende i NT 4.0. Ved nærmere ettersyn finner vi likevel en rekke forskjeller. Blant annet har Active Directory erstattet WinLogon, og spiller nå en sentral rolle i et system som er blitt enda mer omfattende og komplekst.

System- og sikkerhetsarkitektur

Selve systemarkitekturen for Windows 2000 (figur 1) ligner til forveksling på NT, og er naturlig nok fundamentalt den samme. Det er innholdet i en rekke av blokkene som er forandret, utvidet eller fullstendig nytt. Ved nærmere ettersyn ser vi videre at WinLogon Manager er erstattet av Active Directory, som har fått en nøkkelrolle i hele systemet, ikke minst i forbindelse med sikkerhet. Videre har kjernen – det skraverte området på figuren, fått en rekke nye elementer, blant annet *Plug & Play Manager* og *Power Manager*. Begge disse er av størst interesse for bærbare systemer, og det kan argumenteres for at det burde være mulig å fjerne dem fra systemer der de ikke benyttes – i den hensikt å forenkle og stabilisere systemet.

Viktig for de fleste anvendelser er den nye *Virtual Memory Manager* (VM), som sørger for en vesentlig økning i anvendelsesområdet for operativsystemet. Tilsvarende under NT 4.0 var en regulær katastrofe, med den følge at systemene måtte utrustes med store mengder primærhukommelse for å fungere. Til alt hell har slik hukommelse falt dramatisk i pris i løpet av tiden NT har vært med oss, hvilket har avhjulpet problemet betydelig. Imidlertid er det et anerkjent faktum at NT 4.0 vanskelig kan fungere effektivt som Web-tjener, DNS-tjener og for en rekke andre tjenester som byr på stor belastnings-dynamikk.

Videre er det verdt å nevne at POSIX-subsystemet, som ble introdusert i NT 4.0 for å tilfredsstille krav om Unix-kompatibilitet fra det amerikanske forsvaret, aldri virket etter spesifikasjonen i NT og fortsatt ikke gjør det i W2k.

Tabell 2 Oversikt over progresjonen på sikkerhetsfronten fra Windows NT 4.0 til Windows 2000 Advanced Server.

Egenskap	Win NT 4.0	Win 2k
Autentisering	NTLM	NTLM, Kerberos, ^a andre mekanismer
Programmeringsgrensesnitt for sikkerhet (API)	CryptoAPI	CryptoAPI, SSPI
Aksesskontroll for objekter	NTFS-beskyttelsesmekanismer	NTFS-beskyttelsesmekanismer basert på en ny utgave av filsystemet med flere muligheter, større oppløsning.
Administrasjon	SAM-database, Security Configuration Manager	Ny utgave av Security Configuration Manager, Active Directory, Smartkort
Kryptering av nettverks-trafikk	PPTP, SSL, Secure DCOM	PPTP, SSL, Secure DCOM, IPSec, L2TP
Kontroll/logging	Event Logger	Event Logger, Active Directory
Filkryptering	Ingen	Encrypted File System (se kommentar nedenfor)
PKI – styring av sertifikater og krypteringsnøkler	Certificate Server, SSL	Certificate Server, SSL, Active Directory

a. Se kommentar om Kerberos på side 23.

NTLM – NT LAN Manager
API – Application Programming Interface
NTFS – NT File System
SSPI – Security Support Provider Interface
PKI – Public Key Infrastructure
SAM – Security Account Manager
SSL – Secure Socket Layer
PPTP – Point-to-Point Tunneling Protocol
DCOM – Distributed Component Object Model
IPSec – IP Security, standard VPN-protokoll for IP
L2TP – Layer 2 Tunneling Protocol

Tabell 2 sammenligner NT og W2k med fokus på sikkerhetsegenskaper, og viser at Microsoft har tatt oppgaven alvorlig. Som vi nevnte innledningsvis, er imidlertid avstanden mellom intensjoner og virkelighet betydelig. Praktisk erfaring med systemet har foranlediget følgende viktige observasjoner:

- ✓ EFS, det krypterte filsystemet, er for upålitelig til å kunne brukes. Filer forsvinner tilfeldig og sporløst, og Microsoft lover ingen bedring før i neste utgave av Windows (XP).
- ✓ Kerberos-autentiseringen er ikke bare utvidet i forhold til standarden, men har også en implementeringsfeil som kompromitterer sikkerheten (se ramme på foregående side).
- ✓ Støtte for flere VPN-protokoller er viktig, spesielt IPSec, som er standardprotokollen for VPN-forbindelser. Dette forenkler bruken av VPN mot W2k-systemer. Verktøyene som gjør teknologien tilgjengelig for systemadministratorer, er av kurant kvalitet (vi kommer tilbake til dem senere i serien).

Active Directory

Vi har allerede konstatert at Active Directory er en sentral komponent i Windows 2000, og ikke minst i sikkerhetsmekanismene. Tjenesten samler en lang rekke databaser, registre og filer som tidligere var spredt ikke bare over hele systemet, men på mange systemer i et lokalt nett. Katalogtjenesten er sentralnervesystemet i W2k, og erstatter blant annet den primitive og feilbefengte 'utforsker-tjenesten' (*browsing*) fra NT, som har forårsaket flere tjenesteavbrudd (*DoS*) de siste

årene¹¹ enn all verdens Crackere. Blant dataelementene som inngår i Active Directory, finner vi brukerkonti og brukerinformasjon, data om organisasjonen eller avdelingen, sikkerhets-regler, informasjon om filer, filkataloger, filsystemer, skrivere og annet periferiutstyr, tjenester, domener, regler for samspill mellom objekter, nettverksinformasjon og mye mer. Katalogen overtar en rekke funksjoner som tidligere var tjeneste-spesifikke, for eksempel under epost-tjenesten Exchange eller DNS-tjenesten. Sistnevnte er praktisk talt integrert i Active Directory – en i og for seg logisk utvidelse, men med negative konsekvenser for tallrike miljøer (se rammen på side 23).

I tråd med den virkeligheten Active Directory skal fungere i, er mekanismene for distribuert tilgjengelighet og lagring gode. Alle domene-kontrollere i et domene holdes løpende synkronisert, og applikasjoner kan 'abonnere' på gitte informasjonstyper. Katalogen er organisert etter X.500-standarden og har blant flere aksessmekanismer fått et LDAP-grensesnitt.

LDAP – *Lightweight Directory Access Protocol*, se Mellvik-Rapporten nr. 44 og 57.

DoS – *Denial of Service*

For sikkerheten betyr alt dette på den ene siden at katalogtjenesten må være godt sikret i seg selv: Her ligger nøklene til det meste, også av sikkerhetsmessig art, som autentiserings-informasjon, krypterings-nøkler, sertifikater og så videre. På den andre siden fungerer Active Directory som ' mellomvare ' – en tjenesteleverandør for andre applikasjoner – som tilbyr sikkerhetsrelaterte tjenester knyttet til for eksempel autentisering, aksesskontroll, utveksling av nøkler – for å nevne noen.

Som nervesenter i systemet, er Active Directory en komponent som aldri kan behandles alene, uten å se eller ta hensyn til omgivelsene den fungerer i. Vi kan sikre selve katalogtjenesten forlengs og baklengs, men den blir likevel aldri sikrere enn klientene som bruker den. Denne mangesidige utfordringen blir adressert ved at tjenesten har fått mekanismer og muligheter til detaljert aksesskontroll på objekt-nivå: "Hvem har anledning til å lese, skrive eller forandre hva på hvilke tidspunkter og hvor mye?" Større oppløsning er bedre fordi det gir anledning til å håndheve 'need to know'-prinsippet overfor alle tenkelige objekter – og klienter. Samtidig blir det flere varianter, flere detaljer og mer komplisert administrasjon. Med andre ord et tveegget sverd som krever intelligente mekanismer for å kunne utnyttes positivt. Her kommer såkalte policies – retningslinjer – inn. Ved å definere navngitte samlinger av retningslinjer som kan gjelde for større eller mindre grupper av brukere, programmer, tjenester eller andre objekter, kan utfordringen bli håndterbar. Den krever imidlertid fortsatt både disiplin, konsistens og kontinuerlig oppfølging – ved siden av skikkelige verktøy. ■

Neste utgave

Artikkelserien fortsetter i neste utgave, der vi blant annet skal diskutere hvordan forbedringene på sikkerhets-siden kan aktiviseres og utnyttes.

¹¹ De såkalte valg-mekanismene (ELECTION MECHANISMS) i utforsker-tjenesten i NT er lite robust, og forårsaker lett nettverkstormer – FLOODING, som lammer lokalnettet fullstendig.