IT 08 033
Examensarbete 15 hp
September 2008

Analys och omarbetning av ett företagsnätverk

Rickard Henrikson

Institutionen för informationsteknologi
Department of Information Technology

UPPSALA
UNIVERSITET

Teknisk- naturvetenskaplig fakultet
UTH-enheten

Besöksadress:
Ångströmlaboratoriet
Lägerhyddsvägen 1
Hus 4, Plan 0

Postadress:
Box 536
751 21 Uppsala

Telefon:
018 – 471 30 03

Telefax:
018 – 471 30 00

Hemsida:
http://www.teknat.uu.se/student

Abstract

Analysis and revision of a corporate network

Rickard Henrikson

In this paper, a small business network with around 30 users is analyzed with respect to security, performance and usability. Based on this analysis, two suggestions on how to solve the problems listed are given. The first suggestion focus on keeping a low budget, while the other tries to deal with the problems more thoroughly. One advantage of the first suggestion is, in addition to not straining the company's budget more than nessecary, it does not involve too great changes in the way the network is used and administered. On the other hand, the smaller budget leads to certain compromises, and there is a risk that similar problems occur again if, for example, the company would grow. The second suggestion is designed so that it will solve the current problems in a more thorough manner, while still being easy to adapt if the requirements for the network would change. One disadvantage is that it means a bigger investment than the first proposal, as well as a bigger change in the way every day work is carried out.

Handledare: Mats Brisegård
Ämnesgranskare: Iordanis Kavathatzopoulos
Examinator: Anders Jansson
IT 08 033
Tryckt av: Reprocentralen ITC

Sammanfattning

I denna uppsats analyseras ett företagsnätverk med cirka 30 användare med avseende på säkerhet, prestanda och användbarhet. Med denna analys som grund tas två förslag på hur problemen kan lösas fram. Det första förslaget fokuserar på att lösa problemen med en så låg kostnad som möjligt, medan det andra är inriktat på att lösa problemen mer fullständigt. En fördel med det första alternativet är, förutom att företagets budget inte ansträngs i onödan, att det inte innebär alltför stora förändringar i vare sig drift eller användande av nätverket. Med en relativt liten investering kan arbetet fortsätta ungefär som förut, men med bättre förutsättningar. Å andra sidan leder den mindre budgeten till vissa kompromisser, och risken finns att liknande problem uppstår igen inom en överskådlig framtid, om till exempel företaget växer. Det andra förslaget är utformat så att det ska lösa nuvarande problem på ett mer grundligt sätt, och samtidigt vara lätt att anpassa om kraven på nätverket ändras. En nackdel är att det innebär både större investeringar och större förändringar i arbetssättet än i första förslaget.

Innehåll

1 Introduktion

1.1 Om OptoNova AB

OptoNova AB är ett företag verksamt inom verkstads-, trävaru- och förpackningsindustrin, där de utvecklar produkter för automatisk avsyning. Kunderna finns både inom Sverige och i utlandet. Några exempel är Pergo, en laminatgolvstillverkare i Europa och USA, samt olika leverantörer till IKEA. Verksamheten började som en industriell avdelning på Hasselblad Engineering AB, men har sedan dess ökat i storlek och är nu ett eget företag med kontor i Solna utanför Stockholm. Där utförs teoretiska beräkningar i optik, numeriska metoder, bildanalys och mekanikkonstruktion som ett led i underhållet av befintliga och framtagandet av nya produkter. Här bedrivs även konsultverksamhet där företagets tekniska kompetens hyrs ut, samt service och installationer. Totalt har OptoNova ca 30 anställda.

1.2 Syfte

På grund av företagets kraftiga expansion de senaste åren har kraven på nätverket på huvudkontoret förändrats. Syftet med detta examensarbete är att analysera nätverket så att brister inom såväl säkerhet som prestanda och användbarhet kan pekas ut. Med analysen som bakgrund ska förslag presenteras på hur en omorganisation kan ske så att nätverket blir bättre anpassat till företagets storlek, möter kraven på säkerhet som företaget självt och dess kunder ställer samt ger högre prestanda och användbarhet.

1.3 Metod

För att analysera det befintliga nätverket har en serie intervjuer genomförts. Bl.a. har s.k. expertintervjuer med ansvariga för IT-verksamheten hållits, där fokus legat på administration av nätverket. I intervjuer med användarna har fokus legat på användbarheten. Detta har skett dels i mer strukturerade intervjuer med förberedda frågor, dels i lösare konversationer. Utöver detta har personliga erfarenheter från en deltidsanställning som IT-tekniker vid företaget i fråga kunnat utnyttjas. I arbetet med att formulera förslagen har bl.a. ett studiebesök gjorts hos ett företag i ungefär samma storlek. Där fördes en dialog med den ansvarige för IT-driften, med fokus på hur liknande problem lösts där. Där fanns erfarenhet av åtgärder som varit lyckade och inneburit förbättringar, men även mindre lyckade sådana. På OptoNova har fortsatta intervjuer och diskussioner med de anställda hållits i samma stil som under analysen, där förslag till lösningar diskuterats och analyserats.

Förslagen har framför allt grundat sig på erfarenheter från studiebesöket samt kurser i bl.a. människa-datorinteraktion, och sedan växt fram i samråd med användarna. Mot slutet av arbetet presenterades både analysen av nätverket och de föreslagna förbättringarna för företaget i samband med ett seminarium om IT-säkerhet. Närvarande fanns både användare av nätverket och ledning på företaget, och det var ett sätt för alla att få en helhetsuppfattning av det som tagits upp tidigare i mer lösryckta sammanhang, och att få komma med synpunkter på förslagen.

2 Nätverket idag

2.1 Allmänt om nätverket

En Internetanslutning på 8 Mbit/s levereras via ADSL till ett modem på kontoret, som tilldelas ett IP dynamiskt. Modemet kommunicerar med en NAT-router som fördelar uppkopplingen på ett antal switchar. Switcharna är kopplade till en patchpanel som i sin tur ansluter till varje dator på nätverket. Routern används som brandvägg samt DHCP-server, och antivirusprogramvara är installerad på varje enskild dator. På nätverket står en Linux-server kallad Smyger. Smyger är en filserver (Samba) som också kör en DNS- (BIND), en versionshanterings- (SVN), en VPN- (OpenVPN) och en webbserver (Apache). På filservern ligger alla gemensamma dokument och filer, och varje dag säkerhetskopieras detta till en USB-ansluten hårddisk. På webbservern körs företagets interna hemsida, och DNSen används för att ge den ett namn. VPN-servern används för att tillåta anställda ansluta till det interna nätverket utifrån, t.ex. hemifrån eller när de är på resande fot.

2.2 Användbarhet

Efter diskussioner och intervjuer med de anställda på OptoNova har det kommit fram att det finns flera irritationsmoment i nuvarande implementation. T.ex. verkar VPNet inte fungera optimalt. Kanske uppstår det kompatiblitetsproblem när VPN-servern körs i Linux, och klienterna körs i Windows. Många användare upplever i alla fall problem med anslutningen, exempelvis kan vissa inte ansluta alls, och andra kan ansluta men får problem med sin Internetuppkoppling då en VPN-anslutning är aktiv.

En annan sak som poängterats är att strukturen på filservern är dålig. Det saknas en intuitiv känsla för var man kan hitta det man letar efter eftersom samma mappnamn används på flera ställen. T.ex. återfinns katalogen Dator och underkatalogen Admin både under katalogen OptoNova och under

katalogen Gungfly. Vad som är tänkt ska ligga under OptoNova respektive Gungfly är oklart för de flesta.

Väldigt många upplever problem med skrivarna. Varje skrivare har sin egen speciallösning för att bli tillgänglig som nätverksskrivare, vilket resulterar i omständliga installationsprocedurer. Dessutom krånglar de ofta, vägrar skriva ut eller skriver ut fel saker. Windows delar automatiskt ut alla skrivare, och installerar automatiskt andras utdelade skrivare. Det resulterar i värsta fall att man får runt 20-30 installationer av samma skrivare, fast genom olika datorer.

Det finns ett antal trådlösa routrar på kontoret som har införskaffats när någon haft ett behov av att kunna ansluta till nätverket trådlöst. Varje nätverk har sina egna inställningar, och det saknas dokumentation över var dessa nätverk finns och hur man ansluter till dem. Detta gör det svårt för någon annan än den som själv satt upp nätverket att ansluta.

Sammanfattningsvis kan man dock säga att trots en decentraliserad, komplicerad styrning som hindrar både administratörer och användare så verkar användarna vara ganska nöjda med strukturen överlag. Det dagliga arbetet innebär inga större problem, det är när något utöver det vanliga ska göras som problem kan uppstå.

2.3 Prestanda

Ett problem med den struktur på nätverket som används i nuläget är att switcharna är underdimensionerade. Det är switchar vars maxkapacitet ligger för nära hastigheten som tas ut i varje uttag, vilket betyder att den nås väldigt snabbt. Om flera användare utnyttjar mycket bandbredd samtidigt uppstår följaktligen en kamp, och om en ny användare då vill ut på nätverket blir det svårt att få bandbredd. Det borde inte innebära några större problem i dagsläget eftersom det sällan är någon stor belastning på nätverket. Å andra sidan klagar vissa på att nätverket på kontoret stundtals känns långsamt, innebärande att det tar lång tid att öppna dokument eller kopiera filer som ligger utdelade. Detta kan mycket väl bero på denna principiellt felaktiga struktur. Ska en omorganisation göras blir det svårt att motivera att detta inte ska ändras. Vidare är det CIDR-block som DHCP-servern administrerar (102.180.45.0/24) inte reserverat för LAN. För att undvika risken att en dator på Internet inte kan kommas åt p.g.a. att den har en adress tillhörande det blocket bör detta bytas. I samband med detta byte bör även inställningarna för VPNet ändras. I dagsläget hamnar de i blocket 10.9.0.0/16, och kan därifrån inte ta del av andra delade resurser än de från filservern Smyger.

Även den externa anslutningen kan förbättras. I värsta fall trängs runt 25 personer på en ADSL-uppkoppling med upp till 8 Mbit/s, och utan effektivis-

eringar kan det lätt bli för långsamt. Detta samt behovet av en FTP-server motiverar ett byte till en mer stabil uppkoppling. Den senare behövs så att kunder kan ansluta och få tillgång till filer som är för stora för att skicka via email.

2.4 Säkerhetsaspekter

Säkerhetsmässigt finns det mycket att anmärka på i nätverket idag. Trådlösa nätverk med enbart WEP-kryptering är en sak, dåliga eller ibland rent av obefintliga lösenord på de anställdas datorer en annan. Det trådlösa nätverket i kombination med att säkerhetsuppdateringar inte installeras tillräckligt ofta gör de anställdas datorer till en stor brist i säkerheten på företaget. Även säkerheten på servern Smyger är under all kritik. Man kan logga in från Internet med administratörsrättigheter, och även det lösenordet är av dålig standard. Detsamma gäller VPN-lösenordet eftersom det delas av alla som ansluter sig via VPN. Det betyder dels att man inte kan ge olika användare olika behörighet, dels att man inte kan stänga av endast ett konto om någon slutar. Alla som har fysisk tillgång till nätverket får också obegränsad tillgång till allt som delas ut på Smyger, eftersom inga användarkonton används som kan kontrollera vem som tar del av vad. Detta innefattar alltså också de som lyckas bryta sig in via det trådlösa nätverket eller VPNet. Att det står en dator med Windows 98 på nätverket förvärrar läget ytterligare, eftersom Microsoft inte längre ger ut några säkerhetsuppdateringar till det operativsystemet.

Eftersom dagens router är en så kallad SOHO-router (Small Office / Home Office) är den dimensionerad för ett fåtal datorer och inte alls den mängd trafik som företaget genererar. En sådan router erbjuder heller inte speciellt många eller avancerade konfigureringar, och även om dagens router kanske håller eventuella hackare borta för tillfället ställs det sådana krav på säkerhet från kunder vars data hanteras av OptoNova att det är högst tveksamt om dessa kan uppfyllas utan en mer avancerad router.

Det sker ingen säkerhetskopiering på mail, så om en anställds hårddisk skulle gå sönder går alla mail han/hon hämtat från webbhotellet förlorade. Utöver det är anslutningen till webbhotellet okrypterad, så användarnamn och lösenord skickas i ren text när man skickar och hämtar mail, liksom själva mailen. Det innebär att en s.k. man in the middle, d.v.s. en person som kan lyssna på trafiken till och från kontoret, inte bara skulle kunna läsa alla mail utan även få kontroll över alla konton.

3 Lösningarna

Det finns många sätt att lösa de problem som finns på OptoNovas nätverk, och detta examensarbete kommer presentera två förslag på strukturer för ett nytt nätverk. Det ena bevarar mycket av nuvarande organisation och minimerar utgifterna, medan den andra kostar mer men är tänkt att vara effektivare och lösa problemen mer fullständigt, samt att utgöra en bättre grund för utveckling.

3.1 Förslag 1

Följande struktur är utformad för att lösa de mest kritiska bristerna i dagens nätverk, utan att innebära alltför stora kostnader.

3.1.1 Förslag på ändringar

För att kunna möta dagens och framtidens krav ska dagens Internetuppkoppling uppgraderas till att ha en statisk IP-adress istället för dynamisk. Detta kommer att underlätta t.ex. när levererade system ska fjärrstyras från OptoNovas kontor i Solna, eftersom man då kan veta från vilken IP-adress styrningen kommer att ske.

Oavsett om anslutningen förbättras genom en uppgradering eller inte så ska åtminstone utnyttjandet av bandbredden effektiviseras. En proxy-server används bl.a. för att undvika upprepade hämtningar av samma data, och kan med fördel placeras på kontoret. Denna börda läggs på Smyger, en lösning som inte kostar något extra. Detta i kombination med en mailserver gör att man kan reducera den mängd data som måste skickas via Internet avsevärt. I dagsläget går nämligen all mailtrafik via företagets webbhotell, och med tanke på att en stor del av alla mail skickas till någon på kontoret kan större delen av mailtrafiken undvikas. I övrigt betyder det också att de anställdas email lättare kan säkerhetskopieras eftersom de lagras lokalt på kontoret, och ett webbaserat gränssnitt skulle innehålla alla mail, istället för bara de som ännu inte hämtats med en mailklient som i dagsläget.

Adressblocket för intranätet ska bytas från 102.180.45.0/24 till det för LAN reserverade blocket 192.168.1.0/24 och samtidigt byts blocket för VPN-klienter till 192.168.2.0/24. Om routern då administrerar 192.168.0.0/22 kan man fortfarande lätt se vilken dator som fysiskt befinner sig på kontoret och vilken som är ansluten via VPN, samtidigt som VPN-klienter kan ta del av alla delade resurser eftersom de befinner sig i samma subnät.

Dagens switchar avvecklas, och en 48-portars switch med högre maxkapacitet tar över. Varje klient ska dock fortfarande bara kunna få ut 100

Mbit/s för att undvika att samma problem uppstår igen, fast vid högre hastighet. Samtidigt ska de trådlösa routrar som finns bytas ut mot renodlade accesspunkter med WPA2-kryptering, och tillräckligt många nya ska köpas in för att dessa ska kunna samverka och bilda ett homogent trådlöst nätverk på kontoret.

Det ska inte gå att logga in som administratör på någon Linux-server från Internet. De personer som har behov av att fjärransluta via SSH ska ha ett användarkonto på servern ifråga.

Datorn med Windows 98 ska genast kopplas bort från nätverket. Den anställda som använt den datorn får en ny med Windows XP, och får använda den gamla datorn vid behov, och utan nätverksanslutning.

Det öppna kontot i VPN som alla har tillgång till, och som inte har några begränsningar, ska stängas av. Istället ska varje anställd ha ett personligt konto, i vilket eventuella begränsningar kan specifiseras.

Alla anställda ska informeras om hur viktigt det är med antivirusprogram, säkerhetsuppdateringar och bra lösenord för säkerheten på företaget. Detta ska förhoppningsvis leda till att alla använder uppdaterade antivirusprogram, att kvaliteten på lösenorden höjs, och att alla använder sig av automatiska uppdateringar. Viktigt är också att detta kommer att gälla även på nya datorer som köps in.

För att förhindra att hårdvara blir skadat vid strömavbrott ska en UPS köpas in. Det kommer också att förbättra upptiden för mailservern, något som är viktigt om företaget ska hantera mailtrafiken själva.

För att installation och övervakning av skrivarna ska bli enklare föreslås att alla skrivare installeras på en server, t.ex. mailservern eller Smyger, och sedan delas ut därifrån. Det skulle innebära att installationer av skrivare kan ske på ett standardiserat sätt, skrivarkön blir gemensam för alla datorer på nätverket och mindre risk för problem när två datorer försöker skriva ut samtidigt.

3.1.2 Sammanfattning

Sammanfattningsvis bör alltså följande ändringar genomföras:

1. Uppgradera till statisk IP-adress.
2. Placera en proxy-server på kontoret.
3. Placera en mailserver på kontoret.
4. Byt CIDR-block till 192.168.0.0/22.
5. Byt ut switcharna mot en på 1 Gb/s.

6. Byt ut trådlösa routrar mot APer med WAP2.
7. Stäng av möjligheten att logga in som administratör via SSH.
8. Koppla bort datorn med Windows 98 från nätverket.
9. Skapa användarkonton i VPN för varje anställd.
10. Informera anställda om vikten av bra lösenord.
11. Införskaffa en UPS och sätt i drift.
12. Installera alla skrivare genom en skrivarserver.

3.1.3 Nackdelar

Att genomföra ovanstående ändringar ska förhoppningsvis leda till ett bättre nätverk, men fördelarna måste vägas mot nackdelarna. Till att börja med är förslaget utformat för kosta så lite som möjligt, men det går inte att komma ifrån att det ändå kommer innebära en hel del investeringar. T.ex. behöver flera datorer köpas in, och månadskostnaden för Internetanslutningen kommer öka drastiskt.

De besparingar som ändå gjorts leder till lösningar som inte är riktigt fullständiga. Att t.ex. placera en mailserver på intranätet är att kompromissa på säkerheten, eftersom den måste kunna kommas åt från Internet när mail ska skickas till kontoret. En dator som exponeras på Internet kan bli målet för en attack från hackare, och eftersom SMTP-protokollet har så många brister blir det relativt lätt för en obehörig person att ta sig in på mailservern, och därmed även intranätet.

Andra lösningar kanske inkräktar på de anställdas arbetssätt. Om varje anställd ska ha ett eget konto i VPN innebär det att alla måste hålla reda på ännu fler inloggningsuppgifter, och om lösenorden på datorerna ska göras svårare att knäcka blir de också svårare att komma ihåg. I dagsläget behöver de anställda oftast inte gå så långt för att komma in på en dator när behov uppstår, även om de är långt från sin arbetsplats, eftersom lösenorden ofta följer en standardmall. Dessutom är det mycket svårt att kontrollera att en sådan policy verkligen efterlevs.

3.2 Förslag 2

Denna struktur syftar till att mer fullständigt lösa dagens problem, samt att förbereda för andra och större krav i framtiden. Det ska förhoppningsvis motivera den förhållandevis stora kostnad en implementation innebär.

3.2.1 Förslag på ändringar

På många sätt kan man se detta förslag som en vidareutveckling av förslagen i föregående sektion. Därför ska de flesta ändringar därifrån genomföras även här med liten eller ingen justering, och motivationen till att en ändring behövs är densamma. Av de föreslagna ändringarna i föregående sektion ska nummer 4, 5, 7, 8 och 11 genomföras utan modifiering; d.v.s. byt CIDR-block, byt switchar, omöjliggör administratörsinloggning via SSH, koppla bort Windows 98-datorn från nätverket och skaffa UPS. De kvarvarande ändringarna ska antingen genomföras med modifiering, eller så löses problemen på annat sätt.

Dock ska två saker göras utöver detta. För det första ska Smyger, som är en ganska gammal dator, avvecklas. En ny, kraftfull server med Microsoft Windows Small Business Server (SBS) sätts in i dess ställe. SBS är ett paket för företag med upp till 75 datorer som innehåller operativsystemet Windows Server 2003 och mailservern Microsoft Exchange Server. Denna dator ska vara filserver, skrivarserver, SVN-server, DNS-server, DHCP-server, webbserver, och VPN-server. Alternativt kan vissa av dessa tjänster, som DNS, webbserver och SVN köras på en Linux-dator för att avlasta servern lite, men det borde inte behövas om man bara ser till att dimensionera servern för att klara hög belastning.

För det andra ska dagens router bytas ut mot en Linux-server, som förutom att utföra routning också ska agera proxy-server. Denna utrustas med flera nätverkskort som representerar olika zoner, och sedan sätts regler för hur trafik mellan de olika zonerna ska tillåtas. T.ex. ska ett kort kopplas till ADSL-modemet, och således bli en zon som innehåller hela Internet. Trafik från denna zon till de andra zonerna ska vara hårt kontrollerat, eftersom det i denna zon finns hackare, elak kod och dylikt som inte ska få släppas in.

Ett annat kort ska kopplas till företagets intranät, d.v.s. nätverket med alla trådbundna datorer. Från denna zon ska trafik till alla andra zoner tillåtas, eftersom det bara finns tillförlitliga användare där. Däremot skulle det kunna finnas elak kod på någon dator, och därför är uppdaterad antivirusprogramvara på alla företagets datorer nödvändigt för att minska denna risk.

Ett tredje kort ska vara en s.k. demilitarized zone (DMZ), vilket innebär att brandväggen inte kontrollerar trafiken till denna zon, inte ens trafik från Internet. I gengäld finns ingen möjlighet att ansluta till något annat än Internet från ett DMZ. I denna zon ska datorer placeras som kör känsliga tjänster, som t.ex. en FTP-server och ett mailrelay.

Till sist ska ett fjärde kort användas för det trådlösa nätverket. Denna zon är inte garanterad att innehålla bara tillförlitliga användare, och därför tillåts trafik till Internet, men inte till intranätet. För att komma åt intranätet används det VPN som alla fjärranvändare ansluter till. Frånvaron av garanti

beror på att det är möjligt att bryta sig in i ett trådlöst nätverk, om man befinner sig i närheten och är tålmodig. Alla som har ett trådlöst nätverkskort kan nämligen ta emot det data som skickas från och till en trådlös klient på nätverket. Har en illasinnad person lyssnat tillräckligt länge på den trådlösa trafiken, två minuter räcker för ett WEP-krypterat nätverk, kan krypteringen knäckas med rätt program och personen kommer in. Har man då lagt det trådlösa nätverket i en zon som inte tillåts komma åt annat än Internet har hackaren i princip inte kommit närmare intranätet än om han/hon försökt ansluta via Internet. Skillnaden är att han/hon befinner sig i samma zon som alla trådlösa klienter, som då kommer vara mer exponerade för en attack. Det är därför extra viktigt att trådlösa klienter har bra virusskydd och brandvägg, samt att alla tillgängliga säkerhetsuppdateringar är installerade. Precis som i föregående sektion ska nätverket utökas så att hela kontoret täcks av ett homogent trådlöst nätverk, med bara renodlade accesspunkter med WAP2-kryptering.

Samtliga nätverkskort ska ha en kapacitet på 1 Gb/s för att ha rum för framtida uppgraderingar. Detta trots att t.ex. kortet kopplat till ADSL-modemet i dagsläget inte behöver ha en högre kapacitet än 10 Mb/s.

En fiberanslutning istället för ADSL medför alla fördelar med att uppgradera till statiskt IP, men även en förbättring av tillförlitligheten på uppkopplingen. Detta eftersom fiberanslutningar mycket mer sällan har avbrott i tjänsten, och inte störs av trafik på telefonnätet, som t.ex. fax och telefoni. Det, i samband med de mycket högre hastigheter som går att få med fiberanslutningar, framförallt på utgående trafik, skulle innebära en klar förbättring både för användare på kontoret och för folk som utifrån använder tjänster på kontoret som VPN och FTP.

Mailservern som placerades på nätverket i föregående förslag finns även här, i och med att Microsoft Exchange Server ingår i SBS. För att öka säkerheten kombineras den med ett mailrelay. Ett mailrelay fungerar som en mellanhand mellan Internet och en mailserver. När mail ska skickas till kontoret tas de emot av relayet, och mailservern kan sedan hämta mailen från relayet utan att ha behövt kommunicera med någon över en osäker anslutning. I relayet kan man också köra anti-spam-mjukvara som sorterar ut skräppost innan de hamnar hos användarna. Även när mail ska skickas från kontoret går de genom relayet, ännu en gång för att undvika att mailservern behöver exponera sig på Internet. Här behöver dock relayet konfigureras så att enbart mail som kommer från kontoret får gå genom det, annars kan det användas för att skicka spam-mail vilket i slutänden kommer resultera i att andra mailservrar kommer vägra att ta emot mail från relayet. Sammanfattningsvis ska mailrelayet användas för att sortera bort spam och elak kod, och för att slippa tillåta trafik via det osäkra SMTP-protokollet till en dator

på intranätet. Därför ska relayet vara en Linux-server, eftersom det knappt existerar virus till Linux, och den ska placeras i DMZat där det inte gör lika mycket om någon bryter sig in. Ett webbaserat gränssnitt ska köras på Small Business-servern, och där kan kryptering användas eftersom alla moderna webbläsare har stöd för krypterade hemsidor. På detta sätt minimerar man riskerna med att hantera mailtrafik.

I SBS talar man om Active Directory (AD), Microsofts implementation av LDAP. AD är en databas som innehåller information om olika användarkonton och olika resurser, så som skrivare och filer och mappar på en filserver. En domän är ett antal datorer som delar den databasen, och en domänkontroller administrerar databasen och tillgången till domänen. Så som förslaget är tänkt ska datorn med SBS vara domänkontroller, och tillgång till domänen ska endast ges genom ett användarkonto i ADt. Dessa användarkonton är kopplade till konton på de anställdas datorer, så för att en anställd ska kunna ansluta sig till domänen med sitt Windows-konto måste ett motsvarande konto finnas i ADt. När en användare väl autentiserat sig hos domänkontrollern kontrollerar denna att datorn som används uppfyller vissa krav som definierats i s.k. grupprinciper, Group Policies (GP). Dessa GPer anges av systemadministratören, och kan t.ex. vara att kontots lösenord håller tillräcklig hög kvalitet. Om så inte är fallet vidtas någon åtgärd för att ändra på detta. I detta exempel får användaren helt enkelt en dialogruta där han/hon kan ändra lösenordet. Andra GPer som ska definieras är att uppdateringar ska hämtas och installeras automatiskt och att antivirusprogramvara måste vara installerad och uppdaterad. Dessutom kan GPer användas till att automatisera installationen av skrivare och andra inställningar som delas av alla i domänen. Användare kan tillåtas logga in från vilken dator som helst som ingår i domänen, och till och med fjärransluta via VPN, allt med sitt personliga konto eftersom tillgång till domänen är kopplat till användarkontot och inte en specifik dator. Av den anlednigen behöver heller inte VPNet konfigureras med separata konton, eftersom de redan finns på servern.

I domänkontrollern specificeras också vilka resurser som är tillgängliga för vilka konton, så att t.ex. filer tillhörande ett visst projekt bara kan läsas av behöriga personer i det projektet. Detta öppnar också för användarutrymmen på filservern, d.v.s. mappar på filservern som är kopplade till användarkonton, och bara kan läsas av dem. Filerna i dessa mappar kan användarna m.a.o. komma åt oavsett från vilken dator de ansluter till domänen, utan att för den sakens skull riskera att någon obehörig kan läsa dem. Slutligen kan domänkontrollern även inkludera de anställdas datorer i säkerhetskopieringen som utförs dagligen. Detta i kombination med användarutrymmen på filservern innebär en större säkerhet för användarnas filer.

3.2.2 Sammanfattning

För att sammanfatta ska alltså två helt nya saker genomföras jämfört med första förslaget.

1. Byt ut Smyger mot en modernare server med SBS.
2. Byt ut routern mot en Linux-server med flera zoner.

De nya servrarna möjliggör fler ändringar.

1. Automatisera installationen av skrivare.
2. Tvinga fram användandet av antivirusprogram.
3. Skapa användarutrymmen på filservern.
4. Säkerhetskopiera de anställdas filer.
5. Skapa ett DMZ med en FTP-server och ett mailrelay.
6. Sortera ut spam och elak kod i DMZat.

De ändringar som rekommenderas i första förslaget genomförs med eller utan modifieringar.

1. Uppgradera till fiberanslutning (med statisk IP-adress).
2. Låt nya routern också vara proxy-server.
3. Låt Small Business-servern också vara mailserver.
4. Byt CIDR-block till 192.168.0.0/22.
5. Byt ut switcharna mot en på 1 Gb/s.
6. Kör trådlösa nätverket i en egen zon med WAP2.
7. Stäng av möjligheten att logga in som administratör via SSH.
8. Koppla bort datorn med Windows 98 från nätverket.
9. Koppla inloggning via VPN till konton i ADt.
10. Tvinga fram uppdateringar och bra lösenord m.h.a. GPer.
11. Införskaffa en UPS och sätt i drift.
12. Automatisera skrivarinstallationer med GPer.

3.2.3 Nackdelar

Jämfört med första förslaget är detta förslag dyrt och tidsödande att implementera. Utöver det löper en server med SBS större risk att bli smittad av elak kod än en Linux-server som Smyger. Detta eftersom det är mer lockande att hitta säkerhetshål i SBS då det används på många fler servrar än Linux. Detta förslag leder överhuvudtaget till mer komplicerade lösningar där förhoppningen är att de flesta mindre fel och brister ska kunna undvikas. Det betyder dock också att när något väl går fel är risken stor att det är mer komplicerat att lösa problemet. Om Linux-routern kraschar innebär det t.ex. mycket mer arbete att få igång den än att starta om en krånglande SOHO-router.

Mycket i förslaget är menat för att öka säkerheten på företaget, men att uppgradera anslutningen kan faktiskt öka risken för intrång. Stabila och snabba uppkopplingar kan dra till sig illasinnade personer som letar efter bra datorer att sprida elak kod från, eller att lagra olagligt material på.

4 Diskussion

Det har framkommit att det finns många problem med hur nätverket ser ut på OptoNova idag, både ur användbarhets- och säkerhetssynpunkt. Två förslag har presenterats här för att lösa dessa problem. Fördelen med första alternativet är att kostnaden och tidsåtgången är relativt låg. Uppskattningsvis skulle det i skrivande stund kunna implementeras för runt 20 000 kronor i rena materialkostnader, och göras på ungefär fyra veckor. Nackdelen är att problemen inte är lösta fullständigt, och administrationen av företagets datorer är decentraliserad. T.ex. skulle ett byte av en skrivare innebära att alla datorer måste konfigureras om individuellt. Dessutom går det inte på något vis att kontrollera att t.ex. lösenordspolicyn verkligen efterlevs. Förslaget är rimligt att genomföra därför att de flesta av ändringarna verkligen behövs göras. Alternativet att inte göra något kan innebära enorma kostnader. Vad skulle det kosta att förlora en kund för att man inte kan uppfylla kraven på säkerhet, och vad kostar det om företagshemligheter läcker ut?

Det andra alternativet innebär en centralisering av administrationen, vilket i slutänden bör löna sig för både administratörer och användare. Nackdelen är att det innebär en mycket högre kostnad. Bara programvaran för SBS är i skrivande stund runt 40000 kr räknat på 50 användarkonton. Att bara genomföra ändringarna i första förslaget kan dock ses som en alltför kortsiktig lösning. Inom relativt kort tid kommer man kanske sitta i samma sits igen - att ändringar måste göras för att inte riskera förluster p.g.a. att säkerheten

eller prestandan på nätverk och servrar inte är tillräckligt hög. Det andra förslaget löser dels dagens problem på ett mer fullständigt vis, och öppnar samtidigt med sin expanderbarhet för att nya krav i framtiden kan mötas utan att alltför stora omorganisationer behöver genomföras.

Det finns två problem som togs upp i beskrivningen av nätverket som inte fått någon lösning presenterad i något av förslagen. Det är den krånglande VPN-anslutningen och den förvirrande strukturen på filservern Smyger. VPN-problemet, till att börja med, har inte fått någon lösning presenterad för att det inom examensarbetets ramar inte går att specificera exakt vad som är problemet. Mjukvaran som används är rätt konfigurerad, och alla nätverksinställningar är korrekta. Det borde med andra ord inte vara några problem, och därför finns det ingen garanti för att det kommer fungera om t.ex. VPN-mjukvaran byts ut. Att göra om strukturen på filservern faller heller inte inom arbetets ramar, då framtagandet av en bra struktur är en omfattande process som skulle behöva innehålla moment som framtagande av prototyper som de anställda får prova och ge feedback på och genomgång av allt tillgängligt material. Därför har dessa två problem utelämnats ur förslagen, men om en SBS införskaffas finns ett gyllene tillfälle att prova ny VPN-mjukvara samt att göra om strukturen då man ändå gör en migrering från Smyger. Utöver detta har inte riskerna med fysisk tillgång till datorer eller flyttbar lagringsmedia diskuterats i större mån än att lösenorden kritiserats. Detta trots att s.k. social engineering blivit ett allt större säkerhetshot, och en analys av säkerhetsläget på ett företag knappast kan anses vara komplett utan att ha behandlat detta.

A Ordlista

AD *Active Directory* Microsofts implementation av LDAP.

ADSL *Assymetric Digital Subscriber Line* Ett sätt att leverera Internetanslutningar via det fasta telefonnätet.

AP *Access Point* Accesspunkt på svenska. En enhet vars uppgift är att förbinda trådlösa klienter med ett nätverk. En renodlad accesspunkt är som en trådlös switch, medan en trådlös router har routing-funktioner.

CIDR *Classless Inter-Domain Routing* En (gällande) standard för hur IP-adresser ska skrivas och tolkas som ska underlätta vid routning på Internet. En (version 4) IP-adress representeras oftast i dot-decimalnotering, 192.168.1.1 exempelvis. Denna adress består av två delar; nätverksadress och värdadress. Nätverksadressen identifierar ett specifikt nätverk eller subnät, ett s.k. CIDR-block. Värdadressen identifierar en specifik maskin i det nätverket. Hur stor del av IP-adressen som är nätverksadress och hur stor som är värdadress specificeras i en subnätmask som skrivs på liknande vis som en IP-adress. Man kan också identifiera ett CIDR-block genom att ange den lägsta IP-adressen i blocket följt av ett snedstreck och ett tal. Talet ska tala om hur många bitar i den 32 bitar långa adressen som hör till nätverksadressen. T.ex. specificerar 192.168.1.0/29 ett block innehållande adresserna 192.168.1.0 - 192.168.1.7.

DHCP *Dynamic Host Configuration Protocol* Ett protokoll för att dynamiskt tilldela bl.a. IP-adresser över ett nätverk.

DNS *Domain Name System* Ett system som förenklar adressering på ett nätverk. Istället för att använda en dators IP-adress kan man använda dess domännamn, t.ex. www.optonova.se. En DNS-server, även kallad namnserver, håller reda på vilket domännamn som ska kopplas till vilken IP-adress.

Elak kod Även **skadlig kod**, eller **malware** på engelska. Samlingsnamn för olika former av skadliga datorprogram, som t. ex. virus, maskar, och trojanska hästar.

LDAP *Lightweight Directory Access Protocol* Ett protokoll för att kommunicera med katalogtjänster. Katalogtjänster hanterar bl.a. information om ett nätverks användare och resurser.

NAT *Network Adress Translation* Ett sätt att dölja flera datorer bakom en publik IP-adress. Anslutningar till den publika IP-adressen på en viss port översätts till anslutningar till en specifik port på en av de gömda datorerna, och vice versa.

WEP *Wired Equivalent Privacy* Den första generationen av kryptering för trådlös trafik. Numera gammalmodig och lätt att knäcka.

WPA *Wi-Fi Protected Access* Den andra generationen av kryptering för trådlös trafik. Även om det är möjligt att knäcka en WPA-kryptering är det mycket svårare än med WEP. Uppföljaren WPA2 använder sig av den AES-baserade CCMP-algoritmen som anses vara mycket säker.

B Intervjumall

Under analysfasen låg följande frågor som grund för intervjuer med anställda på företaget. Dessa intervjuer genomfördes som diskussioner kring frågorna, snarare än direkta utfrågningar.

1. Vad är din sammantagna inställning till företagets nätverk?
2. Hur pass lätt är det att lära sig att använda nätverket?
3. Känner du att du har kontrollen då du arbetar mot nätverket?
4. Finns det något som fungerar särskilt väl?
5. Finns det något som fungerar särskilt dåligt?
6. Finns det något som krånglar särskilt mycket?
7. Saknas det någonting specifikt, vad gäller funktionalitet?
8. Finns det någon specifik funktion som är överflödig, eller till och med gör nätverket sämre?