

Författare: Anders Berndt
Handledare: Stefan Hansson
LIA-företag: WM-data IT-support

Studie av säkerhetsarbete

En jämförelse av praktiskt IT-säkerhetsarbete kontra teoretiskt
i form av en säkerhetsanalys utförd hos Konstblomman AB,
med efterföljande reflektion över gjorda erfarenheter.

Innehållsförteckning

1	Förord	3
2	Sammanfattning	3
3	Inledning	4
4	Syfte	4
5	Frågeställning	4
6	Metod	5
7	Begränsning	5
8	Resultat	5
8.1	Förarbete	5
8.2	Analys	6
8.2.1	Active Directory	6
8.2.2	Brandväggar	8
8.2.3	Intrångsdetektering	11
8.2.4	Fjärranslutning	11
8.2.5	Logghantering	12
8.2.6	Uppdateringar	12
8.2.7	Backup – Redundans – UPS	12
8.2.8	Virussydd	13
8.2.9	Fysiska risker	14
8.2.10	Kryptering	14
8.2.11	Server	15
8.2.12	Klient	15
8.2.13	Nätverksutrustning	15
8.2.14	Teknisk dokumentation	16
8.2.15	Topologi	16
8.2.16	Säkerhetspolicy	18
8.2.17	Tillgångar och klassificering	18
8.2.18	Personal och säkerhet	18
8.2.19	Risikanalys och katastrofberedskap	18
9	Åtgärdsförslag	19
10	Slutsats	22
11	Källförteckning	23
12	Bilagor	23

Förord

Innan jag ger mig in i examensarbetet vill jag tacka WM-data IT-support i Malmö för att jag fick göra min praktik hos dem, och för att jag fick tillfälle att arbeta så mycket just med säkerhetsbiten. Särskilt tack till Patrik Danielsson, Mats Ekdahl, Anders Söderberg och min handledare Stefan Hansson.

Jag vill också rikta ett tack till Konstblomman AB, som lät mig härja fritt på deras arbetsplats under så lång tid.

Jag passar här också på att nämna att Konstblomman och alla andra namn och IP-nummer som förekommer i arbetet är påhittade.

Sammanfattning

När jag började min praktik på WM-data IT-support och första gången pratade med Stefan Hansson, visade det sig att de ville att jag skulle göra en säkerhetsanalys hos en av deras kunder, Konstblomman AB.

Detta innebar att jag skulle ta fram underlag för att göra en analys, genomföra den, sammanställa resultatet och rekommendera åtgärder för att göra deras IT-miljö säkrare. Tanken var sedan att WM-data skulle ta ställning till vilka tjänster de skulle kunna erbjuda Konstblomman.

Det föll sig naturligt att denna analys också skulle komma att utgöra grunden för mitt examensarbete. Jag ville veta hur det är att arbeta praktiskt med säkerhetsanalys, och jämföra det med vad vi lärt oss under utbildningen. Både WM-data och jag och ville få fram metoder och mallar för hur en säkerhetsanalys kan genomföras, så det förelåg ett ömsesidigt intresse för detta projekt.

Efter ungefär tre månader var jag klar med mitt arbete, och kunde presentera resultatet för min handledare och den tekniker som var huvudansvarig för Konstblommans IT-miljö, och som jag arbetat tillsammans med en del av tiden. Därefter sattes en åtgärdsplan ihop, och arbetet med att säkra Konstblomman kunde fortsätta.

En del av de säkerhetsbrister som tas upp i rapporten blev åtgärdade redan under tiden arbetet med den pågick. Antingen för att det var så enkla saker att det kunde göras i stort sett samtidigt som bristen upptäcktes, eller för att det emellanåt uppstod akuta problem med datordriften. Det viktigaste av det senare var bytet av SMTP-gateway.

Jag gjorde en hel del lärdomar under tiden med arbetet och kunde dra viktiga slutsatser av det. Man måste t ex ha standardfrågor att ställa, men samtidigt vara på det klara med att en del av dem kan komma att gå bort, andra komma till, beroende på vilken miljö det gäller. Dock är det viktigt att alla aspekter på informationssäkerhet är med, att man har helhetssyn på nytta kontra kostnad, och kanske viktigast: att det är kundens upplevelse av IT-säkerhet som gäller.

Inledning

WM-data IT-support har Konstblomman AB som kund. Detta företag sysslar med försäljning av konstgjorda växter för tillverkning av större installationer. De har sina lokaler på ett helt våningsplan i en fastighet i centrala Malmö, där de är ca femton anställda. Dessutom finns lokalkontor i Växjö, Ystad och i Ungern och Rumänien, med ett par anställda på varje ställe.

Konstblomman hade tidigare en anställd tekniker, men sedan drygt ett år är WM-data ansvarigt för IT-miljön på företaget. Vid övertagandet upprättades en mycket begränsad dokumentation, baserad på muntlig redovisning av den avgående teknikern. Denna dokumentation är i stort sett obefintlig när det gäller inventering och beskrivning av IT-miljön. Det har sedan övertagandet inte heller funnits tid eller möjlighet att skapa en ordentlig dokumentation.

Då miljön är väldigt blandad och av skiftande ålder har det hela tiden funnits en oro för säkerheten, både den fysiska (om hårdvaran ska hålla) och den logiska (hur skyddade resurserna är).

Syfte

Syftet med examensarbetet har varit att få rutin på att arbeta skarpt med säkerhetsanalys och att ta fram dokument och mallar att använda i sådant arbete i framtiden, både för mig och för WM-data IT-support.

Frågeställning

När man studerar informationssäkerhet lär man sig bl a hur en komplett säkerhetsanalys bör gestalta sig. Det betonas mycket hur viktigt det är med helhetssyn, att få med alla aspekter – hårda som mjuka, hur säkerhetsarbete och förändring måste genomsyra hela företaget och ha ledningens fulla stöd. ("Datasäkerhet i praktiken", Maiwald, Sieglein, Pagina 2002)

Jag har alltid undrat hur denna ambition står sig gentemot verkligheten, i form av upptagna chefer, begränsad budget och väl uppkörda hjulspår.

- Är frågorna som ställs de rätta?
- Går det att genomföra en "komplett" säkerhetsanalys?
- Påverkas analysarbetet av vad som avslöjas under arbetets gång, d v s håller man sig till frågorna, eller utökas/stryks/revideras de efterhand?
- Påverkas sättet på vilket en säkerhetsanalys genomförs av företagets anda och kultur, eller går det att hålla sig saklig och neutral?

Metod

Examensarbetet utförs genom att först formulera frågor i form av frågeformulär. Därefter söks svaren på frågorna hos företaget, dels genom att studera IT-miljön och dels genom att intervjua personalen. När den undersökningen är klar avser jag att jämföra dess resultat med punkterna i frågeställningen.

Man kan säga att det är en tvåstegsraket: för att få svar på mina frågor måste jag göra en undersökning och ställa andra frågor. Svaren på dem ska ge svaren på de första.

Begränsning

Det faktum att säkerhetsanalysen genomförs på ett relativt litet företag gör att resultatet inte innehåller riktigt alla aspekter som man skulle vilja ha med. Eftersom en säkerhetsanalys dessutom kan göras nästan hur detaljerad som helst har jag begränsat den som jag tycker passar ett företag av Konstblommans storlek.

Resultat

Förarbete

Det finns inom WM-data en avdelning som heter WM-data Security och som arbetar med säkerhetsanalyser, men bara på större kunder. Det saknades med andra ord en motsvarighet i det mindre formatet för WM-data IT-support att erbjuda sina kunder.

ISO17799 är en standard för vad en informationssäkerhetsanalys bör innehålla, och blev därför den naturliga grunden för mitt arbete. ("Handbok i informations-säkerhetsarbete", SIS 2001) Denna är i sin grundform väldigt omfattande och passar inte alls för analys av alla företag, framförallt inte mindre. Den måste alltså krympas och anpassas. En del av arbetet var redan gjort av WM-data Security, och det var deras version som jag satte mig att bearbeta.

Målsättningen blev att ta bort ämnen och frågor som inte kändes relevanta för mindre företag, och att förkorta och förenkla själva frågorna. Det viktiga var att alla aspekter av IT-säkerheten blev kvar, även om många delar togs bort eller gjordes om. Resultatet skulle kunna användas vid både denna och framtida analyser av företag i Konstblommans storlek, så även om det visade sig att alla frågor inte skulle behöva ställas i just detta arbete fick de bli kvar.

Vad jag hade att gå på när jag skulle ta fram analysunderlaget var den lilla information som WM-data hade om Konstblommans IT-miljö. Jag visste ungefär hur många användare det gällde, att det förekom fjärranslutningar, antalet servrar och klientdatorer, att servermiljön var Windows 2000 med Active Directory och att klienterna använde Windows 98, 2000, XP och MS Office. Jag visste också att i stort sett ingenting var dokumenterat.

När denna del av arbetet var klar hade jag fått fram nitton stycken frågeformulär (för exempel, se bilaga 1) som alla behandlade varsin bit av det stora pusslet IT-säkerhet. Dessa bitar, utan inbördes ordning, blev:

1. Active Directory
2. Brandväggar
3. Intrångsdetektering
4. Fjärranslutning
5. Logghantering
6. Uppdateringar
7. Backup – Redundans – UPS
8. Virussydd
9. Fysiska risker
10. Kryptering
11. Server
12. Klient
13. Nätverksutrustning
14. Teknisk dokumentation
15. Topologi
16. Säkerhetspolicy
17. Tillgångar och klassificering
18. Personal och säkerhet
19. Riskanalys och katastrofberedskap

Jag kommer att gå igenom hur säkerhetsanalyset fortskred under dessa nitton rubriker.

Analys

1. Active Directory

För att få en uppfattning av Konstblommans organisation och miljö började jag med att titta på deras katalogtjänst, närmare bestämt Active Directory. Vad jag tittade efter var hur strukturen såg ut, om OU:er var skapade för att spegla företagets utseende och underlätta administration, överhuvudtaget om det var uppsatt utifrån de råd och rekommendationer som finns om hur AD kan och bör utnyttjas på bästa sätt. Inte minst för att få säkerhet i domänen.

Snart gick det att se att detta inte var ett särskilt genomtänkt träd, utan istället installerat med standardinställningar och inte med någon egentlig anpassning till företagets struktur. Det var svårt att överblicka, och i mina ögon i stort behov av att byggas om.

En del ändringar var gjorda, men inkonsekvent och i vissa fall felaktigt. Användarkonton hade direkt behörighet till resurser, GPO:er var satta på fel sätt, gamla konton och testobjekt som inte användes fanns kvar och svaga eller inga lösenord var tillåtna. Alldeles för stora behörigheter gällde på känsliga kataloger, den dominerande inställningen var Full Control för Everyone, och inga säkerhetsgrupper användes för att begränsa behörigheterna.

Det varierade också hur behörigheterna var satta på samma sorts kataloger; ibland som faktiska behörigheter på katalog utan arv uppifrån, ibland som inga behörigheter på katalog utan ärvda uppifrån.

Alla användarkonton var skapade i OU:n Users, där de låg tillsammans med andra objekt: standardanvändare och standardgrupper, diverse testkonton och konton som inte längre användes. Likaså fanns alla klientdatorer i en och samma OU, trots att de fanns på helt olika geografiska platser eller var av olika typ (stationära eller bärbara). Därigenom var ju möjligheterna att t ex utnyttja GPO:er för att styra eventuellt olika säkerhetsnivåer starkt begränsade.

Med andra ord gick det mesta stick i stäv med gällande rekommendationer om hur man ska utnyttja AD för att underlätta sin administration. Trots detta fungerade det hela hjälpligt, men det berodde på att det ju var ett förhållandevis litet träd att hålla reda på. Om företaget växte skulle det hela förr eller senare bli ohållbart.

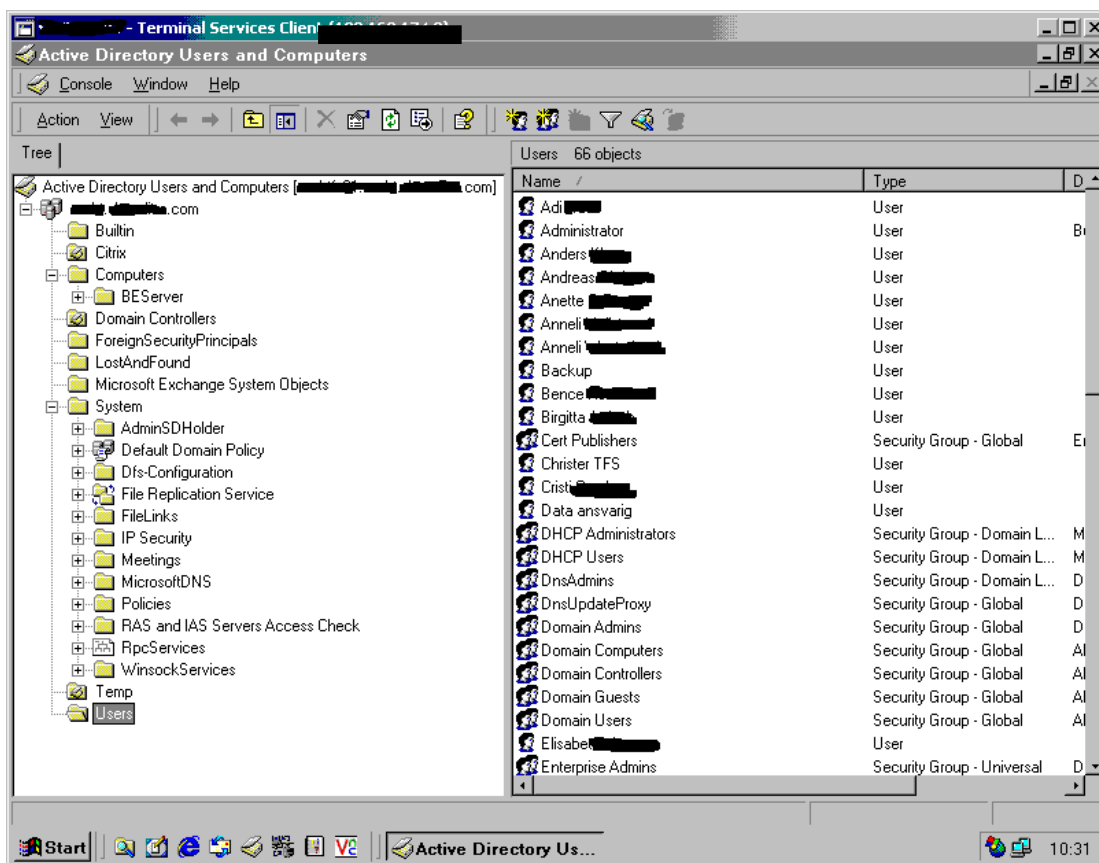


Bild 1: Konstblommans katalogstruktur i Active Directory. Den öppna katalogen Users innehåller alla användare och grupper. I fältet Description i högerkanten står bl a vissa användarkontons lösenord i klartext.

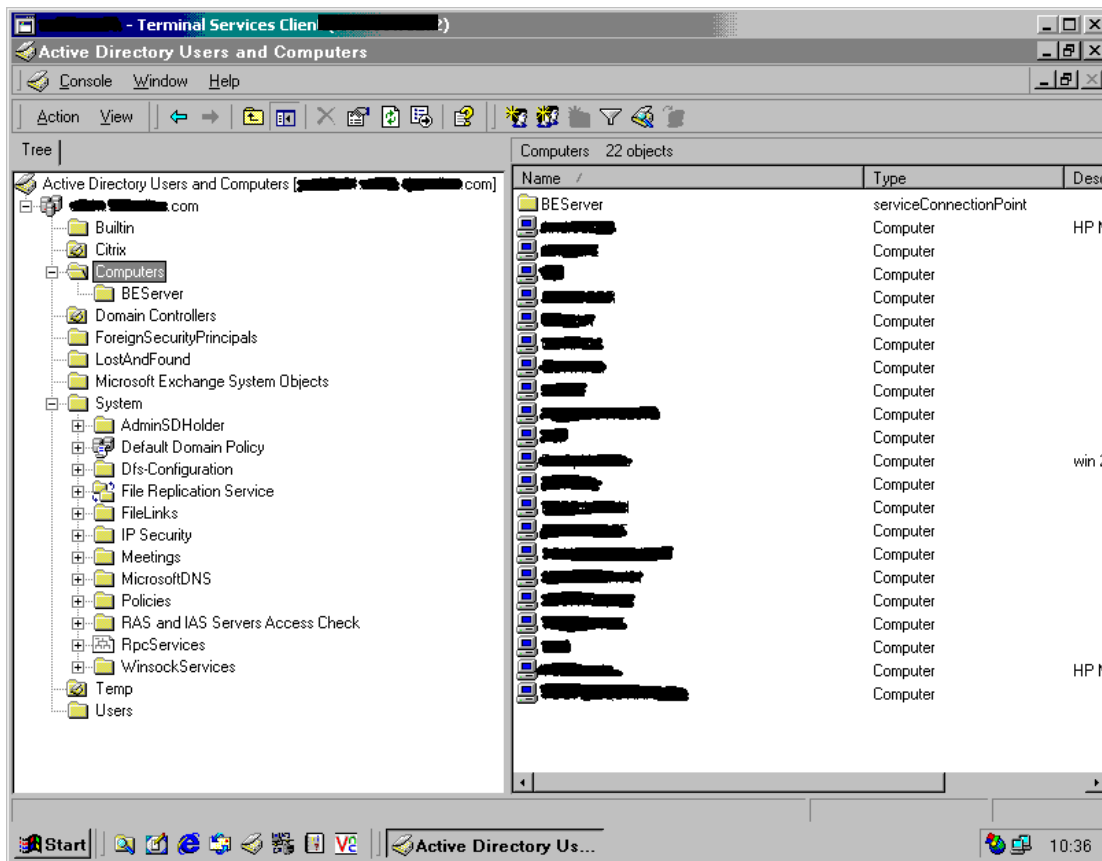


Bild 2: Alla klientdatorer samlade i OU Computers, utan indelning efter arbetsplats eller liknande. Katalogen BEServer är tom, annars ligger samtliga servrar i olika kataloger.

2 Brandväggar

Eftersom det fanns flera vägar in i LAN:et fick jag leta ett tag innan jag förstod vilket som var brandväggen, men det visade sig vara den enhet som satt innanför SDSL-modemet, av märket Nokia IP110 med mjukvara Check Point FW1/VPN1 Server. Den var alltså också ändpunkt för VPN-förbindelserna.

Brandväggstopologin var alltså en single host mellan Internet och LAN, en bra lösning med hänsyn till företagets storlek och verksamhet. Det fanns ingen webbserver eller något annat för åtkomst utifrån, inget som enligt min bedömning motiverade en mer komplex topologi som t ex DMZ.

Genomgång av trafikreglerna visade att det var bra skyddat för intrång utifrån, men att det var helt öppet för all trafik inifrån att ta sig ut. En dator i nätverket kunde därmed, genom användares försorg eller genom att datorn blev smittad av en trojan, öppna vilka tjänster som helst ut mot Internet utan att det märktes, och sedan släppa in vad som helst genom samma portar.

Eftersom brandväggen satts upp av tredje part och ingen konfiguration fanns dokumenterad, var det ingen som visste med säkerhet hur den fungerade, utan det liksom antogs att den gjorde vad den skulle. Någon testning av skyddet för att se om reglerna fungerade som det var tänkt hade aldrig gjorts. Någon form av

penetrationstest e dy hade inte heller genomförts, men det fanns det inte någon anledning att göra i Konstblommans fall.

Brandväggen hade inte heller uppgraderats eller patchats sedan den installerades för tre år sedan. Det behövde inte i och för sig betyda att den var en säkerhetsrisk, TCP/IP ser i stort sett likadant ut idag som för tre år sedan. Men det är alltid en säkerhetsrisk att ha opatchade enheter i nätverket och ska naturligtvis undvikas.

En uppgradering skulle förmodligen kosta Konstblomman mycket pengar. Dessa kunde kanske istället användas till inköp av ett nytt FW/VPN-system, eftersom det finns förhållandevis billiga sådana för mindre företag. Man skulle också kunna sätta upp en Linuxlösning till nästan ingen kostnad. Det fanns gott om pensionerade PC-maskiner som skulle kunna utgöra hårdvara i så fall.

Det förekom inga personliga brandväggar på klientmaskiner. Det hade varit ett billigt sätt att höja säkerheten ett snäpp till, men det skulle också innebära att användarna blev tvungna att godkänna och underkänna förfrågningar om internetåtkomst från allehanda applikationer och tjänster den första tiden. Att utsätta Konstblommans anställda för den prövningen var helt uteslutet. Dock, för företagets bärbara datorer kändes det mycket olustigt att veta att de inte hade lokal brandvägg. När de väl var anslutna via tunnel till domänen hade de ju samma skydd som de stationära maskinerna, men vad var de uppkopplade mot för anslutningar resten av tiden?

Skärmdumparna på nästa sida visar hur delar av brandväggens konfiguration såg ut.

Följande inkommande trafik släpptes igenom brandväggen (regel 1, 3 och 4):

- Alla protokoll från administratör till brandväggens gränssnitt.
- Alla protokoll från alla autentiserade till domänen efter kryptering (VPN).
- SMTP från varsomhelst till extern-mail.

No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	Admins	...	Any	accept	Long	Gateways	Any	
2	Any	...	Any	drop	Long	Gateways	Any	
3	Any	Client Encrypt	Long	Gateways	Any	
4	Any	extern-mail	smtp	accept	Long	Gateways	Any	
5	Any	Any	Any	accept	Long	Gateways	Any	
6	Any	Any	nbdatagram nbname	drop	Long	Gateways	Any	
7	Any	Any	Any	drop	Long	Gateways	Any	

Bild 3. Brandvägsreglerna i Check Point FW1/VPN1. Nr 5 är den regel som tillåter all utgående trafik att passera. Nr 7 stoppar allt som inte hindrats av tidigare regler.

Brandväggen stod även för adressöversättning (>) enligt tre regler:

- Alla protokoll från varsomhelst till extern-mail > mailgateway från original.
- Alla protokoll från mailgateway till varsomhelst > extern-mail från original.
- Alla protokoll från domänen till varsomhelst > extern-surf från original.

No.	Original Packet			Translated Packet			Install On	Comment
	Source	Destination	Service	Source	Destination	Service		
1	Any	extern-mail	Any	Original	...01	Original	Gateways	
2	...	Any	Any	extern-mail	Original	Original	Gateways	
3	...	Any	Any	extern-surf	Original	Original	Gateways	

Bild 4. Reglerna för adressöversättning i Check Point FW1/VPN1.

3 Intrångsdetektering

Något renodlat system för intrångsdetektering fanns inte, och man kan inte säga att det heller förelåg något direkt behov av ett sådant. För ett företag i Konstblommans storlek och verksamhet känns det överdrivet att föreslå att man investerar i ett särskilt IDS. Vad som kan göras för att se mönster är att studera loggen från brandväggen, och då förmodligen först sedan misstanke om intrångsförsök föreligger.

Det verkar inte särskilt proaktivt, det medges, men det handlar om en balansgång mellan säkerhetstänk och ekonomisk verklighet. Det gäller generellt i ett sådant här arbete, och som man som säkerhetsexpert med jämna mellanrum bör komma ihåg att tänka på. Optimal säkerhet ska eftersträvas, inte maximal.

Förutsättningen för att man ska kunna kosta på sig att avstå från IDS är förstås att ett eventuellt intrång genom brandväggen inte får katastrofala följder. Vid genomgången av Active Directory framkom ju att det inte rådde någon säkerhet alls bland resurser och kataloger; detta måste alltså åtgärdas även för att intrångsförsök ska upptäckas och stoppas.

Under den här punkten poängterade jag alltså även vikten av att ha högre logisk säkerhet på resurserna i nätverket än vad som nu var fallet.

4 Fjärranslutning

Fjärranslutningarna tyckte jag fungerade bra ur säkerhetssynpunkt när det gällde anslutningen, med en lagom nivå av autentisering och kryptering. Det förekom flera olika typer: VPN, uppringd modempool och dedikerad ISDN-anslutning.

Problemet som är lätt att förbise när man använder fjärranslutning är att hur säker förbindelsen i sig än är, innebär det en stor risk om miljön varifrån anslutningen sker inte är säker. När anslutningen väl är etablerad är det ju fritt fram i LAN:et.

En hacker behöver i princip bara ta sig förbi en hemdators (eventuella) brandvägg för att komma in i ett företags nätverk med samma behörigheter. Om då Everyone har fulla behörigheter nästan överallt – som var fallet i Konstblommans nät – kan konsekvenserna bli katastrofala. Detta har jag påpekat tidigare under avsnittet om brandväggar, men det förtjänar att upprepas.

5 Logghantering

Logghanteringen fungerade bra. Om fel uppstod på t ex backupen användes loggfilerna för att se varför, och felet noterades och rättades till. Jag bedömde att standardloggning var tillräckligt för Konstblommans miljö.

Loggfilerna kollades varje morgon på distans från WM-datas kontor.

Däremot hade det varit på sin plats att göra prestandaloggning på ett par av serverna, för att se hur de använde minnet. Det fanns tecken som tydde på att de använde växlingsfilen väldigt mycket, trots att de egentligen tyckes ha tillräckligt med minne installerat. Det skulle behöva kollas närmare.

6 Uppdateringar

Patching av datorerna släpade på många håll efter. Framförallt fanns det ingen regelbundenhet eller automatik i uppdateringarna. Jag hade inte hunnit kolla alla datorer i företaget, det kunde hända att en del användare hade automatisk uppdatering aktiverat eller uppdaterade manuellt, men det var i så fall långt ifrån alla.

Eftersom det blir viktigare och viktigare med regelbundna och snabba säkerhetsuppdateringar, kunde det vara värt att fundera på en automatisering av det hela genom t ex MS Software Update Service. Det skulle visserligen innebära en del arbete att sätta upp, men skulle å andra sidan spara tid och pengar i längden och – framförallt – inte kosta något för Konstblomman att införskaffa.

7 Backup – Redundans – UPS

Konstblommans backupschema var bra. Full backup varje kväll, vilket fungerade eftersom datamängden inte var så stor (ca 20 GB, 4-6 timmar med backup och verifiering) och skulle ge snabbast möjliga återställning när det behövdes. Mjukvaran som användes var Veritas Backup Exec 8.0.

Det togs bara backup på två av serverna och inte på den tredje, terminalservern. Den ansågs inte innehålla omistlig data, men jag ansåg att den inte skulle kunna stå stilla så lång tid som det skulle ta att återställa den om den havererade. Enligt uppgift skulle det finnas en imagefil av den men den stod inte att finna. Den borde alltså åtminstone ghostas om.

En annan sak som oroade mig var att backupen då och då misslyckades. Ett par, tre gånger i månaden fungerade det inte, och av lite olika anledningar varje gång: plötsligt nekad åtkomst till gammalt användarkontos mailkatalog, misslyckad verifiering pga dåligt DAT-band, mm. Ofta småfel, men som genererade Backup Failure varje gång.

Men den största anmärkningen när det gällde backupen var att mediet förvarades i serverrummet. Visserligen i ett brandklassat kassaskåp, men eftersom det också förvarades stora mängder papper och annat eldfångt material i samma rum kunde det

inte betecknas som annat än oacceptabelt ur brandsäkerhetssynpunkt. Eftersom det fanns fler kassaskåp på arbetsplatsen skulle en enkel åtgärd ha varit att förvara backupen i något av dem istället. Dock vore den bästa åtgärden – som alltid – att förvara den någon helt annanstans.

DC/Fil- och mailservern, databasservern och terminalservern var redundanta genom att de använde RAID 5, och några av dem var också ghostade. Flera andra vitala datorer behövde också ghostas, och en del som redan var det borde ghostas om eftersom de hade förändrats.

Att ta reda på (dokumentera!) vad som skyddades av UPS, och att testa UPS-funktionen kändes angeläget, då det fanns mycket gammal utrustning i drift. Emellertid skulle det vara svårt att testa funktionen just pga den gamla utrustningen.

8 Virussydd

Virussydd för klienterna i Konstblommans nätverk fanns men var långt ifrån optimalt. Alla hade Norton Antivirus installerat, det skannade i realtid, men inte alla uppdateringar skedde regelbundet eller automatiskt och virusutbrott hade förekommit flera gånger, om än inte av katastrofal omfattning.

Av serverna var det två som inte hade något virussydd installerat: databasservern och terminalservern. Det kanske berodde på att t ex snabba svarstider i en databas har prioritet, eller har det inte blivit gjort av någon annan anledning. Men risken var uppenbar: om någon skulle fjärransluta med en virusmittad dator och arbeta mot terminal- och databasservern skulle de med största sannolikhet också bli smittade. Det fanns ju dessutom ingen backup på terminalservern.

Man kan säga att de två serverna utgjorde en begränsad risk, i betydelsen att alla datorer som omgav dem var väl skyddade, men skulle de bli smittade innebar det driftstopp, återställningstid och irritation. Eftersom det inte fanns någon (för mig känd) anledning att lämna någon dator oskyddad skulle jag rekommendera att virussydd installerades på samtliga, och att någon form av automatik i uppdateringen av virusdefinitionsfilerna implementerades.

Från början förekom två virussydd i nätet, Symantec Antivirus och F-secure Antivirus. Klienterna och serverna använde Symantec, och TFS SMTP-gateway använde F-secure.

Denna SMTP-gateway var orsaken till mycket bekymmer. Den var tänkt att avlasta och skydda mailservern men var så instabil att den stannade helt, till en början bara emellanåt men mot slutet så gott som dagligen. Till slut införskaffades ett nytt programpaket från Symantec, och i det ingick en ny SMTP-gateway såväl som ny version av Norton Antivirus Corporate Edition. Efter att den nya SMTP-gatewayen installerats på ny dator och trimmats in, och alla klienter uppgraderats till senaste versionen och konfigurerats att uppdatera regelbundet mot intern server, fungerade virussyddet till belåtenhet. Och framförallt fungerade mailtrafiken utan avbrott och irritation för första gången på länge.

I detta fall innebar alltså steget att gå från två olika till bara ett virussydd en förbättring, även om bekymren med SMTP-gatewayen nog i första hand berodde på TFS gateway-mjukvaran. Dock ska påpekas att det generellt är bättre om flera olika sorters virussydd förekommer i ett nätverk, då aldrig ett fabrikat är lika bra på allt. Av samma anledning kan man använda personliga brandväggar på klientdatorer fast det redan finns en avancerad brandvägg som skyddar hela nätverket mot omvärlden.

Den nya SMTP-gatewayen innebar en stor förbättring av driftsäkerheten på mailsystemet, inte minst för administrationen och överblicken av virusaktiviteten bland e-posten. Den gick dessutom att konfigurera för att skydda mot spam, på ett par olika sätt. Det intressantaste blev att använda en DNS Block List.

9 Fysiska risker

Serverrummet var visserligen inte låst men låg längst in i byggnaden och var under uppsikt, så det fick jag betrakta som tillfredsställande säkert. Anledningen till att det inte var låst var att det även användes som förvaringsutrymme, och att personalen måste kunna komma och gå för att hämta och lämna saker. Stöldmärkning eller fastlåsning av datorer och utrustning förekom inte.

Brandrisken var tvungen att påpekas. Datorutrustningen var förhållandevis gammal, eluttagen väl nyttjade och sladdar och kablar i oordning. Detta i kombination med faktumet att rummet användes till förvaring av stora mängder papper, dokument och annat brännbart material, och konsekvensen en brand skulle innebära för företagets resurser, gav stor anledning till oro.

Det är allvarligt om det går att komma åt servrar och klienter med bootbar media. Detta borde som standard vara omöjligt för den som inte har behörighet till de lösenordsskyddade BIOS-inställningarna. I detta fall var ju datorerna under uppsikt, så risken att någon obehörig skulle kunna göra något var att betrakta som liten, men icke desto mindre skulle jag komma att rekommendera att man avaktiverade boot från CD och diskett, och låste BIOS med lösenord på samtliga datorer där det inte var gjort.

10 Kryptering

Tunnlingen med VPN gjorde att fjärranslutningarna över Internet till Konstblomman var väl skyddade. Övriga fjärranslutningar var dedikerade ISDN- och 56k-modemuppkopplingar och hade inget behov av kryptering.

E-post krypterades inte, vilket kunde innebära en säkerhetsrisk om den användes för känslig information.

De bärbara datorerna var ett orosmoment, då det vid eventuell stöld var fritt fram att läsa allt på hårddisken. Om känslig information förvarades på dem borde den ligga i en väl krypterad katalog. Det finns bra gratis verktyg att använda för sådan kryptering.

11 Server

Det allvarligaste problemet i Konstblommans servermiljö var att två av datorerna inte var servrar, utan vanliga PC-maskiner. De hade tidigare varit klientdatorer, och alltså varit i bruk i flera år innan de blev servrar. Den ena hade visserligen en ny hårddisk, men risken för hårdvarufel pga ålder och låg prestanda måste ändå bedömas som stor. En av PC-servrarna använde dessutom Windows 2000 Professional som operativsystem.

En server var en IBM AS/400, som enligt uppgift bara användes vid revision en gång om året. Den lät jag vara ifred.

För att få en överblick på säkerhetsnivåerna på såväl servrars som klienters konfigurationer, kunde en analys med t ex MS Baseline Security Analyzer göras.

Minnesresurserna verkade vara ansträngda på några av servrarna. Fil- och mailservern - tillika domänkontrollanten - hade oförklarligt tappat kontakten med databasservern vid ett par tillfällen. Båda dessa servrar använde växlingsfilen mycket. Kontroll av detta kunde göras med prestandaloggning.

12 Klient

Det kändes angeläget med en inventering av klientdatorerna, vilken hårdvara det satt i dem och vad de använde för programvaror. En del var nya eller ominstallerade, andra hade bytt ägare, men det fanns ingen heltäckande dokumentation. En lista över nya datorer hade påbörjats, och den borde naturligtvis fyllas på med mer information. Jag hade fått mina uppgifter om namn och operativsystem från Active Directory, men det förekom säkert inaktuella datorobjekt där också, precis som det fanns t ex inaktuella användarkonton.

13 Nätverksutrustning

Nätverksutrustningen var i fungerande skick, om än gammal. Ordentlig märkning av utrustning och kablage hade underlättat arbetet.

Det fanns flera olika enheter som alla hade väldigt många inbyggda funktioner, och därigenom hade kunnat inkräkta på varandra om de varit dåligt konfigurerade. Det fanns bl a VPN-, NAT- och DHCP-server i tre olika enheter, men de delade på uppgifterna och lät varandra vara ifred. Dock gjorde det att man inte gärna ville ge sig in och ändra för mycket i deras konfigurationer, helst bara titta.

IBM 2210 routern var den del av nätverket som jag visste minst om. Det var där som ISDN-uppkopplingarna kom in och gick vidare i nätet. Men vilka funktioner utförde den? Jag hade t ex inte sett att fjärranvändarna som använder ISDN-uppkoppling autentiserades någonstans. Skedde detta i routern, eller bara i Windows?

Konstblomman använde sig av IP-telefoni, och en del av nätverket utgjordes av utrustningen för det. Telenätet höll till på ett eget logiskt nät. Den enda kopplingen till

resten av nätverket bestod av ett ethernet-gränssnitt mot den centrala switchen, för att telenätet skulle kunna administreras via applikationer på klientdatorerna, och för att det fanns en server som tillhandahöll röstmeddelanden och pausmusik. På LAN-skissen på sidan 17 är det den vänstra fjärdedelen som utgör IP-telefoninätet.

14 Teknisk dokumentation

Dokumentation är som alltid A och O. Jag hade inventerat och dokumenterat en hel del under min analys, men mer arbete återstod för att komma upp på en bra nivå. Klienterna behövde komma med mer i inventeringen, och det gällde att få till standarddokument som var lätta att fylla på med nya uppgifter efterhand.

Utrustning och kablage behövde få en tydlig och konsekvent märkning.

Licenshanteringen var ett känsligt område som måste dokumenteras. Det var osäkert vilka typer och hur många licenser som fanns, och om fler måste inhandlas för att programvara i nuläget användes olicensierat. Vid närmare efterforskning visade det sig att i alla fall ett program som det bara fanns enanvändarlicens till användes av i stort sett alla på företaget.

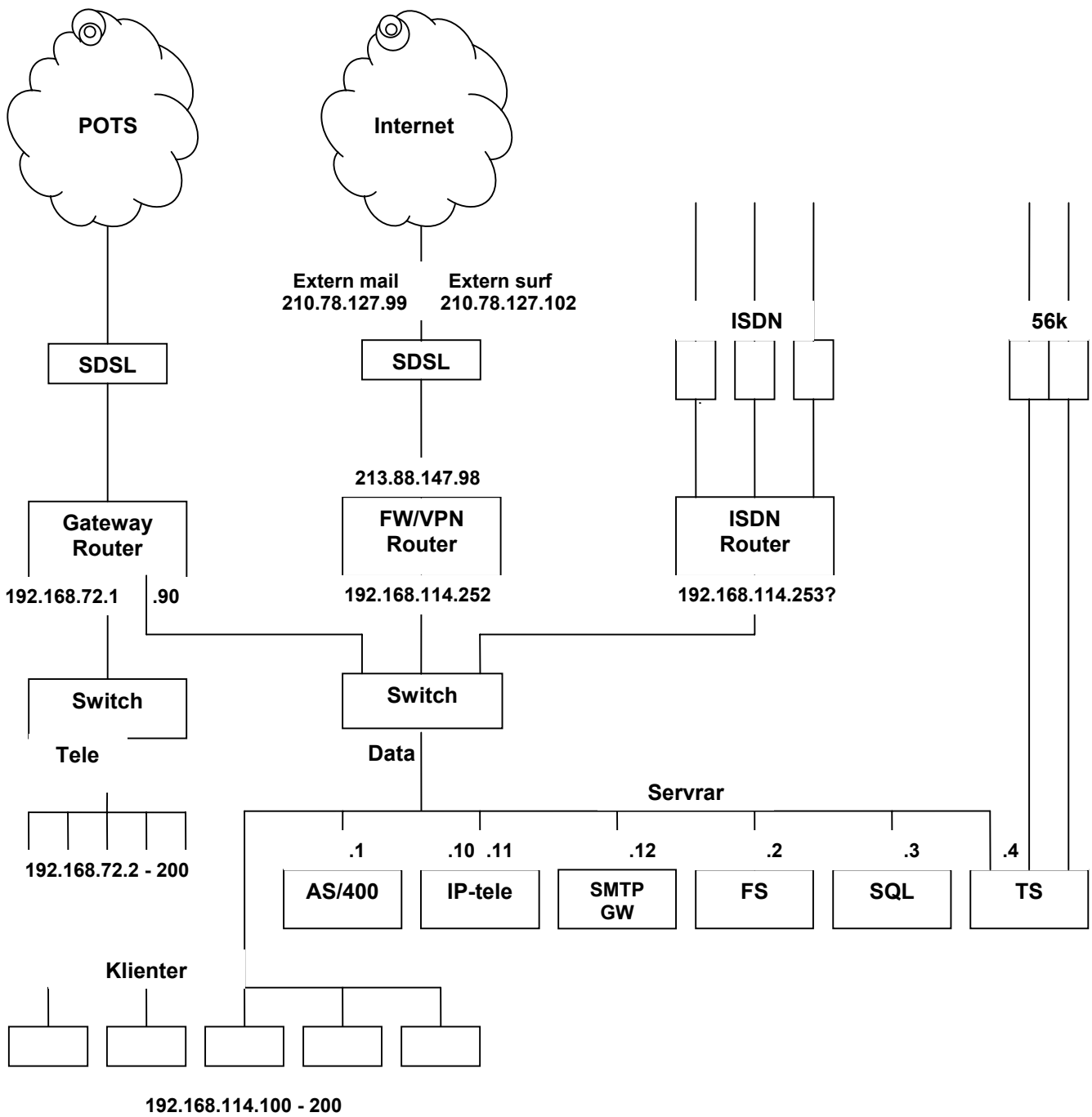
15 Topologi

Det rådde oklarhet om var nätverkets default gateway 192.168.114.253 befann sig. IP-numret på brandväggens insida, som jag först antog var DG, var 192.168.114.252. Om man gjorde en traceroute till utsidan av nätet, t ex till Extern surf 210.78.127.102, så gick vägen ut först via .253, och sedan direkt via .252. Frågan var alltså var .253 fanns? Förmodligen i ISDN-routern, konfigurationen på den var ju okänd.

Vad var anledningen till att trafiken först gick till .253, och att den var default gateway överhuvudtaget? Jag misstänkte att ISDN-routern en gång varit den ursprungliga förbindelsen ut och att DG-inställningen hängt kvar sedan dess. I vilket fall som helst verkade det innebära att all trafik, helt i onödan, tog en extra runda i LAN:et innan den kunde hitta ut.

Det fanns inget dokument över den fysiska topologin än. Jag hade tänkt göra ett bara över serverrummet, men då det intressantaste var kabeldragningen, uttag och klienter i andra änden, borde den omfatta hela arbetsplatsen. Ett sådant dokument hade också kunnat innehålla en efterlängtd inventering över klientdatorerna och skrivarna: rum, uttag, namn, användare.

På nästa sida återfinns en beskrivning av det logiska nätverket. Om detta är PDF-varianten av examensarbetet ser skissen lite konstig ut. Den blir bättre vid utskrift.



Skiss 1. Nätverkets logiska topologi, funktion och IP-nummer.

16 Säkerhetspolicy

Konstblomman var ju ett förhållandevis litet företag. Jag misstänkte att det kanske inte fanns någon skriven informationssäkerhetspolicy, och efter att ha låtit rätt person läsa igenom det frågeformuläret fick jag det bekräftat. Det var en förhållandevis liten personalstyrka, alla kände varandra och det var en stämning av familjeföretag över det hela. Någon särskild säkerhetspolicy hade aldrig funnits och det kändes inte heller aktuellt att införa någon.

17 Tillgångar och klassificering

Av i stort sett samma anledning som i förra punkten fanns det inte något att hämta under den här rubriken heller. Några särskilda dokument eller rutiner för klassificering eller förvaltning av information fanns inte, och var inte heller aktuellt i nuläget.

18 Personal och säkerhet

Det hade inte utarbetats några skrivna rutiner eller dokument för anställda avseende informationssäkerhet, också det beroende på karaktären av familjeföretag. Att man skulle ha skrivna avtal om att man inte fick bete sig på vissa sätt i IT-miljön på en sådan arbetsplats var en främmande tanke.

Utbildning i praktiska IT-frågor behövdes ibland, och skedde spontant när behov fanns. Detta fungerade bra.

En förbättring av arbetsmiljön för IT-personalen skulle leda till effektivare insatser och bättre säkerhet. I det ingick bättre dokumentation, märkning av utrustning och kablage och uppdatering/ombyggnad av Active Directory, men även t ex lätt ommöblering bland skärmar och tangentbord i serverrummet.

19 Riskanalys och katastrofberedskap

Naturligtvis förfogade Konstblomman över resurser som det var av stort värde att skydda, men man förlitade sig på de säkerhetsfunktioner som var i bruk: backup, brandsäkert kassaskåp, brandvägg, virussydd, människors ärlighet, mm.

Liksom många andra mindre företag levde man i en till vissa delar falsk trygghet, men detta fick ju ställas i relation till många andra faktorer, t ex vilken verksamhet som bedrevs, vilka risker som fanns mot just den verksamheten, vad det skulle kosta att ha bättre skydd. Med andra ord sådana frågor som en riskanalys hade kunnat ge svar på, men även det bedömde jag som en mindre realistisk åtgärd att föreslå i dagsläget, främst på grund av ovannämnda falska trygghetskänsla. Det skulle behövas mer tid för att motivera och övertyga om vikten av en riktig riskanalys.

Åtgärdsförslag

Här följer en sammanställning av den ordning i vilken jag ansåg att säkerhetshöjande åtgärder för respektive kategori borde genomföras. Prioriteringen gick från mest brådskande (tre utropstecken) till minst eller inte brådskande (ett utropstecken). Denna prioritering avsåg enbart hur viktiga åtgärderna var, inte hur omfattande eller kostsamma de skulle vara att genomföra.

- !!! Fysiska risker
Uppdateringar - Patchning
Backup - Redundans - UPS

- !! Active Directory
Brandväggar
Fysiska risker
Fjärranslutning
Kryptering
Server
Teknisk dokumentation
Personal och säkerhet

- ! Intrångsdetektering
Logghantering
Klient
Nätverksutrustning
Topologi
Säkerhetspolicy
Tillgångar och klassificering
Riskanalys och katastrofberedskap

Nästa sammanställning visar vilka åtgärder som jag skulle velat genomföra i respektive kategori. Detta var en önskelista; en del åtgärder skulle inte bli aktuella pga för stor kostnad, arbetsinsats, eller för att säkerhetsnivån inte stod i proportion till företagets verksamhet och önskemål. Dessa åtgärder, som jag bedömde som mindre genomförbara, är markerade med *.

!!!

Fysiska risker

Flytta brandfarligt material från serverrummet.

Uppdateringar - Patchning

Patcha klienterna till senaste service pack för respektive operativsystem + Windows update.

Patcha MS Office till senaste service pack + Office update.

Uppdatera/patcha övrig mjukvara.

Implementera MS SUS

Backup - Redundans – UPS

Ändra förvaringsplats för backupmedia.

Testa återställning från backupmedia.*

Testa UPS.*

!!

Active Directory

Bygga om OU-strukturen.

Inventera/åtgärda inaktuella objekt.

Skapa ändamålsenliga regler/GPO:er.

Skapa/befolka säkerhetsgrupper

Begränsa resursbehörigheterna

Brandväggar

Uppgradera/patcha Check Point, ev. byta till annan brandvägglösning.*

Sätta begränsningar på utgående trafik.*

Fysiska risker

Inaktivera start av datorer från annan media än hårddisk.

Låsa tillgång till BIOS med lösenord.

Fjärranslutning

Undersöka ISDN-routern.

Säkerställa att fjärranvändarnas datorer var säkra mot intrång.*

Kryptering

Kryptera känslig information på bärbara datorer.*

Server

Mäta minnesanvändning med prestandaloggning.
Byta de två PC-servrarna mot riktiga servrar.*

Teknisk dokumentation

Skapa standard för teknisk dokumentation.
Inventera klientdatorer och skrivare.

Personal och säkerhet

Utbilda personalen i säkerhetsmedvetenhet.*
Förbättra miljön för IT-personalen.

!

Intrångsdetektering

Implementera ett IDS-system.*

Logghantering

Utarbeta regler för loggning och automatisera sammanställningar.*

Klient

Inventera klientdatorerna.

Nätverksutrustning

Märka utrustning och kablar.

Topologi

Dokumentera den fysiska topologin.

Säkerhetspolicy

Utarbeta och skriva en informationssäkerhetspolicy.*

Tillgångar och klassificering

Inventera och klassificera företagets tillgångar.*
Utse förvaltare av tillgångarna.*

Riskanalys och katastrofberedskap

Genomföra en heltäckande riskanalys.*
Utarbeta en plan för katastrofberedskap.*

Slutsats

När jag började arbetet med frågeformulären blev det först många fler än nitton rubriker. Jag var rädd att missa något och tog därför med alldeles för mycket. Efterhand blev det till en mer hanterbar men ändå uttömmande samling frågor som jag tyckte verkade lagom för ett företag i Konstblommans storlek. Efter att ha genomfört analysen anser jag att det blev bra och rätt. Formulären blev flexibla, de kan enkelt byggas ut med mer detaljerade frågor för komplexare miljöer eller färre för enklare, men med samma heltäckande grundstruktur och samma ”basfrågor”.

Säkerhetsanalyser kan betraktas olika. Vi som arbetar med att utföra dem ser dem på ett sätt, beslutare hos kund på ett annat, och användare på ett tredje. Det vi menar med en komplett analys är i regel inte vad kunden menar. Eller rättare sagt: det finns olika stadier av fullkomlighet, och en viktig egenskap man måste ha som säkerhetsexpert är att känna av när optimal säkerhet råder. Med det menar jag att ibland kommer man inte längre i säkerhetsarbetet därför att det inte lönar sig. Det kan vara för att det blir för dyrt, för att man inte klarar av att övertyga kunden om risker man vet finns, eller för att man själv som expert tenderar att tänka på maximal säkerhet istället för optimal.

Svaret på frågan om en ”komplett” analys kan genomföras beror alltså på vad man menar med komplett: ja, när säkerhet uppnås efter de förutsättningar som råder är den komplett, och nej, eftersom det alltid finns fler frågor att grotta ner sig i blir den aldrig komplett. Dock är det alltid kunden som, efter att ha fått alla fakta och valmöjligheter tydligt presenterade av oss, bestämmer innebörden i begreppet säkerhet för sin egen del, och aldrig vi.

Det stod från början klart för mig att om man nu ska skapa och använda standarddokument och standardarbetsätt, så kan man ju inte börja ändra i dem i någon större omfattning efterhand som nya förhållanden upptäcks. I så fall har man misslyckats med standardiseringen. Men att detaljer dyker upp som får en att göra något tillägg eller en omformulering är naturligtvis ofrånkomligt. Det är också så att någon speciell egenhet i just den IT-miljön man befinner sig i för tillfället kan göra att man ställer några frågor där som man aldrig kommer att ställa någon annanstans.

I Konstblommans fall var det ju så att bl a avsnittet som behandlade säkerhetspolicy och personalfrågor gick bort i stort sett helt, eftersom det inte var läge att påpeka säkerhetsfördelen med att få personalen att skriva under ett papper på att de inte tänkte bete sig kriminellt. Ett exempel på hur analysen ibland inte bara kan, utan måste, anpassas när man har börjat lära känna miljön bättre.

Konstblommans lokaler präglades alltså av en ganska familjär och anrik stämning som var lätt att falla in i. Jag var där nästan dagligen i ett par månader och påverkades naturligtvis av miljön. Min bestörtning över att vanliga PC-maskiner användes som servrar var t ex påtagligt dämpad efter att en längre tid hade gått utan att de havererat.

Just av den anledningen gäller det dock att vara på det klara med om det är så lugnt som det verkar eller om det finns tickande bomber i bygget. Om det, som hos Konstblomman och från deras synpunkt (som är den som gäller) helt riktigt, inte finns några skrivna regler för godtagbart bruk av IT-resurser, känner jag att man på något sätt borde få bekräftat att det verkligen är lugnt på den fronten. Jag har ingen aning om hur det skulle gå till, men det hade i så fall undanröjt en säkerhetsbrist av det mer komplexa slaget.

Det är klart man påverkas av miljön man arbetar i, och lika klart borde det vara att man är medveten om och anpassar sig efter det. Värt att påpekas här är att normalt säkerhetsanalysarbete i regel inte ser ut som det jag utförde hos Konstblomman: vecka efter vecka med i stort sett obegränsat med tid till mitt förfogande, och med möjlighet att lära känna miljön bättre än de flesta. Vanligtvis har man ett givet begränsat uppdrag, snål tidsram, och klara regler för hur mycket av miljön man får röra sig i. Under sådana arbetsförhållanden är det naturligtvis mycket mindre risk för att analysarbetet ska påverkas av vilken anda och kultur som råder på arbetsplatsen.

Slutligen kan det alltså konstateras att teori och praktik i det här sammanhanget – som i de flesta andra – har ett behov av att finna varandra och komma överens om vilken väg som är den bästa att slå in på. Ju snabbare det sker i en ny och okänd miljö, desto smidigare kommer arbetet att gå. Men för att utveckla den förmågan krävs mycket kunskap, träning och framförallt erfarenhet. Det senare är jag väldigt tacksam över att ha fått mig till livs under min tid hos WM-data IT-support.

Källförteckning

Maiwald, Sieglein: Datasäkerhet i praktiken, Pagina Förlags AB, 2002.
STG/TG99 AG6 (arbetsgrupp): Handbok i informations säkerhetsarbete, SIS Förlags AB, 2001.

Bilagor

1. Teknisk dokumentation, exempel på frågeformulär. (Ej tillgängligt via hemsidan.)