Avdelning för datavetenskap

Jon Nilsson

Spårbarhet

En underskattad dimension av informationssäkerhet

Traceability

An underestimated dimension of information security

Examensarbete (10p)
Dataingenjör

Datum:	07-10-12
Handledare:	Donald F. Ross
Examinator:	Martin Bloom
Ev. löpnummer:	C2007:09

A Karlstads universitet 651 88 Karlstad
B Tfn 054-700 10 00 Fax 054-700 14 60
C Information@kau.se www.kau.se

Denna rapport är skriven som en del av det arbete som krävs för att erhålla en kandidatexamen i datavetenskap. Allt material i denna rapport, vilket inte är mitt eget, har blivit tydligt identifierat och inget material är inkluderat som tidigare använts för erhållande av annan examen.

_____

Jon Nilsson

Godkänd:

_____

Handledare: Donald F. Ross

_____

Examinator: Martin Bloom

Sammanfattning

Målet med examensarbetet var att undersöka spårbarhet hos olika inforamtionssäkerhetsåtgärder åt företaget Veriscan i Karlstad. Examensarbetet ger först en teoretisk genomgång av olika säkerhetsåtgärder för att sedan försöka hitta gemensamma nämnare till de säkerhetsåtgärderna som innehåller spårbarhet.

I en värld full av teknik och information som flödar är det viktigt att ha kontroll över de data som anses vara viktig för organisationen. Skulle informationen hamna i orätta händer kan det innebära förödande konsekvenser för organisationen och i vissa fall även deras kunder. Har en incident väl inträffat måste man ha säkerhetsåtgärder som generera spårdata som gör att konsekvenserna av incidenten kan rättas till och att den skyldigt åtalas om brott begåtts.

Uppsatsen handlar om att undersöka vilka säkerhetsåtgärder som bidrar till spårbarheten. Kravet var att skapa en lista med säkerhetsåtgärder där ett poängsystem visade spårbarheten hos säkerhetsåtgärderna. Resultat av min undersökning är att det finns flera åtgärder som bidrar till spårbarheten och att den gemensamma nämnaren är spårgenerering eller loggning. Prioritet 1 var att belysa de systemtekniska säkerhetsåtgärderna och i mån av tid även de fysiska och de logiska säkerhetsåtgärderna.

Ämnet spårbarhet är väldigt nytt och jag känner är att jag har varit ute på väldigt ny mark. Det har varit svårt att hitta information om just spårbarhet. Detta område är väldigt nytt och jag känner att det kommer att bli stort inom en snar framtid. Under projektets gång har jag lärt mig mycket om informationssäkerhet och bredden av ämnet. Även att det är ett av de viktigaste ämnen för organisationer idag och kommer vara för en tid framöver.

Traceability - An underestimated dimension of information security

Abstract

The goal with this dissertation was to examine traceability within a company in different information security contexts. The company´s name was Veriscan and they are a company that measures other company's information security. This dissertation gives first a theoretical review of different counter measures to try and find a common denominator for those counter measures that contain traceability.

In a world full of technique and information that flows around is it important to have controll over the information that has value for the company. If this information got into the wrong hands, it would be a catastrophy for both the company and its clients. If an event has happend the company needs to have some security tools that generate trace data so that the consequence of the event can be coreccted and the guilty parties can be prosecuted if a crime has been commited.

This dissertation examines those security measures that contribute to traceability. The requirement was to create a list of counter measures that had a score table for how much the countermessures helped traceability. The result of this study was that there are many counter measures which contribute to traceability and that these counter measures had one or two aspects in common. Either it was trace generating or the counter measure had computer logging implemented. The first priority was to discuss the system technical counter measures and if there was time even the physical and the logical counter measuers should be examined.

It has been hard to find new information about traceability. This subject is new and I feel that will be a major subject in the future. During this papper I have learned much about how big this subject really is. Security is growing at rapid rate and because of that it will be one of the most important subjects for companies today and for a long time.

Förord

Till att börja med vill jag tacka min handledare Donald Ross för hans hjälp och många idéer. Fia Ewald som var min handleradre från Veriscan ska ha stort tack för all hennes hjälp, speciellt med förslaget till examensarbete. Lorentz Lundmark som är delägare i Veriscan för hans stöd och glada humör. Ulf E Larson lärare vid Chalmers för hans hjälp med loggning och intrång. Alf Nilsson för hans bidrag med information och bidragande med studiebesök vid IT-enheten i Karlstad.

Innehållsförteckning

Figurförteckning

Tabellförteckning

1 Inledning

I en värld full av teknik och information som flödar är det viktigt att ha kontroll över den information som anses vara viktig för organisationen. Skulle informationen hamna i orätta händer kan det innebära förödande konsekvenser för organisationen och i vissa fall även deras kunder.

Nu när hela samhället är ett informationssamhälle, datorerna utvecklas i en snabbare takt och används mer i olika delar av vår vardag ökar också flödet av information. Säkerheten kring all denna information är just nu viktigare än någonsin. Idag är det materiella värdet på många produkter bara en bråkdel av det totala värdet. Det största värdet är kunskapen som finns inbyggd i produkten. Om denna informaion kommer ut, den information som företaget har lagt ner miljonbelopp på att ta fram, är det ren katastrof. Informationssäkerheten är med andra ord en av de viktigaste sakerna för företag och privat personer.

Veriscan är ett företag som ägnar sig åt att mäta eller betygsätta andra företags informationssäkerhet. Veriscan har 5 olika nivåer för mätning och dom mäter fysisk, logisk och systemsäkerheten hos företag. I kapitel 2.6 finns en tabell över Veriscan modell för mätning av inforamtionssäkerhet.

Veriscan hade en fundering om vilka säkerhetsåtgärder som är kopplade till spårbarhet. Denna fundering gav dem till mig som uppsats arbete. Denna uppsats har alltså till uppgift att ta reda på vilka säkerhetsåtgärder som innehåller spårbarhet eller som bedrar till spårbarhet.

1.1 Motivation till denna studie

Anledningen till denna rapport att jag känner starkt för området säkerhet och framför allt för informationssäkerhet. Detta uppdrag som jag fått av Veriscan känns spännande och framför allt utmanande. Målet är att få mer och fördjupad kunskap inom området och jag tycker att detta projekt är perfekt för att få en ökad förståelse för informationssäkerhet.

1.2 Problemställning

Intressanta frågor är bland annat. Finns spårbarhet? I vilken form finns spårbarhet? Blir spårbarhet en följd av införd åtgärd?

Dessa frågor har jag försökt att svara på via att gå igenom åtgärderna i detalj för att hitta vad i säkerhetsåtgärden som bidrar till spårbarhet. Det som bidragit till spårbarheten har sedan undersökts noga och gåtts igenom för att skapa ett svar på de frågor som ställts.

1.3 Veriscans behov

Veriscan har som mål att få en lista med olika systemsäkerhetsmässiga, logiska och fysiska säkerhetsåtgärder som kan kopplas till spårbarhet. Veriscan vill även ha vilka säkerhetsåtgärder som är indirekt kopplade till spårbarhet och vilka säkerhetsåtgärder som ger spårbarhet som följd.

1.4 Avgränsning

Jag har kommit överns med Donald och Veriscan att de systemtekniska säkerhetsåtgärderna kommer att vara i focus i uppsatsen. I mån av tid kommer även de fysiska och logiska säkerhetsåtgärderna att tas upp.

Finns det beroende av spårbarhet? Är spårbarhet en följd av denna åtgärd? Detta är några av de frågor som ska undersökas i varje säkerhetsåtgärd. Avgränsningen på systemtekniska åtgärder gör det möjligt att gå in i en mer detaljerad beskrivning av säkerhetsåtgärderna.

1.5 Syfte och mål

Syftet med min rapport är att få djupare förståelse och kunskap inom området informationssäkerhet. Detta ska ske genom att undersöka flera olika säkerhetsåtgärder i letandet efter spårbarhet och genom att aktivt läsa och utvärdera olika säkerhetsåtgärder.

1.6 Disposition

I kapitel 2 beskrivs och definieras information, informationssäkerhet och spårbarhet. Uppsatsen ska undersöka olika säkerhetsåtgärder, och se om det existerar spårbarhet eller om spårbarhet blir en följd av införd åtgärd. Genom att skapa en klar definition av spårbarhet blir det enklare att se om en säkerhetsåtgärd innehåller spårbarhet eller om spårbarhet blir en följdåtgärd. Finns det spårbarhet? Blir spårbarhet en följd? Dessa frågor ska besvaras i kapitel 3.

I kapitel 4 belyses mekanismerna bakom spårbarhet mer detaljerat. I detta kapital tas det fram varför en säkerhetsåtgärd innehåller spårbarhet eller har spårbarhet som följd.

Hur kan man gå tillväga för att leta reda på information om ett intrång? Kapitel 5 handlar om analys av intrång. Här går jag igenom vart man hittar relevant information vid intrång och vart denna information ska hämtas från, även hur informationen ska hanteras.

För att förtydliga detta finns det ett scenario i kapital 6. I detta scenario går jag igenom hur det skulle kunna gå till om ett intrång sker.

Kapitel 7 är slutsatsen som jag kommit fram till efter detta examensarbete.

2 Bakgrund

Begreppet informationssäkerhet är komplext och kan ses i flera olika dimensioner. En vanlig uppdelning är att dela upp ämnet i fyra stycken grundpelare, sekretess, tillgänglighet, riktighet och spårbarhet. Ett problem har alltid varit att koppla dessa dimensioner till konkreta säkerhetsåtgärder, framför allt spårbarhet. Denna uppsats ska ta upp ett antal säkerhetsåtgärder och undersöka om dessa innehåller spårbarhet eller ej, samt undersöka om spårbarhet blir en följd av införd säkerhetsåtgärd. För att kunna förklara vilka säkerhetsåtgärder som innehåller spårbarhet krävs en klar definition av spårbarhet och för att kunna göra en definition på spårbarhet krävs det definitioner av information och informationssäkerhet. Därför kommer en definition av information att ges först, följt av en definition av informationssäkerhet. Efter definitionen av spårbarhet kommer en förklaring av och exempel på ett informationssystem. Detta görs för att enkelt kunna förklara Veriscans modell för mätning av informationssäkerhet.

2.1 Information

Det finns olika definitioner på vad information är. Att det finns flera olika definitioner beror på att information har olika betydelse i olika sammanhang. Nedan listas en definition och en iakttagelse av information som känns relevanta för denna rapport.

Definition av information: ”Information är en generell beteckning för det meningsfulla innehåll som överförs vid olika former av kommunikation mellan sändare och mottagare.” [1]

Iakttagelse av information: ”Sedd ur ett användarperspektiv kan information sägas uppstå först när ett meddelande tolkas av mottagaren.” [2]

Ur dessa definitioner kan man tolka information som innebörden av ett meddelande. Man kan säga att information påverkar mottagaren genom t.ex. ökad förståelse. En annan betydelse är att information är det vi har kunskap om och att data är representationen av denna kunskap.

Exempel: Ett barns ålder är fyra år. Normalt representerar vi detta med siffra (4), men vi skulle också kunna använda romerska siffror (IV), streckmarkeringar (||||) eller annat

uttryckssätt som vi enas om. Informationen i sig har inte ändrats i något av dessa förhållanden, även om representationen av datat har gjort det.

Beskrivning av information: ”Information förekommer i många former. Den kan vara tryckt eller skriven, elektronisk lagrad, skickad med post eller elektronisk, visad på film eller muntlig. Oavsett vilken form informationen har, eller på vilket sätt den överförs eller lagras, bör den alltid ha ett godtagbart skydd.” [3]

Informationsbehandling: ”Datorbehandling av information, informationsbehandling, är ett samlingsbegrepp för alla former av insamling, lagring, distribution och bearbetning av information för att få ny, eller mer användbar, information.” [1]

”Tillgång till information är oumbärligt för en organisations verksamhet och måste följaktligen få ett lämpligt skydd. I en allt mer integrerad affärsvärld så blir det allt viktigare och viktigare att skydda information.” [3]

Ett av de problem som finns med information är att ta reda på om information har olovligt beskådats, kopierats eller ändrats. En person skapar t.ex. en kopia av information när han stjäl den. Vilket medför att originalet är kvar och uppvisar inga tecken på att vara stulen.

2.2 Informationssäkerhet

2.2.1 Historia

Kommunikation har alltid funnits mellan människor. Informationen som utbytts har ibland behövts skyddats från andra människor som inte ska ta del av informationen. I andra fall har anteckningar eller andra typer av informationsbärare behövt skyddas. I det gamla Grekland använde historiken Herodotos (484 BC - 425 BC) en metod för överföring av information. Han rakade en slavs huvud och tatuerade in meddelandet på huvudet. Slaven fick sedan när håret växt ut igen gå med meddelandet till dess mottagare. Han använde denna metod för att göra revolt mot perserna. [5]

Gaius Julius Caesar (100 BC - 44 BC) kom på den berömda Ceasarchiffern. Ceasarchiffern pratas det om än idag.

Postväsendet infördes runt 1600 - 1700 talet och med det blev säkerhet för de brev som skickas också infört eftersom breven skickades av, för sändarna okända personer. Säkerhetsåtgärden var att regeringar införde hårda straff för den som öppnade försändelser. [5]

Nästa steg i utvecklingen var när telegraferna började komma. Både elektriska och optiska telegrafer användes för att skicka meddelande över stora avstånd. Ett problem var då att alla meddelanden som skickades, blev tvungna att läsas av de personer som skötte om telegrafen där meddelandet skickades. För att motverka detta skrevs meddelandet som skulle skickas på ett hemligt språk som parterna kommit överens om.

År 1876 uppfinner Alexander Graham Bell telefonen och televäxel systemet växer fram. All hantering av samtal sker manuellt, vilket innebär att operatören kan avlyssna samtalet. [4]

När datorerna gjorde sitt intågande i historien började en ny era av informationssäkerhet. I början så användes hålkort för informationslagring och dessa fick bara hanteras av vissa personer. Allt eftersom datorn utvecklades kom det fram nya sätt att hantera information på. Internet växte fram och med det kom nya sätt att skicka information mellan olika platser på jorden. Internet har infört ökad tillgång på information och med det även infört större krav på säkerheten kring den information som skickas.

Informationssäkerhet har alltid varit viktig, men nu när hela samhället är ett informationssamhälle är säkerheten viktigare än någonsin. Idag är det materiella värdet på många produkter bara en bråkdel av det totala värdet. Det största värdet är kunskapen som finns inbyggd i produkten. En mobiltelefon kostar kanske tio kronor att tillverka, men bakom ligger mångmiljonbelopp i utvecklingskostnad. Om utvecklingsinformationen kommer ut, den information som företaget har lagt ner miljoner på att ta fram kommer ut, är det ren katastrof. Informationssäkerheten är med andra ord en av de viktigaste sakerna för företag och privat personer. Det finns många olika sätt att hantera information idag, CD-skivor, USB-minnen osv. Säkerheten kring information måste eller bör vara så pass bra att ingen obehörig kan ta del av den. Tyvärr kan man konstatera att så är inte fallet. I takt med att datorerna utvecklas och används mer i olika delar av vår vardag kommer informationssäkerhetsarbetet att vara en viktig fråga även i framtiden.

2.2.2 Definition av informationssäkerhet

Definition av informationssäkerhet: ”Informationssäkerhet är säkerhet rörande informationstillgångars önskade tillgänglighet, sekretess, riktighet, spårbarhet och oavvislighet.” [1]

Informationssäkerheten gäller alla informationstillgångar. Informationssäkerhet innefattar all information som har med företaget att göra. Informationssäkerhet kan beskrivas i tre områden:

1. Fysisk säkerhet

   Med fysisk säkerhet menas de säkerhetsåtgärder som oftast ger upphov till fysiska skydd. Ett serverrum med begränsad tillgång är ett exempel på en fysisk säkerhetsåtgärd för en eller flera servrar.
2. Logisk säkerhet

   Regler och processer för hantering av information eller hantering av objekt hör till den logiska säkerheten. Ett exempel på detta är hur ett företags otillåtna händelser skall hanteras.
3. Systemsäkerhet.

   Systemsäkerhet handlar om datorsystem och nätverk osv. Virusskydd är ett bra exempel på en systemteknisk säkerhetsåtgärd.

”Informationssäkerhet uppnås genom att lämpliga skyddsåtgärder införs, inklusive riktlinjer, processer, organisation samt program- och maskinvarufunktioner. Dessa åtgärder behöver utformas, införas, övervakas, granskas och förbättras, där så krävs, för att säkerställa att organisationens specifika säkerhets- och verksamhetsmål uppnås.” [3]

2.3 Spårbarhet

Det finns två olika områden inom spårbarhet. På engelska heter dessa områden traceability [9] och accountability [26]. Det engelska ordet traceability motsvaras av svenskans spårbarhet. Traceability syftar på fullständighet av information i varje steg av processkedjan och accountability syftar på ansvar hos individen. Dvs. att det varje personer gör ska kunna spåras tillbaka till personen i fråga. Accountability motsvarar svenskans oavvislighet.

Definition av oavvislighet: ”Oavvislighet innebär att ett specifik åtagande eller en utförd handling i efterhand inte skall kunna förnekas av utföraren.” [1]

I denna rapport kommer oavvislighet inte att ingå mer detaljerat.

Definition av spårbarhet: ”Spårbarhet innebär att i efterhand entydigt kunna härleda specifika aktiviteter eller händelser till ett identifierat objekt, oftast en användare.” [7]

Konstaterande av spårbarhet: ”Spårbarhet: att vissa eller alla aktiviteter i ett system ska kunna härledas till en användare.” [6]

”Skyddsmekanismer som autentisering och auktorisation bildar grundskyddet som används för skydd av ett system, en applikation eller liknande. När skyddsmekanismerna inte fungerar, när en säkerhetsöverträdelse eller IT-incident är ett faktum, måste man ha det näst bästa alternativet – att kunna spåra vad som inträffat, vem som gjorde det som genererade spårdatat och, när detta har inträffat”. [1]

I denna uppsatts tolkas spårbarhet som att man ska kunna härleda vad som har hänt. Detta gäller alla olika områden inom informationssäkerhet. Dvs. de fysiska, logiska och systemtekniska delarna av ett informationssystem.

2.4 Vad är ett informationssystem?

”Ett informationssystem är ett system som behandlar, d v s insamlar, bearbetar, lagrar och distribuerar information. Innefattar såväl ett systems tekniska utrustning som dess mänskliga aktiviteter och rutiner.” [11]

Ordermottagning, lagerbokföring, fakturering, platsbokning, flygresor, medicinska behandlingar, personaladministration, banksystem är alla olika exempel på informationssystem.

Mätning på informationssäkerhet görs på ett företags informationssystem. Inom detta stora informationssystem finns det oftast mindre informationssystem där mätning av säkerhet är möjlig.

2.5 Exempel på ett informationssystem

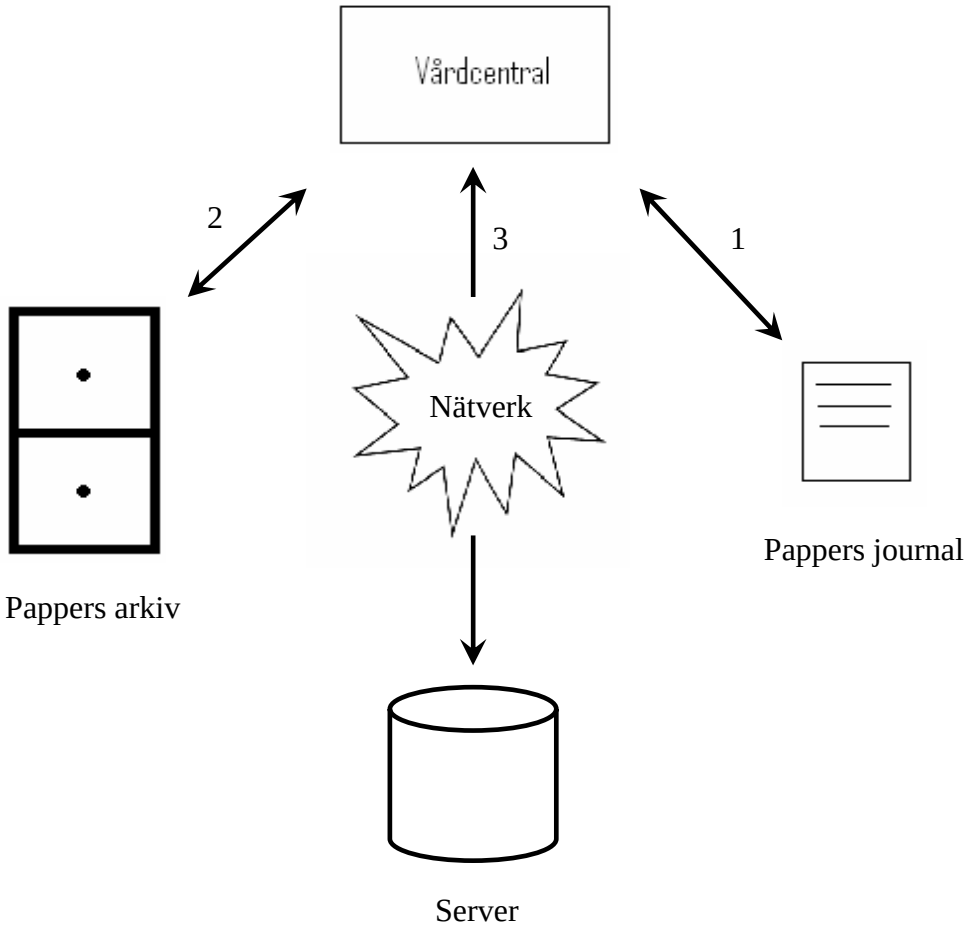
Ett bra exempel på ett informationssystem är en vårdcentral (VC). På en VC finns det journalhantering både i form av pappershandlingar och digitaljournaler. Det finns även lagring av alla pappersjournaler i ett speciellt rum med olika arkivskåp. Digitala journaler lagras på en server. All information skall sedan på något sätt vidare. Recept skall elektroniskt till Apoteket. Remisser skall till sjukhuset och provsvar skall tillbaka till journalerna osv.

2.5.1 Begrepp

I detta exempel kommer två begrepp att användas, objekt och sekundärt objekt. Ett objekt är en bärare av information. En cd-skiva är ett objekt, även ett vanligt papper med information på är ett objekt. Exempel på objekt: papper, server, nätverk

Ett sekundärt objekt är en teknisk skyddsåtgärd som behöver egna skyddsåtgärder. Några exempel på sekundära objekt är: arkivskåp, serverlokal och brandvägg.

2.5.2 Exempel på ett informationssystem



Figur 2.1: Bild av ett VC scenario

I figur 2.1 finns det flera olika objekt. Pappersjournalen, nätverket och servern är alla objekt. Dessa objekt kräver olika skydd. Pappersjournalen kräver logiska skyddsåtgärder. Servern och nätverket kräver systemsäkerhetsåtgärder. Pappersjournalen kräver även en fysisk skyddsåtgärd i form av ett arkivskåp. Jag kommer att gå igenom exempel på skyddsåtgärder för pilarna 1, 2 och 3 nedan.

Logisk skyddsåtgärd (1)

Pappersjournalen har logiska skyddsåtgärder i form av signering. Alltså regler som beskriver hur och när pappret ska signeras. Pappersjournalen måste enligt lag i Sverige signeras och detta är en spårbarhetsåtgärd eftersom man i efterhand enkelt kan gå tillbaka och se vilken läkare som senast signerade journalen. Eftersom signeringen inte är någon teknisk

åtgärd så finns det inget sekundärt objekt. Man behöver inte skydda pennan som signaturen görs med. Logisk skyddsåtgärd är i detta fall reglerna for signering.

Fysisk skyddsåtgärd (2)

Arkiveringsskåpet är en fysisk skyddsåtgärd för pappersjournalen. Skåpet blir ett sekundärt objekt eftersom det kräver skydd i sig. Om man skyddar servern med ett serverrum så blir serverrummet en fysisk skyddsåtgärd.

Systemskyddsåtgärd (3)

För att skydda nätverket användes en brandvägg. Brandväggen är en systemskyddsåtgärd. Även antivirusprogram på datorerna är en systemteknisk skyddsåtgärd. Båda dessa säkerhetsåtgärder är sekundära objekt eftersom dem kräver uppdateringar och tillsyn.

2.6 Veriscans modell

Denna tabell visar Veriscans olika informationssäkerhets nivåer. Företag kan välja i Veriscans produkt vilken av dessa fem nivåer dem vill ha utvärderad. [8]

Veriscan 1	Ingångsnivå för organisationer som vill få snabb överblick över väsentliga faktorer för att nå en god informationssäkerhet.			
Veriscan 2	Nivån är lämpad för organisationer med höga krav på att system och kommunikationer fungerar utan avbrott.			
Veriscan 3	Nivån är framtagen för organisationer som eftersträvar att följa LIS, klassa information och system samt har höga krav på sekretess.	X	X	X
Veriscan 4	Nivån är anpassad för organisationer som förutom höga krav på tillgänglighet och sekretess även har ett uttalat behov av hög grad av spårbarhet i de transaktioner som utförs i system och kommunikationer.	X	X	X
Veriscan 5	För företag och myndigheter där säkerhetsaspekten är helt central.			
		Logisk	Fysisk	System

Tabell 2.1: Veriscans modell.

Veriscan 1 är den nivå som innefattar det som krävs för en god informationssäkerhet och Veriscan 5 är en nivå på informationssäkerhet som gör att säkerhetsaspekten är central för företaget. Denna rapport kommer att undersöka säkerhetsaspekter inom Veriscan 3 och Veriscan 4, samt att avgränsningen gör att arbetet hamnar inom systemtekniska delen. I mån av tid kommer fysiska och logiska åtgärder att tas upp.

2.7 Överblick

I detta kapitel har definitioner på information, informationssäkerhet och spårbarhet förklarats. Definitionen av spårbarhet kommer att vara den centrala knutpunkten i hela denna uppsats. I kapitlet gick Veriscans modell igenom, och med den modellen visades inom vilka ramar denna uppsats kommer att undersöka spårbarhet.

Fysisk säkerhet, logisk säkerhet och systemsäkerhet har förklarats och det har även getts ett exempel på ett informationssystem där dessa begrepp får en mer bildlig förklaring.

3 Teoretisk genomgång av olika säkerhetsåtgärder

Denna uppsats ska förklara vilka säkerhetsåtgärder som innehåller spårbarhet eller har spårbarhet som följd. För att få fram vilka objekt som skulle undersökas inom ett informationssystems systemtekniska del ställdes tre frågor:

1. Vilka objekt är spårbara?
2. Vilka hot finns det mot objektet?
3. Vilka skyddsåtgärder finns det mot dessa hot?

Efter att ha ställt dessa frågor började det framträdda fyra stycken objekt. Anledningen var att ta fyra objekt som skulle kunna finnas inom varje informationssystem och därför blev objekten:

1. Arbetsstation
2. Server
3. Nätverk
4. Databas

Dessa fyra objekt finns nästan inom varje informationssystem hos företag och det verkade därför logiskt att ta dessa. I bilagorna A, B och C finns dessa objekt listade i tabeller. Tabellerna är uppdelade i hot och lösningar för hoten. Dessa tabeller användes som grundmaterial för detta kapitel. I tabellerna finns det en kolumn för spårbarhet. Denna kolumn kan vara numrerad 0, 1 eller 2. Detta är ett system för att se vilka säkerhetsåtgärder som bidrar till spårbarhet. Skalan är sådan att: 0 betyder ingen spårbarhet, 1 är spårbarhet kan finnas och 2 är att spårbarhet finns.

I detta kapitel kommer några av tabellerna från bilagorna A, B och C att gås igenom för att skapa en bild av vilka olika huvudområden det finns inom spårbarhet. Tabellerna som tas upp kommer att få en djupare förklaring där hoten och lösningarna till hotet kommer att förklaras.

Genomgång av tabellerna ger möjligheter att hitta olika huvudkategorier för spårbarhet. Dessa huvudkategorier kommer att få en djupare förklaring i kapitel 4.

3.1 Objekt: Arbetsstation och server

Arbetsstation och server är två objekt som är väldigt lika i hot och lösningar, därför har dessa två lagts ihop. En arbetsstation kan exempelvis vara en stationär dator. En server kan exempelvis vara en: filserver eller e-post-server. Skillnaden mellan en stationär dator och en server är att på servern lagras information från många användare medan en arbetsstation oftast bara har information från en användare. Detta innebär att servern är mer utsatt för informationsstöld och/eller modifierings hot än en arbetsstation.

3.1.1 Hot: Skadlig kod

Skadlig kod: Skadlig kod är kod som utför skadliga/otillåtna operationer på ett system. Koden finns i program, instruktionssekvens eller också kan koden vara självreproducerande.

Exempel på skadlig kod är virus och maskar.

Ett virus är ett datorprogram som sprids genom att lura användare att starta det. Vanligen sprids virus genom en bifogad fil till e-brev med någon rubrik som gör den intet ont anande användaren mycket nyfiken [9][27]. Viruset kan efter öppning utföra olika negativa operationer som exempelvis:

Ta bort information.
Förstöra hårdvara.
Flytta filer till andra platser.
Skicka sig själv vidare till alla e-post kontakter.
Skicka vidare information som finns på datorn.

ILOVEYOU var ett sådant virus. E-postläsarna öppnade den fil som skickades med brevet och viruset aktiverades. Viruset skickade sig själv vidare till alla kontakter i adressboken. Total kostnaden för att åtgärda denna virus attack var 7 miljarder kronor.

En mask är en form av självreplikerande datorprogram som själv sprider sig från dator till dator över Internet. På grund av detta är maskar oftast beroende av säkerhetshål för att kunna

spridas vidare. Genom att masken inte exekveras av någon användare så måste masken själv hitta öppningar i exempelvis en brandvägg för att kunna infektera ett företag. [7][27]

Code Red är en känd mask som spred sig över Internet och attackerade olika servrar. Code Red masken startade en DoS (se kap 3.2.1) attack mot ett antal hårdkodade ip-adresser, bland annat Vita huset. Detta gjordes efter att Code Red funnits på servern ett tag. I och med att masken väntade så blev DoS attackerna mer omfattande på grund av att fler servrar deltog i DoS attacken. [18]

Lösningen för att stoppa skadlig kod är att filtrera bort den innan den kommer in i systemet och kan börja exekvera sig själv.

Filtrering sker via brandvägg, antivirus, proxy eller e-post filter. Nedan följer förklaringar av varje filtreringsåtgärd.

Skyddsåtgärd	Lösning/ teknisk lösning	Spårbarhet	Sekundärobjekt
Filtrering	Brandvägg	2	Brandvägg
	Antivirus	2	AV program
	Webbfilter	2	
	Proxy	2	Proxy
	E-post filtrering	1	

Tabell 3.1: Skadlig kod kontra lösningar

3.1.2 Lösning: Brandvägg

På en arbetsstation eller en server är brandväggen ett program som används som en kontrollmekanism för nättrafik till och från systemet. En brandväggs uppgift är att fungera som en väktare placerad innan Internet. Denna väktare avgör huruvida de paket som vill passera genom brandväggen till företagets nätverk eller datorn i hemmet skall släppas igenom eller inte. Men omvänt så kan brandväggen också avgöra om trafik som kommer från andra

hållet skall släppas ut eller ej. För att en brandvägg ska klara av att filtrera trafik måste brandväggen jobba efter vissa regler. Dessa regler är bestämda av en systemadministratör eller en användare. Ett exempel på en regel är begränsningen av ftp-trafik. Man kan sätta upp en regel som begränsar hur många datorer i nätverket som kan ta emot publik ftp-trafik. Det kanske bara är en dator som skall kunna göra detta, då släpper vi igenom trafik till den datorn men nekar trafik till de övriga. Inom regelverket kan man vanligtvis använda parametrar såsom IP-adress, portnummer eller program. Det är även vanligt att man specificerar att alla sessioner måste initieras från brandväggens insida. En brandvägg loggar även den trafik som skickas igenom. Loggning är spårbarheten inom brandväggar. [19][9]

3.1.3 Lösning: Antivirus

Ett antivirusprogram är ett program som aktivt och/eller inaktivt finner och tar bort eller reparerar filer som är infekterade av datorvirus. Detta beror på vilket antivirus program man skaffar. Alla antivirusprogram har olika metoder att detektera virus. Vissa söker igenom alla nya filer som skapas, andra kanske gör en genomsökning varannan timme på datorns lagringsutrymme. De flesta antivirusprogram kan även upptäcka och oskadliggöra andra former av skadlig kod. För att antivirusprogrammet ska ha möjlighet att detektera nya varianter av virus så uppdateras definitionsfilen regelbundet, vilket ofta sker automatiskt. Ett antivirusprogram lagrar information om vilka filer som programmet har undersökt efter virus och även vilka filer som har blivit borttagna på grund av virus. Denna information lagras i antivirusprogrammets loggar över genomsökningar. Ett antivirusprogram ger även felmeddelanden om ett virus har upptäckts på exempelvis en diskett eller i ett e-post meddelande. Loggning och felmeddelanden är spårbarheten i antivirusprogram. [27]

3.1.4 Lösning: Webbfilter

Skadlig kod kan inkomma på annat sätt än via e-post, exempelvis via webben. Tyvärr så kan man inte lika smidigt virusskanna centralt då responstidskraven är helt annorlunda. Dessutom sker en hel del trafik krypterad och är således svår att skanna. Nu för tiden är den troligaste anfallsvägen inte via bilagda filer utan troligare webbsidor som utnyttjar svaghet i exempelvis java/javascript/active-x/webbläsare. Lösningen på detta problem är att exempelvis

stänga av active-x på sidor som man inte litar på och sedan ställa på det igen på säkra sidor. Ett webbfilter hjälper till med att kontrollera vilka sidor som är säkra och vilka som är osäkra. I ett webbfilter kan man även ställa in sidor som webbläsaren inte ska ha tillgång till. Man låser exempelvis tillgången till vissa sidor med visst innehåll. Ett webbfilter loggar all trafik som sker på Internet för användaren. Genom denna loggfil kan man ta reda på vilka sidor en person varit inne på eller vilka program som en person laddat ner från Internet. Loggning är spårbarheten inom webbfiltrering. [27]

3.1.5 Lösning: Proxy

En proxy är en mellanhand mellan två kommunicerande parter. Proxy gör så att det är möjligt att olika nätverkstjänster tillåter klienter att göra indirekta nätverksanslutningar till andra nätverkstjänster. Med hjälp av en proxyserver kan man stänga av olika platser på Internet som olika webbsidor, online spel mm.

En klient ansluter till proxy-servern, sedan vill klienten ha en anslutningsfil eller annan resurs som är tillänglig på en annan server. Proxyservern tillhandahåller tjänsten genom att ansluta till den andra servern. Eftersom en proxy används som en mellanhand mellan två kommunicerande parter, ligger spårbarheten i loggningen av trafik mellan dessa två parter. [21][9]

3.1.6 Lösning: E-postfilter

E-postfilter eller spamfilter är ett program som har till uppgift att automatiskt skilja skräppost (även kallat spam) från önskad e-post. Skräppostfilter kan köras på såväl enskilda persondatorer som e-postservrar. Filter på servern överlåter administrationen till den som underhåller e-postservern. Det kan vara svårt att avgöra om värdepost av misstag sållats bort som skräppost därför är e-postservrars filter ganska restriktiva. [27]

Det finns numera företag som säljer uppdaterade listor på kända spamkällor, vilket fungerar bra.

Några av dessa lösningar kommer att behöva skydd för sig själva, exempelvis en brandvägg måste skyddas från angrepp utifrån. När en teknisk lösning på ett hot kräver skydd

så blir det ett sekundärobjekt. Sekundär objekt och deras skyddsåtgärder finns listade i Bilaga D. För att se alla hot och skyddsåtgärder för objekten arbetsstation & server se Bilaga A.

3.1.7 Hot: Incidenter inom företaget

En incident är en oväntad händelse inom ett företagssystem. Den oväntade händelsen behöver påverka systemet i den grad att en farlig situation kan uppstå. Säkerhets luckor som utnyttjas klassas även som incidenter.

Med incidenter menas exempelvis:

1. Någon tar information från företaget och säljer till annat företag (spion)
2. Av misstag råkar någon inom företaget stänga av filserver så ingen annan på företaget kommer åt den.
3. Någon öppnar avsiktligt eller oavsiktligt portar i företagets brandvägg så en attack utifrån är möjlig.
4. Någon laddar ner ett virussmittat program till sin dator som infekterar företaget.

Inom företaget menas: anställd som avsiktligt eller oavsiktligt använder/utnyttjar/stjäler företagets resurser.

För att lösa hot som begås av anställda, vare sig om det är avsiktligt eller oavsiktligt måste att antal åtgärder läggas in i systemet. Idén är att begränsa anställdas möjligheter till att göra misstag som leder till incidenter. Även att se till så anställda måste göra eventuella olagligheter från sina egna konton i företagets nät så att personen och händelsen går att spåra. Det handlar även om att lägga in rutiner för säkerhetskopieringar så att om en anställd lyckas ta bort något går det att få tillbaka. Nedan förklaras de åtgärder som är listade i tabellen 3.2 .

Skyddsåtgärd	Lösning/ teknisk lösning	Spårbarhet	Sekundärobjekt
Övervakning av trafik	HIDS (Host Intrusion Detection System)	2	
Rättigheter/Åtkomst	Konfiguering via GPO (group policy)	0	
Regler för användning	Policys	0	
Inloggning	Unika ID	2	
	Lösenordsdesign	0	
Kontohantering	Account management	1	Management program
Övervakning av objekt	System Management	1	Management program
Säkerhetskopiering	Manuell säkerhetskopiering	1	Lagringsmedia
	Backuprobot	0	Lagringsmedia
Skydd mot annan användare	CTRL-ALT-DEL (Ny inlogg)/Lås maskin	0	

Tabell 3.2: Incidenter inom företaget kontra lösningar

3.1.8 Lösning: HIDS

HIDS (Host Intrusion Detection System) är en form av IDS (Intrusion Detection System). IDS är ett intrångsdetekteringssystem som används för att upptäcka intrång eller intrångsförsök i ett system. HIDS existerar på själva systemen som övervakare, HIDS övervakar exempelvis loggfiler och processer. Spårbarheten i HIDS ligger i spårgenerering vid en eventuell attack och lagring av information om attacken, vart den kommer ifrån, hur den kom in, vad den gör. [22][24]

3.1.9 Lösning: GPO

GPO (Group policy) är en Microsoft teknologi där man ger olika grupper av användare olika rättigheter. Varje användare får en grupp som den tillhör och får då samma rättigheter som alla andra i gruppen. Inom GPO finns det övervakning av användare. GPO övervakar exempelvis login, logut och mjukvaruinstallationer.

GPO finns i Windows 2000, XP, Vista, server 2003. [28]

3.1.10 Lösning: Inloggning

För att inloggningen ska fungera enkelt och smidigt bör varje anställd ha ett unik ID som han/hon loggar in med på företagets system. Genom att varje person har unika ID är spårbarheten lättare eftersom varje ID i loggen direkt kan kopplas till en unik användare av systemet.

Genom att ha lösenordsdesign gör man det svårt att ta reda på lösenord för andra användare i systemet. I lösenordsdesign beskrivs det hur ett lösenord ska skapas. Det finns även kontroller av lösenorden faktisk är skapade på ett korrekt sätt.

Ett bra lösenord ska:

1. Ha både stora och små bokstäver.
2. Ha både siffror och/eller specialtecken.
3. Vara lätta att komma ihåg så man inte behöver skriva ner lösenordet någonstans
4. Vara minst sju eller åtta tecken långt.
5. Kunna skrivas fort så ingen annan hinner se.

Bra lösenord hjälper till att förhindra brott inom företaget. En anställd måste göra eventuella olagligheter från sitt eget konto och då blir det lättare att spåra vad han/hon har gjort. [26]

3.1.11 Lösning: Kontohantering

Account management eller kontohantering är det program som skapar/ändrar/tar bort konton för användare av systemet. Även rättighets- och åtkomstinställningar görs via account management. Account management ger användare, efter att ha identifierat sig med användarnamn och lösenord, tillgång till privat data (exempelvis e-post) och egna

inställningar. Kontohanteringsprogram sparar undan alla ändrade inställningar på konton så att det i efterhand går att se om personer har utnyttjat sina rättigheter. Denna information lagras i antingen loggfiler för programmet eller i krypterade filer på systemet.

3.1.12 Lösning: Övervakning av objekt

System management är övervakning av själva objektet (i detta fall antingen en dator eller server). Vilka processer som är igång, hur mycket CPU kraft som används, hur mycket ledigt minne som finns på diskar mm. I Windows har man aktivitetshanteraren som ett exempel på ett program som sköter viss övervakning. Aktivitetshanteraren övervakar CPU, processer och nätverkstrafik. Dock så varnar det inte om något skulle vara fel. Övervakningsprogram av exempelvis grafikkort och CPU-temperaturer varnar när temperaturen når en kritisk nivå. Ett övervakningsprogram ska/bör ha varningar och felmeddelanden inbyggda så att användaren vet om något gått fel. Dessa felmeddelanden är det första spår man undersöker vid fel eftersom felmeddelandet innehåller information om vad det var som hände. [16][17]

3.1.13 Lösning: Säkerhetskopiering

Säkerhetskopiering innebär att man spara viktiga filer i en extra kopia som senare kan återställas om originalet skadas eller försvinner. Säkerhetskopior lagras oftast på ett medium frånskilt det medium originalet kopieras från. Det finns olika sätt att utföra säkerhetskopiering. Det kan göras manuellt eller via en robot. Roboten är en automatiserad rutin som exempelvis kör säkerhetskopiering av servrar en gång om dagen. Detta kan ställas in efter behov. Med manuell säkerhetskopiering menas att en person utför det arbete som roboten skulle ha gjort. Skillnaden mellan en manuell säkerhetskopiering och att en robot gör det, är att roboten är programmerad vad den ska kopiera men personen som utför den manuella säkerhetskopieringen kopierar det som är viktigt för stunden. Om en person utför en säkerhetskopiering av systemets information vet man vilken person det var och kan spåra denna person om det skulle vara något fel på informationen som säkerhetskopierades.

3.1.14 Lösning: Skydd mot annan användare

Med skydd mot annan användare menas att man lägger in rutiner för låsning av system när man inte är där. Ett exempel är att låsa arbetsstationen när man går ifrån den och kräva en ny inloggning när man kommer tillbaka. Det bidrar till att ingen annan kan göra olagligheter på en annan användares konto och återigen måste en användare som vill göra olagligheter göra det från sitt eget konto.

Sekundär objekt för tabell 3.2 och deras skyddsåtgärder finns listade i Bilaga D. För att se alla hot och skyddsåtgärder för objekten arbetsstation och server se Bilaga A

3.2 Objekt: Nätverk

I objektet nätverk ingår hårdvara som routrar, switchar och brandväggar. Även trafiken mellan dessa enheter ingår. Inom nätverket måste både enheter och trafik övervakas och skyddas. I nätverket finns servrar och arbetsstationer inkopplade. Det finns även databasservrar och e-postservrar inkopplade. Nätverket är det största området som behövs skyddas inom ett företag och därför förmodligen det viktigaste.

3.2.1 Hot: DoS

DoS står för Denial Of Service och är överbelastningsattack mot ett system. Syftet är att inte någon annan får tillgång till systemet. För att utföra en DoS attack finns det tre möjliga tillvägagångssätt:

1. Att man missbrukar/utnyttjar en sårbarhet eller svaghet som får systemets programvara att krascha.
2. Att man sänder (överbelastar) så mycket trafik att systemet eller applikationerna kollapsar.
3. Att man sänder så mycket skräptrafik så att legal/giltig trafik hindras att komma fram.

Det finns inte mycket man kan göra mot DoS attacker. Dels är det så att om man märker att en attack har börjat så går det inte att stoppa den. En DoS attack brukar gå tillväga så att det skickas en request till en server där sändarens adress är modifierad att peka på någon annans adress. Genom att skicka en massa request till olika servrar så börjar målet att överflödas med anslutningar och data. För att stoppa en DoS attack måste den som blir utsatt ta kontakt med de servrarna som skickar information och säga till deras administratörer att avbryta sina sändningar. Om man som attackerare då har skickat sin request till 10 000 servrar så finns det inte mycket att göra för att stoppa attacken. Offret måste ta kontakt med 10 000 olika administratörer för attackerande servrar ska sluta skicka information.

Det man kan göra är att se till så Dos attacken inte gör så mycket skada på verksamheten. Dels genom uppdateringar och säkerhetskopior, men även genom att ha övervakningsprogram som hela tiden varnar om belastningen blir för hög så man kan stänga av sitt system. [24][27]

Skyddsåtgärd	Lösning/ teknisk lösning	Spårbarhet	Sekundärobjekt
Incidenthantering	Policy för incidenthantering	0	Dokument
Övervakning av objekt	System Management	1	Management program
Övervakning av trafik	Network Management	1	Management program
	HIDS, NIDS	2	
Säkerhetskopiering	Manuell säkerhetskopiering	1	Lagringsmedia
	Backuprobot	0	Lagringsmedia

Tabell 3.3: DoS kontra lösningar

3.2.2 Lösning: Incidenthantering

Incidenthantering handlar om hur man ska hantera en incident när den väl har inträffat. Några exempel på punkter som ska finnas med i en incidenthanteringspolicy:

Hur man ska gå tillväga för att åtgärda problemet.

Hur efterarbetet ska gå till i form av spårning och efterforskning. [15]

3.2.3 Lösning: Övervakning av objekt

System management är övervakning av själva objektet (i detta fall handlar det om exempelvis routrar, switchar och filservrar). Vilka processer som är igång och varnar om det är någon process som inte ska vara igång men som ändå är det. Om det på en filserver helt plötsligt startar en process som heter trojan.exe skickas det en varning till lämplig system administratör som sedan får ta lämpliga åtgärder. Man kan bygga in system management i network management. Varningar och felmeddelanden är spårgenererande och ingår därför i spårbarhet. [16][17]

3.2.4 Lösning: Övervakning av trafik

Network Management är ett program som konstant övervakar ett nätverk för att detektera långsamma och/eller kraschade system. Ett network management program övervakar även trafiken inom nätverket samt nätverksenheter som exempelvis routrar, switchar och brandväggar. [16][17]

Exempel**:** Det är lunchtid på en tisdag. Företagets e-handelsplats går ner då webbservern kraschar. Med hjälp av ett övervakningsprogram skickas ett SMS direkt till IT-chefen och ansvarig tekniker som löser problemet och företaget minimerade affärsförlusten. I detta exempel var det SMS som skickades ett felmeddelande. Vid en senare analys börjar analysarbetet med att ta reda på hur det kunde hända. SMSet var det första spåret vid händelsen.

HIDS (Host Intrusion Detection System) och NIDS (Network Intrusion Detection System) är former av IDS (Intrusion Detection System). IDS är ett program som granskar nätverkstrafik efter kända signaturer eller avvikande fenomen i syfte att identifiera intrångsförsök. Till skillnad från en brandvägg, som också granskar trafiken, är IDS mer intresserad av innehållet i trafiken. En vanlig placering av en IDS är mellan Internet och brandväggen. Det är också vanligt att man placerar IDS på det interna nätverket eftersom många oönskade företeelser kommer inifrån företaget. Om man bara vill ha larm för trafik som verkligen kommer in i nätverket bör IDS placeras innanför brandväggen. Beroende på vart man placerar IDS och hur allvarligt ett intrång skulle vara där, kan systemet ställas in för att larma på olika sätt. Är risken låg kan det exempelvis räcka med att logga händelsen medan mer akuta fall kan innebära att ett system som är kopplat till IDS skickar ett SMS till någon

ansvarig. En IDS är dock bara ett larmredskap och för att säkerheten ska upprätthållas måste eventuella larm följas upp av åtgärder. [22][24][27]

3.2.5 Lösning: Säkerhetskopiering

Precis som för arbetsstation och server innebär säkerhetskopiering att spara viktiga filer i en extra kopia som senare kan återställas om originalet skadas eller försvinner. Skillnaden mellan att säkerhetskopiera i nätverket är att inom nätverk så bör även inställningar av routrar, brandväggar mm, sparas undan så vid eventuellt fel på hårdvara eller mjukvara så går det snabbt att sätta upp en ny och konfigurera den nya enheten.

Sekundär objekt för tabell 3.3 och deras skyddsåtgärder finns listade i Bilaga D. För att se alla hot och skyddsåtgärder för objektet nätverk se Bilaga B

3.2.6 Hot: Intrångsförsök

Intrångsförsök betyder att någon ej anställd försöker ta/ändra/radera information från företaget utifrån, ex hacker. En hacker är en person som excellerar i programmering och som vetgirigt tar till sig program och hårdvara. En hackare använder sina kunskaper till att skaffa fram tillgänglig information om ett system. Genom att analysera eller manipulera systemet försöker hackaren förstå och få kunskap om systemet. Att hacka kräver kunskaper om hur datorer är uppbyggda och hur datorer arbetar med data.

Skyddsåtgärd	Lösning/ teknisk lösning	Spårbarhet	Sekundärobjekt
Filtrering	Brandvägg	2	Brandvägg
	Proxy	2	Proxy
	DMZ	1	
Kryptering	Krypteringsteknik	0	
Övervakning av trafik	IDS, NIDS, HIDS	2	
BKS	ACL i NTFS	0	
	Anv.ID och lösen	2	
Lura attackerare	Honeypot	2	

Tabell 3.4: Intrångsförsök kontra lösningar

3.2.7 Lösning: Brandvägg

I nätverket är brandväggen antingen en hård- eller mjukvaru- komponent som används som en kontrollmekanism av trafik till och från nätverket. Brandväggen kontrollerar all trafik och bestämmer om trafik är behörig eller ej. För att avgöra vilken trafik som är behörig eller ej arbetar brandväggen efter vissa regler. Dessa regler är bestämda av en systemadministratör. I regelverket kan man vanligtvis använda parametrar såsom IP-adress, portnummer eller program. Det är även vanligt att man specificerar att alla sessioner måste initieras från brandväggens insida. Förutom att filtrera trafik till företagets nätverk används brandväggen

till att logga information om den trafik som passeras. Loggning är den spårbarhet som finns inom brandväggar. [9][19]

3.2.8 Lösning: Proxy

En proxy är en mellanhand mellan två kommunicerande parter. Proxy gör så att det är möjligt att olika nätverks tjänster tillåter klienter att göra indirekta nätverksanslutningar till andra nätverkstjänster. Med hjälp av en proxyserver kan man stänga av olika plaster på Internet som olika webbsidor, online spel mm. Eftersom en proxy används som en mellanhand mellan två kommunicerande parter, ligger spårbarheten i loggningen av trafik mellan dessa två parter. [9][21]

3.2.9 Lösning: DMZ

DMZ är förkortning av DeMilitarized Zone, vilket egentligen är datorer eller servrar som måste vara mer eller mindre direkt anslutna till Internet för att fylla sina funktioner. Detta är vanligt förekommande hos företag. Ett DMZ är placerat mellan det externa nätet (Internet) och det interna nätet. DMZ skyddas av samma brandvägg som det interna nätet men brandväggen tillåter mer trafik in till DMZ. Att exponera servrar mot omvärlden är ett måste för att vissa funktioner ska fungera som exempelvis externa webbservrar, FTP, DNS och e-postservrar. Servrar som placerats i ett DMZ måste anses vara utsatta för alla typer av attacker och ska därför inte innehålla någon funktion som inte absolut behövs för uppgiften eftersom varje extra funktion innebär ökad sårbarhet. Normalt används samma intrångsskydd mellan ett DMZ och det interna nätet som till Internet.

Man kan placera e-postservern innanför DMZ istället. Fördelen med detta är att intern e-post inte behöver gå via brandväggen vilket innebär mindre belastning på brandväggen. En nackdel är att men inte får den loggning som sker via brandväggen.

Genom detta resonemang kan man placera flera olika servrar i DMZ för att få den loggning som brandväggen gör. Tyvärr så kan man inte placera alla servrar i DMZ för servrarna är sårbara i DMZ. [9][20][21]

3.2.10 Lösning: Kryptering

Kryptering av trafik som sker på nätverket hjälper mot eventuella attacker mot trafiken. Exempelvis en hacker som ligger och lyssnar av trafiken inom nätverket. Genom att kryptera all trafik inne i nätverket blir all den information som stjäls från företaget oanvändbar för andra utanför företaget som inte har dekrypteringsnyckeln. [26]

3.2.11 Lösning: Övervakning av trafik

HIDS (Host Intrusion Detection System) och NIDS (Network Intrusion Detection System) är former av IDS (Intrusion Detection System). IDS är ett program som granskar nätverkstrafik efter kända signaturer eller avvikande fenomen i syfte att identifiera intrångsförsök. Till skillnad från en brandvägg, som också granskar trafiken, är IDS mer intresserad av innehållet i trafik. En vanlig placering av en IDS är mellan Internet och brandväggen. Det är också vanligt att man placerar IDS på det interna nätverket eftersom många oönskade företeelser kommer inifrån organisationen. Om man bara vill ha larm för trafik som verkligen kommer in i nätverket bör IDS placeras innanför brandväggen. Beroende på vart man placerar IDS och hur allvarligt ett intrång skulle vara där, kan systemet ställas in för att larma på olika sätt. Är risken låg kan det exempelvis räcka med att logga händelsen medan mer akuta fall kan innebära att ett system som är kopplat till IDS skickar ett SMS till någon ansvarig. En IDS är dock bara ett larmredskap och för att säkerheten ska upprätthållas måste eventuella larm följas upp av åtgärder. [22][24][27]

3.2.12 Lösning: BKS

BKS står för behörighet- och kontrollsystem och hanterar användar-ID och lösenord samt vilken grad av åtkomst till informationsobjekt en person i systemet har. BKS har även hand om rollhantering inom systemet. ACL som betyder access control list, finns inom NTFS. ACL är rättigheter på exempelvis filer eller mappar. Detta går att ställa in i NTFS.

3.2.13 Lösning: Inlogging och lösen

För att inloggningen ska fungera enkelt och smidigt bör varje anställd ha ett unik ID som han/hon loggar in med på företagets nätverkssystem. Genom att varje person har unika ID är spårbarheten lättare eftersom varje ID i loggen direkt kan kopplas till en unik användare av systemet.

Genom att ha en bra lösenords design så gör man det svårt att hacka tills sig lösenord för användare i nätverket.

Ett bra lösenord ska bestå av:

1. Ha både stora och små bokstäver.
2. Ha både siffror och/eller specialtecken.
3. Är lätta att komma ihåg så man inte behöver skriva ner lösenordet någonstans
4. Är minst sju eller åtta tecken långt.
5. Kan skrivas fort så ingen annan hinner se.

Genom att ha bra lösenord förhindras brott inom företaget. En anställd måste göra eventuella olagligheter från sitt eget konto och då blir det lättare att spåra vad han/hon har gjort. [26]

3.2.14 Lösning: Honeypot

En honeypot är en avancerad fälla som är designad för att lura till sig obehörig personer som försöker utnyttja systemet. Honeypot är till för att detekterar och i vissa fall motverkar intrång. En honeypot kan vara i olika former som exempelvis filserver eller oskyddade trådlöst nät. En honeypot är ett system eller ett nätverk med kända sårbarheter som ser attraktiva ut för hackare eller andra ovälkomna attackerande gäster. En honeypot har inget riktigt syfte och därmed ej heller en legitim aktivitet, så om någon försöker interagera med den, är det med stor sannolikhet enbart för att utföra olagliga och förstörande aktiviteter. Anslutningen kontrolleras noggrant av administratörerna. Honeypoten samlar in data som kan användas för att hitta nya taktiker och verktyg som hackarna använder samt även spåra dem. [29]

Sekundär objekt för tabell 3.4 och deras skyddsåtgärder finns listade i Bilaga D. För att se alla hot och skyddsåtgärder för objektet nätverk se Bilaga B

3.3 Objekt: Databas

Det finns flera olika former av databaser och för att kunna göra en korrekt hotbild mot databaser har en begränsning gjorts mot Oracle databaser. Många av hoten och lösningarna kommer att stämma in på andra typer av databaser. Dock så handlar tabell 3.5 och 3.6 om säkerhetsåtgärder och hot mot Oracle databaser.

3.3.1 Hot: Utnyttjande av standardinställningar

Oracle databaser har ett standardlösenord och ett standardkonto när man installerar databasen. Vid installation skapas en så kallad superanvändare till systemet. Superanvändare har äganderätt till all data i databasen. Namnet och lösenordet till detta konto är oftast standardiserat och om det inte ändras kan obehöriga personer ta sig in via detta konto och ändra information i databasen. Om superanvändarens användarnamn och lösenord inte hanteras varsamt och det kommer till känna för en annan person än administratören så kan denna person ändra hela Oracle databasen. Från superanvändarkontot kan all data i databasen ändras, även alla inställningar för användare av databasen. För att lösa problem med standardinställningar finns det olika lösningar som kommer att listas nedan med en förklaring på varje åtgärd. [23]

Skyddsåtgärd	Lösning/ teknisk lösning	Spårbarhet	Sekundärobjekt
Installationshantering	Mallar för uppsäkring, script	0	Policy
	Kompetent personal	0	
Administratör konto	Lösenordsdesign	0	
Systemkonton	Unika ID	2	
	Lösenordsdesign	0	

Tabell 3.5: Utnyttjande av standardinställningar kontra lösningar

3.3.2 Lösning: Installationshantering

Installationshantering handlar om att installationer av Oracle databaser bör ske av kompentent personal. Vem som helst kan sätta upp en Oracle databas men då blir det standardinställningar, vilket bör undvikas om det går. Genom att ha mallar för hur en installation ska gå till så blir säkerheten mycket högre än om en okunnig person skulle sköta installationen.

3.3.3 Lösning: Unika ID

Oracle har precis som vilket annat system användarnamn och lösenord. Därför gäller samma säkerhet för användarnamn och lösenord som för vilket system som helst. Dvs. att varje systemanvändare ska ha ett unik ID som han/hon loggar in med. Genom att varje person har unika ID är spårbarheten lättare eftersom varje ID i loggen direkt kan kopplas till en unik användare av systemet. Äldre verksamhetssystem har olika ”hårdkodade” användar-ID och lösenord vid SQL-frågor mot databasen. Det unika användar-ID följer inte med vid accesser mot databasen.

3.3.4 Lösning: Lösenordsdesign

Varje systemanvändare ska ha ett bra systemlösenord som gör att det blir svårt att hacka.
Ett bra lösenord ska bestå av:

1. Ha både stora och små bokstäver.
2. Ha både siffror och/eller specialtecken.
3. Är lätta att komma ihåg så man inte behöver skriva ner lösenordet någonstans
4. Är minst sju eller åtta tecken långt.
5. Kan skrivas fort så ingen annan hinner se.

Bra lösen ord hjälper till att förhindra brott inom företaget. En anställd måste göra eventuella olagligheter från sitt eget konto och då blir det lättare att spåra vad han/hon har gjort. [26]

Sekundär objekt för tabell 3.5 och deras skyddsåtgärder finns listade i Bilaga D. För att se alla hot och skyddsåtgärder för objektet databas se Bilaga C

3.3.5 Hot: Mjukvarufel

Programvarufel kan vara när företag har många system som använder exempelvis Oracle databas. Det kan vara svårt att få alla system att samtidigt gå över till samma version av Oracle. När man inte uppdaterar version finns det en stor risk att bugg och säkehetsfixar inte rättas till. Programvarufel kan även vara att olika processer slutar fungera som dom ska. Processer kan sluta fungera genom att dom kräver åtkomst till samma minnesutrymme.

Skyddsåtgärd	Lösning/ teknisk lösning	Spårbarhet	Sekundärobjekt
Metoder	Metod för utveckling/uppgradering	0	
	Test innan produktionssättning	0	Testnät men testutrustning
	Metod för systemimplementation	0	
Systemdokumentation	Användarhandledning till system	0	Dokument
Driftdokumentation	Användarbeskrivning till objekt	0	Dokument
Säkerhetskopiering	Manuell säkerhetskopiering	1	Lagringsmedia
	Backuprobot	0	Lagringsmedia
Övervakning av objekt	System Management	1	Manager programmet

Tabell 3.6: Programvarufel kontra lösningar

3.3.6 Lösning: Metoder

En metod är ett planmässigt tillvägagångssätt för att uppnå visst resultat. Med detta menas inom utveckling och uppgradering att man måste ha en plan att jobba efter. När man uppgraderar en Oracle databas är det mycket som man måste tänka på. Här hjälper det att ha fasta regler för hur man ska gå till väga. Det som många gör är att testa innan man sätter en ny version i skarp drift. I testnätet kontrolleras så att allt funkar som det ska.

3.3.7 Lösning: Systemdokumentation

Systemdokumentation beskriver hur ett system är uppbyggt. Själva dokumentet är till stor hjälp när ett system skall underhållas och vidareutvecklas, dessutom är det ett utmärkt sätt att förbättra kommunikationen under systemutvecklingsarbetets gång. Systemdokumentationen hjälper inte mot programkrascher men hjälper till att få systemet att

fungera igen. Vid en eventuell ominstallation av programmet kan dokumentet hjälpa till genom snabbare installation och rätt konfigureringar. [10]

3.3.8 Lösning: Driftdokumentation

Driftdokumentationen innehåller instruktioner om hur systemet och produkter ska installeras och konfigureras. Även dokumentering av utrustning inom företaget, instruktioner för hur saker fungerar. En driftdokumentation kan även innehålla telefonnummer till leverantörer av företagets resurser. Driftdokumentation är till för den personal som ansvarar för den dagliga driften av ett datasystem.

En uppdaterad driftdokumentation av företagets datanätverk ger ökad trygghet och medverkar till en kostnadseffektiv nätverksdrift. Rätt sammanställd bidrar dokumentationen till kortare driftstopp, lägre konsultkostnader och enklare uppgraderingar. [10]

3.3.9 Lösning: Säkerhetskopiering

Säkerhetskopiering innebär att spara viktig information på ett medium frånskilt det medium originalet kopieras från så det senare kan återställas om originalet skadas eller försvinner. Det finns olika sätt att utföra säkerhetskopiering. Det kan göras manuellt eller via en robot. Roboten är en automatiserad rutin som kör säkerhetskopiering av information en gång i veckan exempelvis, detta kan ställas in efter behov. Med manuell säkerhetskopiering menas att en person utför det arbete som roboten skulle ha gjort. Skillnaden mellan en manuell säkerhetskopiering och att en robot gör det är att roboten är programmerad vad den ska kopiera men personen som utför den manuella säkerhetskopieringen kopierar det som är viktigt för stunden.

3.3.10 Lösning: Övervakning av objekt

System management är övervakning av själva databasen. Hur mycket ledigt minne det finns på diskar och liknande. Ett övervakningsprogram på Oracle ska/bör ha varningar inbyggda så att användaren vet om något gått fel. Dyrare övervakningsprogram har inbyggda rutiner för automatisk felavhjälpning. Programmet klarar enklare omkonfigureringar av minne och tablespace.

Sekundär objekt för tabell 3.6 och deras skyddsåtgärder finns listade i Bilaga D. För att se alla hot och skyddsåtgärder för objektet nätverk se Bilaga C

3.4 Säkerhetsaspekterna

Inom ett informationssystem finns det mycket som behöver sparas. All trafik mellan servrar och persondator, inloggningar på nätverk eller datorer, men även trafik mellan personer är några exempel på information som skulle behöva sparas.

Om exempelvis en hacker försöker eller lyckas ta sig in i ett företags informationssystem så måste företaget se till att hackern lämnar spår efter sig så att det i efterhand går att rätta till det som hände och ta reda på vart attacken kom ifrån. Eventuellt polisanmäla den skyldige om brott begåtts.

I tabellerna i detta kapitel har det tagits upp ett antal olika skyddsåtgärder. Dessa tabeller var en del av de tabeller som finns i bilagorna A, B och C. Det finns även åtgärder som innehåller spårbarhet eller som har spårbarhet som följd. Autentisering har spårbarhet som följd eftersom loggning är enkelt att införa vid in- och ut- loggning på objekt. Åtgärder som brandvägg har redan ett loggningssystem i sig. I båda dessa exempel finns spårbarhet med i olika former. Brandväggen har inbyggt spårbarhet i åtgärden men i autentisering är det en följd av införd åtgärd i och med att in/ut-loggning kan sparas undan i loggfiler. Inom systemdelen av informationssäkerhet är det loggning som står i centrum för spårbarhet.

Eftersom loggning står i centrum för spårbarhet inom det systemtekniska så måste loggningsmekanismer vara så pass bra och noggranna att det i efterhand enkelt går att vandra bakåt i processkedjan för att ta reda på vad som har hänt och hur det hände.

Det finns även spårbarhet inom andra områden som har tagits upp nämligen, övervakning och IDS (Intrusion Detektion System). Inom övervakning finns spårbarhet i form av rapporter och felmeddelanden när oväntade händelser inträffar. Dessa felmeddelanden är det första spåret vid oväntade händelser i system. Detta spår används för att senare analysera hela händelsen.

IDS och övervakningsprogram är inte så olika. Skillnaden är att IDS hela tiden ligger och söker av efter oväntade mönster som eventuellt skulle kunna indikera på en attack. Vid sådana

mönster varnar IDS systemadministratörer som kan stoppa attacken. Vissa IDS system kan även ta beslut om egna åtgärder, dessa kallas för IPS (Intrusion Prevention System).

IDS och IPS sparar även undan information om angriparen så att en analys kan ske vid ett senare tillfälle. Dessa tre huvudområden: loggning, övervakningsprogram och IDS/IPS kommer att gås igenom i mer detalj i kapitel 4.

3.5 Överblick

I detta kapitel har fyra stycken olika objekt listats: arbetsstation, server, nätverk och databas. Anledningen till att just dessa fyra objekt listats är att i stort sett varje företag har dessa fyra objekt i sina informationssystem. Till dessa fyra objekt listades även en mängd med hot och till varje hot ett antal skyddsåtgärder. Detta gjordes för att kunna identifiera vilka skyddsåtgärder som hade spårbarhet som följd eller vilka skyddsåtgärder som redan har spårbarhet inbyggt. I tabellerna i detta kapitel har även ett antal sekundärobjekt listats. Alla sekundärobjekt är listade under Bilaga D. Under Bilaga Där även skyddsåtgärder för sekundärobjektet att listade.

Sist i kapitlet identifierades tre stycken huvudområden som i kapitel fyra kommer att förklaras mer i detalj.

4 Mekanismer för spårbarhet

I detta kapitel kommer mekanismerna som ger eller innehåller spårbarhet beskrivas närmare. De skyddsåtgärderna som har undersökts i denna uppsats finns i bilagorna A, B och C. I kapitel 3 gick några av dessa säkerhetsåtgärder igenom för att hitta några gemensamma nämnare. De som fanns gemensamt för alla åtgärder som innehöll spårbarhet var att antingen spara undan spårdata eller generera spår som senare går att följa. De mekanismerna som tillhandahöll detta var: loggning, övervakning, IDS/IPS.

I detta kapitel kommer loggning att tas upp först. Sedan kommer övervakning att gås igenom. Därefter kommer IDS/IPS att förklaras.

Sist i kapitlet kommer en del om hur man går till väga vid intrång i ett system. I denna del av kapitlet kommer informationsinsamling att gås igenom men även hur information analyseras och vilka steg som finns inom en analysfas.

4.1 Loggning

Loggning betyder att man kontinuerligt samlar in information som sedan kan användas för att spåra en händelse eller följd av händelser. Loggning används även för att samla information om användarmönster och kartläggning av en enskilds användares aktivitet. En loggfils uppgift är att ge information om en händelse eller följder av händelser.

Loggar kan existera på exempelvis routrar, brandväggar, switchar, datorer och servrar. Loggfiler ser olika ut beroende på vart dem kommer ifrån. I Bilaga E finns en loggfil från en Cisco switch. Bilaga F är en säkerhetsloggfil från en Windows XP maskin. Dessa loggfiler skiljer sig mycket åt när det gäller information som fås fram och utseende. I loggfilen från Cisco switchen i Bilaga E får man inte så mycket användbar information. Det man ser är när switchen ändrar state från ”up” till ”down”. När state sattes till ”up” så öppnades porten för trafik och vid ”down” stängdes porten ner. Att man bara ser detta beror på att denna switch bara skickar vidare trafik från en nod i nätverket till en annan nod i nätverket. Switchen går inte in i paketen för att titta på innehållet.

I Bilaga F finns det en säkerhetsloggfil från en Windows XP maskin. Första bilden i Bilaga F visar hur man får fram säkerhetsloggen i Windows XP. Genom att gå in i administratörsverktyg kan säkerhetsloggen öppnas. Dock så gäller det att den är konfigurerad korrekt. I denna logg kan man se tider och vilka personer som har loggat in. I bild två har en rad markerats och det har även tagits fram extra info för händelsen. Händelsen har nummer 528 och det är successful login. Man kan även se vilken tid personen i fråga loggade in.

Bilaga G innehåller en rad från en loggfil hämtad från en brandvägg. Det finns i Bilaga G förklaringar på vad varje element i raden från loggfilen betyder.

Loggningsmekanismer kan ställas in på olika noggrannhet i hur mycket information som ska sparas till loggfiler. Om man exempelvis bara loggar tid, datum och händelse så motsvaras detta av en ganska låg nivå av loggning eftersom väldigt lite information lagras i loggen. Loggfiler måste vara så pass innehållsrika att det inte går att ta miste på informationen som finns. Om man i detta fall hade ökat nivån av noggrannhet i loggningen och haft med exempelvis MAC-address, IP-adress, användar ID, då hade det gått att använda loggen för att i efterhand analysera händelser.

Ju mer man loggar, desto mer data får man, men desto mer plats tar också loggarna upp. Det betyder att loggarna ofta konfigureras att vara avstängda per default, eller logga få saker. Det är ett problem, då det som inte loggas, heller inte kan bevisas ha hänt. Sedan vill man lägga loggarna på en sådan nivå så att man från sammanhanget kan förstå vad som händer och så att man inte får för mycket information.

I exempelvis ett e-postprogram loggas oftast uppgifter om avsändare, mottagare, klockslag och ärendemening för varje e-postmeddelande som går via aktuell e-postservern. Uppgifterna kommer att lagras i en loggfil och blir därmed tillgängliga för läsning. [25][30]

Man delar upp loggar i olika kategorier beroende på vart de finns i ett system. Det finns, ex nätverkstrafiksloggar, applikationsloggar och systemloggar, vilka alla loggar händelser. Sedan finns det ex brandväggs- och IDS-loggar som loggar alerts, dvs talar om när något som strider mot policyn inträffar. Nedan listas information om varje kategori.

1. Nätverksloggar:

   Samlas in av en nätverkslyssnare, dvs ett verktyg som lyssnar på ett eller flera nätverksinterface och sparar den trafik som passerar. Har man lyssnaren på en host ser

den bara trafiken till den specifika datorn (givet att du inte har en hub i nätet), har man lyssnaren på en central switch, ex SPAN-port eller router kan du se all trafik på den delen av nätverket. Vad man kan få ut av nätverkstrafik beror på två saker, dels hur mycket av datan man loggar, och dels om trafiken är krypterad eller inte. Är trafiken krypterad med en tillräckligt stark kryptering kan man inte läsa innehållet i trafiken, och beroende på vilken nivå av OSI modellen man krypterar blir mer och mer av paketet oläsligt. Har man ingen kryptering kan man se allt. Har man bestämt att logga all data i paketet, dvs både headrar och payload kan man se t.ex lösenord och användarnamn till ex telnet och ftp sessioner. Vanligtvis ser man också käll- och destinationsIP adress. Nätverkssniffning kan vara ett sätt för en attackerare att få tillgång till en skyddad dator, dvs, via någon annans konto.

2. Applikationsloggar:

   Loggar till ex syslog, kan ge meddelanden om vem som har loggat in och när. Specifikt för applikationer, ex login-programmet. Här kan man också se när en maskin startat om och när inloggningsförsök misslyckas.

3. Brandväggsloggar, IDS-loggar:

   En brandvägg och IDS kan ge alerts på vissa inkommande paket eller vissa händelser i ett system. Dessa kan ge varningar och indikationer om att något fuffens händer i systemet.

4. Systemloggar:

   Loggar som övervakar access till olika objekt, som visar vilka filer som är öppna och vilka processer som kör på ett system. På Linux kan mycket sån här info fås från /proc-filsystemet.

Genom att logga händelser och spara undan loggfilerna under långa perioder får man en uppskattning om vad som är normala händelser inom systemet. Vid en undersökning av loggfiler kan man isolera ovanliga händelser genom att filtrera bort de normala händelserna. Detta görs med hjälp av logghanteringsprogram. Ett program som sköter logghantering är EventReporter. Programmet sparar ner loggar på textfiler och skickar loggarna sedan vidare till en databas. [32]

4.1.1 Syftet med loggning

Syftet med loggning är att i efterhand kunna reda ut vilka händelser som gjorts, hur, när och av vem. Loggar är underlaget för att klargöra vad som skett vid misstanke om eller inträffade säkerhetsrelaterade incidenter. Det är då av avgörande betydelse att datorklockor är synkroniserade för att loggar ska vara tillförlitliga vid en utredning eller en uppföljning. Det är även av största vikt att loggarna inte har blivit modifierade av någon, loggarna måste lagras på en plats som är helt säker inom företagets nät.

”Trafikdata, uppgifter om vad på nätet som pratat med vad, är en form av loggar som man också kan ha stor nytta av vid utredning av incidenter. För att ha tillgång till bra sådana data måste man ha implementerat loggningen innan incidenterna sker. ” [27]

”I princip all dator- och nätutrustning kan generera loggar. Det är av stort värde om dessa samlas på en central plats i organisationen dels så att rapporter kan skapas t.ex. dygnvis men även för att kunna gå tillbaka i tiden i samband med undersökning av incidenter.” [27]

Det finns som sagt olika former av loggning inom ett informationssystem. I nätverk har man till exempel filserver, e-postserver, datorer, routrar och brandväggar. Alla dessa kan skapa en loggfil. Om alla dessa komponenter som filserver, brandvägg, switchar och routrar skapar varsin loggfil, blir det många olika typer av loggfiler att gå igenom vid ett larm om oväntad aktivitet. Istället för att varje objekt ska ha en egen loggfil sparade på själva objektet så finns det lösningar, där en central loggningsenhet samlar in loggarna från olika objekt och sammanställer dessa till en enda loggfil. [27]

Det finns olika metoder och sätt att skapa en central loggenhet. Ett sätt att göra detta är att spara undan alla loggar från nätverket till exempelvis en SQL databas. [31].

”En normal systemmiljö är ofta komplicerad och består av flera system länkade till varandra i t.ex. nätverk. I dessa miljöer förekommer flera olika loggar. Ofta krävs registrering i flera system, exempelvis in- och utloggning i nätverk, behörighets- och transaktionsloggar för enskilda applikationssystem samt loggning i kommunikationsutrustning, t.ex. brandväggar, för att få en tillräckligt klar bild av användares förehavanden. En samordning av flera loggar kan behövas för att få den spårbarhet som är loggningens egentliga syfte.” [10]

”Vid intrång och liknande är det givetvis också värdefullt att man har loggarna sparade på en server som är separerad från systemet som är utsatt för intrånget, eftersom man inte kan lita på att filerna på det utsatta systemet är oförändrade.” [27]

I ett system där loggarna lagras på en gemensam plats, blir det lättare att se vad som har hänt i hela systemet, eftersom man enkelt kan ta ut alla händelser mellan exempelvis ett visst klockslag på vissa enheter. Loggningssystemet kommer då att sammanställa en loggfil som innehåller den information som är relevant vid just det tillfället. Denna information måste sedan noggrant gås igenom för att hitta avvikande information. [25]

För att kunna detektera eventuella fel inom ett loggsystem bör loggarna gås igenom med jämna mellanrum. Det är systemägarens uppgift att besluta om:

1. Hur ofta de ska analyseras
2. Vem som ansvarar för analyser av dem
3. Hur länge de ska sparas
4. Hur de ska förvaras.

”För att kunna genomföra spårningen i ett IT-system behövs kunskap om systemets bearbetningar och den kronologiska ordningen för dem. Hjälpmedlen för detta är en eller flera bevakningsfunktioner i form av loggning. Med utgångspunkt från en strategi för loggning och rätt inställningar i systemen kan dessa hjälpmedel säkerställa vems identitet som använts och när den använts. För att uppgifterna ska bli tillräckligt verifierade kan de ibland behöva kompletteras med tjänstgöringslistor, in- och utpasseringsuppgifter, attestuppgifter m.m.

Varje IT-system ska åtminstone ha möjlighet till full spårbarhet när det gäller information som bedömts ha ett högt skyddsvärde.” [10]

4.1.2 Slutsats

Loggning är en mekanism som är till för att ta reda på vad som har hänt i efterhand. Med hjälp av informationen som finns i loggfiler får man spårbarhet. Loggfiler innehåller information om händelser vid olika tidpunkter och vilken användare/dator som gjorde vad. Genom att läsa i en loggfil kan man skaffa sig en uppfattning om vad som hände. Genom att

kontakta tillverkare av system och be om exempelvis händelsenummers förklaringar kan man exakt se vad som har hänt.

Fördelen med loggning är att informationen som sparas undan är svår att modifiera om man inte är väl insatt i systemet.

En nackdel som kan förekomma med loggning är att all den information man får blir svårhanterlig. Detta gäller stora företag med många enheter som genererar loggar i deras system. Det kan vara så att all den information man får kan bli svår att tyda och det tar lång tid att ta sig igenom en loggfil. Dessutom skapas det många olika typer av loggfiler på olika enheter som gör letandet efter fel ännu svårare. Det finns verktyg för att söka igenom loggfiler men detta verktyg måste köras på varje objekt som har loggfiler och man kan fortfarande få svårt att tyda informationen.

Detta löses med hjälp av en central loggenhet som sammanställer olika loggar från flera objekt och ger en loggfil med alla händelser. Vanligtvis är en sådan enhet en loggserver som står väl skyddat i det egna nätet. En loggserver ska spara undan loggarna från hela systemet och det går inte att ändra på loggfilerna efter det att dem sparats på loggservern.

På loggservern kan man sedan använda samma verktyg för sökning i loggfiler som användes på alla enheter som nämndes tidigare. Skillnaden är att en loggserver ger en loggfil med den samlande informationen för sökningen.

Loggning är det enda verktyget som används för att lagra undan information om händelseförlopp. Genom denna undanlagring går det att i efterhand ta reda på vad som hände, vid vilken tid det hände och även vem som gjorde det. Säkerhetsåtgärder som innehåller loggning bidrar till spårbarhet. Även säkerhetsåtgärder som ger loggning till följd bidrar till spårbarhet.

4.2 Övervakning

Med hjälp av övervakning får man reda på om system fungerar som dom ska. Ett övervakningsprogram ger exempelvis en varning eller ett felmeddelande om en hårddisk har mindre än 80 % ledigt utrymme kvar eller om en hårddisk går sönder. Övervakningsprogrammet säger även till vilken disk det är samt vart disken finns. Dessa meddelanden innehåller information om vad som har hänt. Meddelanden från övervakningsprogrammet måste skickas till rätt personer inom en viss tid. Övervakningsprogram kan meddela tekniker via e-post, SMS eller på annat sätt om det är att föredra. Felmeddelanden från övervakningssystem är det första spåret vid ovanliga händelser. När ett meddelande levereras från ett övervakningsprogram är det detta meddelande som används som grund för vidare undersökning av händelse. Meddelandet startar en utredning om händelsen. Detta är det första spåret vid en eventuell händelse.

4.2.1 Vad är ett övervakningsprogram?

Övervakningsprogram kan kontrollera att olika objekt inom ett företag fungerar som dom ska. Exempelvis kan processer och tjänster på en server kontrolleras. Det går även att placera ut fysiska enheter som övervakar till exempel temperatur och fuktighet i serverrum och varnar om ett gränsvärde passeras. Även virtuella enheter, så kallade agenter kan placeras ut. En agent kan övervaka en PC, en annan agent kan övervaka en skrivare.

I Bilaga H finns det flera bilder på hur ett övervakningsprogram kan se ut. Bilderna är hämtat från ett program som heter Nagios. Detta program övervakar servrar och har väldigt många olika funktioner inbyggt i sig. Man kan som exempel enkelt ta reda på hur lång tid servrarna har varit aktiva och vilken tjänst som varje server tillhandahåller. Även hårddisk utrymme kan övervakas. [16]

Det finns tre stora områden inom övervakning. Dessa tre områden är applikationer, nätverk och system. Nedan listas några exempel inom varje övervakningskategori.

1. Applikationer (Applikationsövervakning)

Hur mycket resurser kräver applikationerna?
Är applikationerna i drift?

2. Nätverk (Nätverksövervakning)
   Last på nätverket?
   Prestanda på nätverket?
   Tecken på angrepp?

3. System (Systemövervakning)
   Vilka processer är igång?
   Vem är inloggad?

4.2.2 Applikationsövervakning

Applikationsövervakning innebär att ett program övervakar de applikationer som körs på det objekt som programmet är installerat på. Objektet kan vara exempelvis någon form av server eller en dator. Om ett applikationsövervakningsprogram är installerat på exempelvis en e-post server, övervakar programmet de processer som används för att e-post servern ska fungera korrekt. Programmet bevakar de processer som ska vara aktiva på en e-post server och varnar om fler processer startas eller om någon process stängs ner. Applikationsövervakning kan användas bland annat för att förhindra att användare kör känsliga applikationer som Regedit. Systemadministratören kan upprätta en lista över applikationer som inte får köras på datorn.

Applikationsövervakningsprogram har ibland samarbeten med utvecklarna av den applikation som ska övervakas och skapar gemensamt olika konfigurationer för hantering av händelser.

Det finns olika typer av applikationsövervakningsprogram. Vissa använder checksummor av datorns filer för att upptäcka manipulerade filer. Andra program kanske genomför en genomsökning av nya filer. Upptäcker applikationsövervakningsprogrammet något ovanligt kan programmet konfigureras för att avbryta applikationen eller att låta applikationen köras med eller utan användarens tillstånd.

4.2.3 Nätverksövervakning

Ett nätverksövervakningsprogram är ett program som automatiskt bevakar ett företags olika nätverkskomponenter som exempelvis olika former av servrar (filserver, e-post server). Programmet larmar automatiskt så fort någon av komponenterna i nätverket tycks ha råka ut för problem. På så sätt kan problemet snabbt upptäckas och förhoppningsvis också snabbt åtgärdas. Nätverksövervaknigsprogram upptäcker fel på nätverkskomponenter genom att läsa av trafik på nätverket efter ovanligt långa responstider på exempelvis en e-post server.

Big Brother är ett webbaserat system för nätverksövervakning. Programmet klarar av att hantera båda Linux och Windows servrar. Programmet ligger hela tiden och känner av om tjänster och servrar är uppe och fungerar som dem ska. Vid upptäckt av fel skickas genast ett e-post meddelande eller liknande till de personer som ska åtgärda felet. [17]

4.2.4 Systemövervakning

Systemövervakning är övervakning av det system som programmet är installerat på. Med systemövervakning kan man övervaka databasstorlekar och diskutrymmen. Ett systemövervakningsprogram kan även ha koll på till exempel att laddningsfiler kommer när de skall och att program exekveras när de skall och med vilket resultat.

Varningar startas automatiskt vid ovanliga händelser som exempelvis när en disk är full eller när en process helt oväntat slås av eller sätts på.

4.2.5 Slutsats

Övervakningsprogram finns i olika former. Oavsett form finns det en form av spårbarhet, denna form ligger i att programmen skickar ut felmeddelanden när objekt i informationssystemet inte fungerar. Dessa felmeddelanden och varningar som skickas av övervakningsprogrammet innehåller information om den händelse som har inträffat. Om exempelvis en router i nätverket har gått sönder skickar övervakningsprogrammet ett felmeddelande till lämpliga personer inom företaget och dessa personer får ta hand om problemet. Det felmeddelandet som ges från övervakningsprogrammet är det första steget i spårningen av händelseförlopp. Om ett meddelande levererades att en hårddisk på en filserver

kraschade är detta meddelande det första steget i att ta reda på vad som hände och hur det gick till.

Om det är så att övervakningsprogram är korrekt konfigurerade så kan man enkelt se vad det var som gjorde att ett system slutade att fungera. Nackdelen med övervakningsprogram är liknande. När programmet inte är korrekt konfigurerade så hjälper programmen inte mycket med spårbarheten på grund av att övervakningsprogrammet inte känner av de fel som den skulle ha känt av om programmet varit rätt konfigurerat.

Alltså ger övervakningsprogram/system spårbarhet som följd av införd åtgärd.

All information loggas och övervakas, och alarmering kan ske genom att ett e-post eller SMS omedelbart sänds ut till den person som är ansvarig för just den funktion eller det felet som uppstått. Om e-postservern slås ut då måste personen som är ansvarig för den servern tillkallas omgående. På så vis får man en enkel och direkt kontroll och spårbarhet när en oväntad händelse inträffar.

4.3 IDS

IDS står för Intrusion Detection System vilket på svenska översätts till intrångsdetekteringssystem. IDS är ett program som granskar nätverkstrafik efter kända signaturer eller avvikande fenomen i syfte att identifiera intrångsförsök. Ett IDS använder sig av antagandet att den nättrafik som angriparen eller ett skadligt program orsakar skiljer sig från den normala trafiken. Man kan dock inte utgå ifrån att skillnaden mellan den normala nättrafiken och angriparens eller det skadliga programmets trafik skulle vara särskilt stor. IDS strävar efter att upptäcka avvikelser i nätverkstrafiken och agera enligt förutbestämda regler för att hindra skador. Om det exempelvis handlar om ett intrång, så ju fortare det upptäcks desto snabbare kan angriparen identifieras och raderas från systemet. Generellt kan det sägas att ju tidigare intrånget upptäcks, desto mindre skada hinner uppstå. Med hjälp av IDS är det också möjligt att samla information om attacktekniker och denna information kan utnyttjas när mer effektiva system för intrångsdetektering utvecklas. IDS kan ställas in på olika noggrannhets nivåer på nätverkstrafik. Vid användandet av mindre noggrannhet blir allt fler angripare fast, men detta leder också till allt fler falsklarm. På ett motsvarande sätt ger en mer

preciserad noggrannhet mindre falsklarm, men samtidigt blir antalet icke-upptäckta angripare större.

Två av de mest använda metoder vid intrångsdetektering är den statistiska metoden och den regelbaserade metoden.

Den statistiska metoden kräver en databas med ett förutbestämt urval av normal nättrafik. Genom statistiska tester jämförs trafiken under analys med denna databas och på basis av jämförelsen analyserar systemet om det är frågan om en angripare eller ett skadligt program eller normal nättrafik.

Den regelbaserade metoden för sin del bygger på en rad förutbestämda regler och med hjälp av dessa försöker systemet identifiera, om det är frågan om fingeravtrycket hos det skadliga programmet eller angriparens beteende. [22][24]

Det finns 2 huvudtyper av IDS: HIDS och NIDS. HIDS och NIDS fungerar på två helt olika sätt.

4.3.1 NIDS

NIDS står för Network Intrusion Detection System och är nätverkbaserat IDS. Ett NIDS har sensorer utplacerade i nätverket, dessa sensorer rapporterar till en huvudserver om ovanligheter i nätverkstrafiken uppstår. NIDS har lägre kostnad än HIDS och är därför ett vanligare val hos företag. NIDS kan övervaka en större del av nätverket än vad HIDS kan och kan ställas in till att ha noggrannare övervakning på vissa objekt som exempelvis brandväggar, routrar, mm. Det går även att ställa in mindre noggrann övervakning på andra objekt. NIDS har även en annan stor fördel jämfört med HIDS. NIDS är nämligen mycket svårare att påverka utifrån. NIDS körs på en maskin som nätverket själv inte har tillgång till och det gör att en hacker inte kan ta sig in på NIDS och stänga av den. Detta innebär att det spår som en hacker exempelvis lämna efter sig i nätverket inte försvinner och man kan spåra vad som har hänt, rätta till och se till att det inte händer igen.

Det finns två stora nackdelar med NIDS. Den första är trafiken på nätverket. NIDS får inte missa någon trafik som skickas på nätverket och det innebär att placeringen och konfigureringen måste vara så pass noggrann att paketförluster inte inträffar. Detta innebär ofta att man placerar flera NIDS sensorer vid switchar eller routrar. Den andra nackdelen är att NIDS är känslig för anti IDS verktyg. En hacker kan gömma sitt intrång med olika tekniker i trafik som NIDS släpper förbi. En teknik kan vara att en hacker tar sig in i

krypterad trafik och gör sitt angrepp via den krypterade trafiken. Vissa NIDS kan dekryptera trafik med det öppnar andra sårbarheter som företag inte är beredda att acceptera. [22][24]

4.3.2 HIDS

HIDS står för Hostbased Intrusion Detection System på svenska blir det Värdbaserade intrångsdetekteringssystem. HIDS existerar på själva systemen dom övervakar, HIDS övervakar exempelvis loggfiler och processer. HIDS är bättre än NIDS på att detektera intrång eftersom vanlig trafik och intrångstrafik är ovanligt lika varandra och det kan därför ge problem för NIDS att se om en attack pågår. Detta är HIDS styrka jämfört med NIDS. HIDS är säkrare på att upptäcka attacker och ger mindre falska varningar än NIDS. HIDS system kan kontrollera alla delar av exempelvis en dator. Det finns lösenordsregister undan krypterade på en dator och HIDS kan se attacker mot dessa register.

En nackdel för HIDS är att för att enbart kunna använda HIDS i ett system krävs det att HIDS är installerade på alla sårbara objekt inom ett system. Detta kan bli väldigt många HIDS på grund av att det kan finns många sårbara objekt inom ett system och att även kan finnas många olika typer av system exempelvis Unix, Windows. Att installera HIDS på varje känslig punkt i nätverket är ett måste eftersom HIDS har en begränsad syn över nätverket. HIDS kan inte se om en attack sker på någon annat objekt än det objekt som HIDS är installerad på. Detta beror på att HIDS inte tittar på information som inte är menad för enheten som HIDS bevakar.

Det finns även vägar runt HIDS. Exempel: Eftersom HIDS tittar på loggar kan en attack som inte skrivs till loggen utföras, utan att HIDS säger till att en attack har skett. HIDS säger till först när ett fel i en logg upptäcks. [22][24]

4.3.3 Hur IDS ser om det är en attack

IDS har olika metoder för att detektera ovanligheter inom nätverkstrafiken. Nedan listas tre olika sätt att detektera intrång med IDS

1. Signaturbaserade detektion

IDS jämför mot en signatur databas. I denna signaturdatabas står det exakt hur olika attacker ser ut. Det som händer i nätverket jämförs mot denna databas och stämmer de överens så är det en attack på gång.

2. Protokollavvikelser

   Inom denna kategori tittar IDS på själva protokollet som används exempelvis: Telnet, http & SMTP. Ser IDS om det exempelvis kommer för många tecken, tecken på fel ställe, ogiltiga tecken. Även checksummor används som kontroll data för intrång. Detta sätt har en klar fördel mot Signaturbaserade detektion då man kan upptäcka ett intrång långt innan det finns signaturer för en attack.

3. Beteendeavvikelser

   Avvikelser från standarden är det som IDS reagerar på här. Man låter IDS stå och övervaka systemet utan att Internet är inkopplat under en tid för att IDS ska kunna få en uppskattning av hur ”normal” trafik i nätverket är. När man sedan kopplar på Internet och avvikelserna blir för stora så kan en attack IDS se om en attack pågår. Detta är ett väldigt svårt sätt att upptäcka en attack på. [24]

4.4 IPS

IDS kan bara detektera intrång vilket betyder att IDS kräver en faktor som tar till korrekta åtgärder vid intrång. IPS som står för Intrusion Prevention System är en utveckling av IDS. IPS innehåller liknande detekterings regler som IDS men IPS kan ta egna beslut om åtgärder vid intrångsdetektering. En IPS kan ges möjligheten att avbryta förbindelser som har klassificerats som ovanliga. Anledningen till att en IPS klarar av att ta egna åtgärder vid intrångs detektering är att en IPS är en blandning av IDS och en brandvägg. Genom denna blandning kan öppna portar stängas och trafik till objekt avbrytas. Detta är styrkan med IPS. IPS har en styrka till jämfört med IDS och det är antalet falska alarm. En IPS har mindre falska alarm än en IDS och detta beror på att en IDS är mer precis än IPS.

Detta är också svagheten hos IPS. Genom att vara mindre precis fångas inte alla intrång upp av ett IPS. Om IPS skulle leverera falsklarm och ta egna åtgärder för en ovanlighet som inte är ett intrång och börja stänga ner delar av systemet, skulle detta leda till svårigheter för

företag eftersom driften kanske skulle gå ner på grund av att IPS tror att en attack sker. Det är alltså viktigt att när IPS agerar att det verkligen är en attack som pågår.

Precis som hos IDS finns det för IPS även HIPS och NIPS. Host och network baserade IPS.

4.4.1 Slutsats

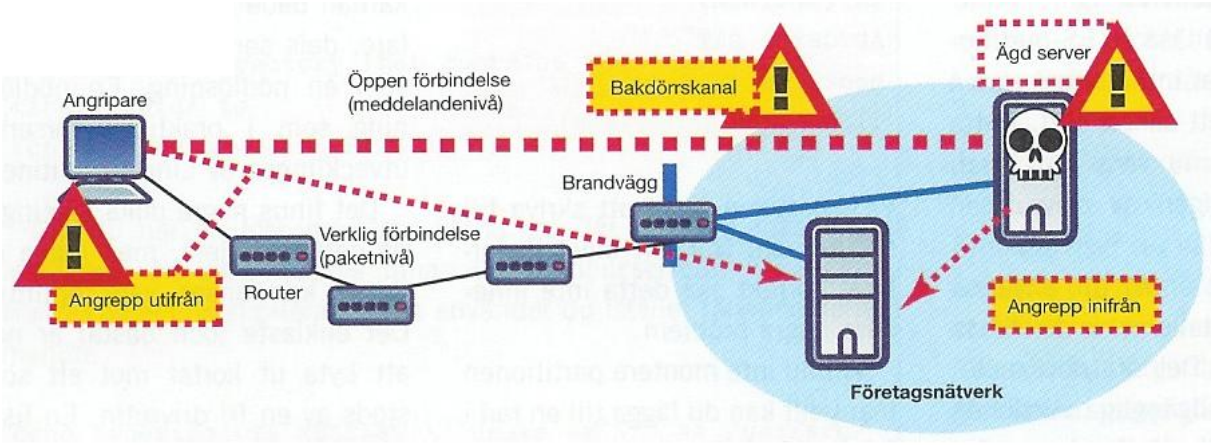
Spårbarhet i IDS finns i samma form som för övervakningsprogram/system, varningar och felmeddelanden. Skillnaden är att IDS endast övervakar trafik i nätverket eller trafik till och från objekt. IDS ligger och läser av nätverkstrafik och letar efter kända attackmönster men även ovanlig aktivitet jämfört med det som IDS anser vara normal aktivitet. IDS ger även information om attacken samt lagrar allt som en eventuell angripare gör. Ovanlig trafik som upptäcks av IDS måste på något sätt skickas till ansvariga system tekniker som kan ta korrekta åtgärder. En lösning på detta är att istället för IDS använda IPS. Tyvärr så klarar inte ett IPS av att detektera alla attacker, däremot upptäcker IDS fler attacker än IPS men IDS ger även fler falska alarm. Genom att IDS och IPS detekterar intrång och ger detaljerad information om vart i nätverket attacken är och hur attacken ser ut, gör att det är ett första steg i spårbarhet precis som övervakningsprogram. Men IDS och IPS lagrar även information om attacken som vid ett senare tillfälle kan användas som underlag för spårning av hur det skedde, varför det skedda och vem det kunde ha varit. Detta gör att IDS och IPS klassificeras som säkerhetsåtgärder med spårbarhet inbyggt och spårbarhet som följd. [27]

5 Intrång i informationssystem

Idag är kunniga angripare duktiga på att dölja sina spår. En angripare kan exempelvis radera eller ändra i loggfiler, ändra datumstämplar eller installera special kod som har till uppgift att dölja körande processer.

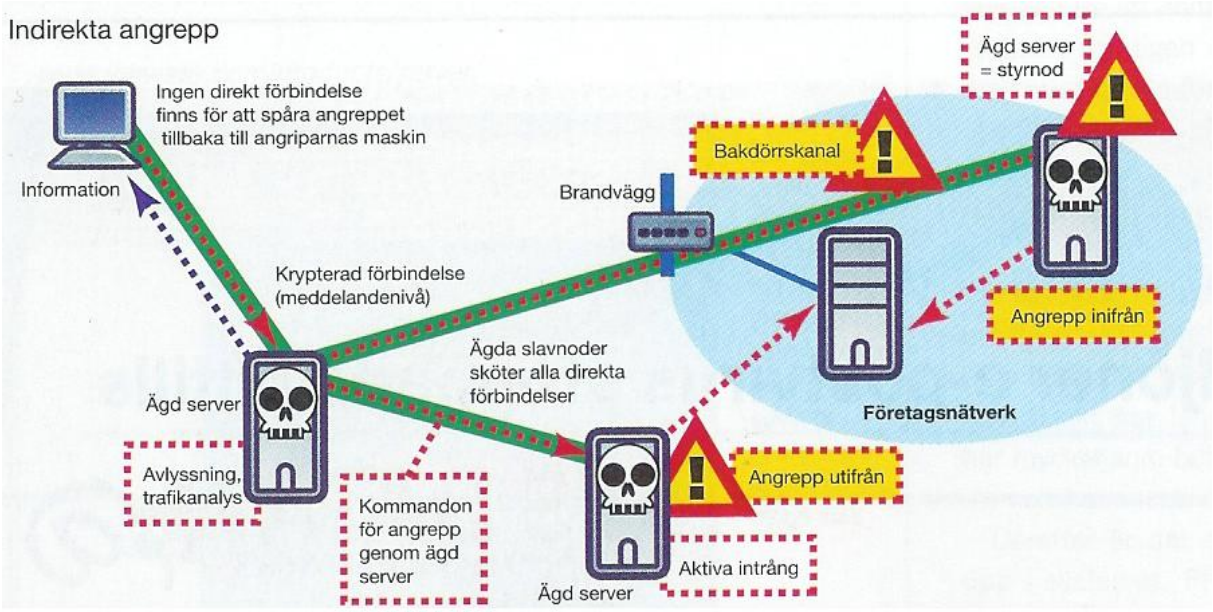
”Till exempel kan trojankod få operativsystemet att leverera falsk information och blockera kända analysverktyg.” [30]

I figur 4.3 och figur 4.4, som är citerade från tidningen DatorMagazin nummer 2/2007 visas två exempel på hur en attack skulle kunna gå till.



Figur 4.3: Direkt attack

Figur 4.3 visar hur en attack såg ut för några år sedan. Det är en så kallad ”rakt på attack”. Dessa typer av attacker var enkla att spåra eftersom den ägda serverns hårddisk ofta innehöll tydliga spår efter hela angreppsförloppet. Denna information kunde analyseras i efterhand och eftersom angriparen gjorde en direktanslutning till den ägda servern gick det att få tag på angriparens IP-adress. Detta gör att denna sorts attack är spårbar.



Figur 4.4: Indirekt attack

Idag är det vanligare att attacker sker i flera steg över olika kontaktnät. Figur 4.4 visar en tänkbar situation där en attack sker från en annan ägd server, en så kallad ”indirekt attack”. Angriparen använder sig av ägda servrar utanför företagets nätverk för att utföra attacken. Detta innebär att den ägda servern innanför företagets nätverk innehåller spår till en ägd server utanför nätverket. Man kan då i vissa fall eventuellt få angriparens IP-adress. Men det är väldigt sällan det lyckas. Angriparen använder oftast krypterad kommunikation till den ägda servern utanför företagsnätverket, vilket gör att det inte går att spåra angriparen. [30]

Det finns två olika sätt att hantera intrång när det väl upptäcks:

1. Ta ner systemet.

   Att ta ner systemet och skapa en kopia av hela systemet och göra en analys av kopian för systemet utan att tillföra någon information kallas för att göra en död analys.

2. Låt systemet köra vidare.

   Det är allt mer vanligt att företag väljer denna kategori under ett intrång. Dels blir det inget driftstop plus att observation av angriparen är möjlig. Denna metod kallas för att göra en levande analys. Det man också brukar göra vid en levande analys är att försöka skydda resterade delar av nätverket. Angriparen kommer då inte längre in i systemet utan får börja ta den information som

han/hon kommit över. Denna metod är en avvägning, dels kan man ta reda på vart attacken kommer ifrån men det kan också vara så att angriparen undertiden kommer åt känslig information. Fördelen med att låta systemet försätta gå är att man kan samla in mer bevis mot angriparen. En förutsättning för levande analys är att man har ett NIDS. NIDS hjälper till med insamling av bevis och det är även NIDS som först indikerar på intrång.

5.1.1 Sparande av intrångsinformation

Vid larm om intrång bör hanteringen av händelsen ske i förbestämda steg. Dessa steg bör finnas i en policy för intrångshantering. Det första, som tillkallade experter och tekniker ska göra vid ett intrång är att, skapa kopior av all relevant information oförändrad. Dessa kopior är underlaget för analysarbetet av händelsen som inträffade eller som händer just nu. Eftersom det finns två olika metoder för hantering av intrång blir experternas och teknikernas första uppgift att bestämma om systemet ska tas ner eller om systemet ska fortsätta köra. När väl detta är bestämt måste informationen börja sparas undan. Nedan följer de steg som bör gås igenom vid sparandet av informationen om intrånget. Förutom dessa steg måste tekniker och experter som utför detta noggrant dokumentera alla åtgärder dom vidtar. [27][30]

1. Spara undan flyktiga minnesplatser som RAM och device minne. Exempel på program som gör detta är: savecore, memdump, Helix och Windows Forensics Toolkit (WFT).
2. Skapa och spara undan listor med information från systemet. Listor med information om: inloggade användare, suspekta foldrar, aktuella processer och öppna filer.
3. Frys och lagra undan alla relevanta loggfiler.
4. Spara undan bilder hur nättrafiken ser ut.
5. Hårddiskar inom systemet som ska sparas. När det gäller hårddiskar måste exakta kopior skapas, så kallade image filer. Med hjälp av program som unrm och lazarus återskapas borttagna filer. Programmen hjälper även till med att identifiera förlorad eller gömd information. I dessa image filer är det viktigt att även opartitionerade sektorer tas med och skadade sektorer eftersom angripare kan gömma sina spår på dessa platser.

6. Förutom information på systemet kan det finnas andra data som behövs vid analysen. Till exempel: loggar från loggserverar och från andra system, information från andra drabbade.

När man gjort allt och angriparen har blivit utkastad från systemet börjar analysen av information som avbildats. Original information ska alltid finnas bevarad då nya analyser kan behövas. [27][30]

5.1.2 Analys av intrångsinformation

Det första man ska göra i en analys är att ta reda på vilken information som har med intrånget att göra. Inkallade experter och tekniker har till sitt förfogande kopior på hela systemet som skapades genom att använda listan i avsnitt 4.4.1. Experter och tekniker bör börja med att leta efter:

1. Utbytta program: Inkräktare byter ofta ut programfiler av en rad olika skäl. Det kan handla om root-kit som döljer intrång genom att inte visar vissa filer, processer och nätuppkopplingar.
2. Ändrade konfigurationsfiler: Nytillagda användare, tillagt förtroende, borttagna säkerhetskontroller, start av inkräktarens program vid systemstart.
3. Nya program: som letar efter säkerhetshål, manipulerar loggar, installerar root-kit, sniffar tangentbord och/eller nätverk.
4. Loggfiler: Från loggservern eller loggar från angriparens egna program som snifferprogram eller loggar från program som delar ut filer.

För att hitta denna information måste experterna och teknikerna använda program som är designade för att leta igenom hårddisk image filer. Program som The Coroners Toolkit (TCT) eller The Sleuth Kit (TSK) kan användas för att söka igenom image filer. [27]

”För varje år växer datamängderna som måste hanteras. Redan nu kan hundratals gigabyte av data behöva analyseras i ett enskilt fall.” [30]

Bland dessa hundratals gigabyte kan det finnas information som inte har med intrånget att göra, så nästa steg blir att filtrera bort den information som inte har med intrånget att göra. Genom att kontrollera checksummor kan man ta fram om filer ändrats. Detta förutsätter att du

vet vilka checksummor som filerna borde ha. För att kontrollera filerna använder man motsvarande filer som inte är drabbade av intrånget. Dessa filer hittas på säkerhetskopior.

Filer och särskilt program kan döpas till namn som är identiska med eller liknar andra filer eller program i systemet. I stället för att kalla snifferprogrammet sniffer, så får det heta svchost.exe eller något annat som inte sticker ut allt för mycket i den lokala miljön. Dessa delar är svåra att hitta om man inte har god kännedom om vad som är normalt i systemet.

Det enklaste sättet att få en överblick över intrånget är att skapa en tidslinje. Att skapa en tidslinje hjälper till med förståelsen för händelseförloppet. En tidslinje är ett bra sätt att nysta upp den information som finns tillänglig för intrånget.

I en tidslinje är det bra att ha information från:

1. Loggar för drabbade system (helst från en fristående logg-server som inte har påverkats av incidenten).
2. Inloggningsinformation.
3. Information om nätverkstrafik, till exempel från brandväggar och IDS-system
4. Filåtkomsttider från MAC-time-analys (Förklaras senare)

”När information från flera källor sammanställs till en tidslinje är det givetvis viktigt att tiderna inte blir fel så att tidslinjen ger fel uppfattning om vilken ordning olika händelser inträffade. Problem är att olika datakällor kan ha olika tidsinställningar. Vissa loggar kan ha sekundupplösning, medan andra loggar bara har minutupplösning. När du sorterar ihop detta till en tidslinje måste du på något sätt hantera detta, så du inte lurar dig (eller andra) att tro att något som hände mellan 14:05:00 och 14:05:59 hände exakt 14:05:00.” [27]

”En MAC-time-analys bygger på att varje fil på systemet har ett antal tidsstämplar. På ett typiskt Unix-system (där tekniken utvecklades) finns tre olika:

1. Modify (M): Sätts när filens innehåll modifieras.
2. Access (A): Sätts när filens innehåll läses.
3. Status Change (C): Sätts när status informationen i filens modifieras. Detta kan ske utan att innehållet påverkas, t.ex. då rättigheterna ändras på filen.

Dessa finns också i Windows på deras filsystem NTFS. Enda skillnaden är att C betyder creation istället för change

Fördelen med MAC-time-analys är att man får mycket information från de filer som har skapats, modifierats eller lästs under intrånget. MAC-time-analys är sorterad på tidpunkt och tack vare sorteringen kan samband som annars inte hade setts lyftas fram.

”Exempel: Inkräktare brukar försöka gömma filer på konstiga ställen och i bibliotek med konstiga namn. Om filer och kataloger skapas vid en tidpunkt du vet att incidenten pågick så syns dessa tydligt i MAC-time-analysen under denna period.” [27]

Efter det att man har skapat en uppfattning om vad som har hänt är det dags att dokumentera resultatet. Denna rapport som kan vara allt från några rader till en komplett skriftlig rapport. Denna rapport ska vara till grund för vidare åtagande i ärendet. Rapporten ska kunna användas vid polisanmälan och även kunna användas som grund för eventuella beslut om nya säkerhetsåtgärder som ska iföras i företagets informationssystem.

5.1.3 Slutsats

Det är svårt att kunna ta reda på om man blivit attackerad om det är så att en attack är väl genomförd och angriparen har lyckats ta bort de synliga spåren efter sig. Det finns då inget synligt efter en attack och inget system har gett någon varning om attacken. Finns det inget att göra då? Jo, det finns det. Det finns alltid spår någonstans på hårddisken hos det system som har blivit angripet. Problemet är att om man inte börjar leta efter det så hittar man det aldrig. Spår som lämnas kvar på ett angripet system kan exempelvis ligga i opartitionerat område på hårddiskar, i sektorer på hårddiskar som flaggats som trasiga. Dessa gömställen för spårdata hittas inte om man inte använder speciella verktyg. En lösning på problemet är att från en säker kodkälla exempelvis en CD-skiva använda säkra analysverktyg som exempelvis root-kit. Eftersom dessa verktyg användas utifrån och använder rådata från exempelvis en hårddisk går det inte att dölja de spår som finns där. De analyseringsprogram som sköter detta har direkt access till en hårddisk styrkrets och själv tolkar filsystemet efter kända signaturer för intrång [30]. Däremot så måste någon komma på idéen om att köra detta verktyg på ett system som inte gett ett tecken på intrång.

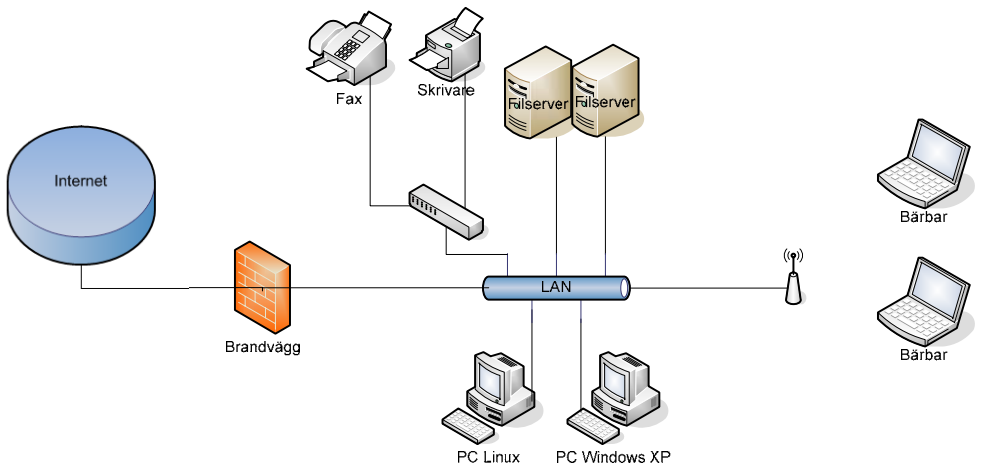
Däremot om ett IDS eller IPS talar om att ett intrång håller på. Då öppnas många möjligheter att övervaka angriparen, analysera vad angriparen gör och samla in bevis för eventuellt åtal. När ett IDS eller IPS upptäcker en attack gäller det använda sig av de steg som finns beskrivna i 4.4.1 och 4.4.2. Genom att lagra och analysera den information som en angripare ger ifrån sig vid ett angrepp hjälper andra företag genom att angriparens mönster kommer att hamna i databaser för IDS och IPS.

”Tyvärr är det så att de flesta intrång upptäcks av en slump.” [30]

Alla de system som ska detektera intrång och alla de program som ska kontrollera loggar har inte tillräckligt med information om alla olika nya attacksignaturer. Det som oftast händer är att personer inom företaget märker när objekt inte fungerar som de ska. Filer är ändrade, filer försvinner, det tar lång tid att accessa en viss del i databasen, är några exempel på saker som användare märker. Idag pågår det arbete för att utveckla de system som hjälper till vid detektering av ovanliga aktiviteter inom nätverk. Företagen bakom utvecklingen lovar mycket. Det återstår bara att se om tekniken förmår att leva upp till löftena och samtidigt värna om systemsäkerheten. [27][30]

6 Ett möjligt scenario

Antag ett scenario där en elev, Per försöker ändra sitt betyg på en kurs från en linux maskin i en av skolans datasalar. Figur 7.1 är en bild av hur en skolas nätverk kan se ut. I denna bild sitter eleven på Linux maskinen och försöker ta sig in på en filserver där elevernas betyg sparas undan.



Figur 7.1: Nätverk anslutet till Internet

I scenariot är A och B är olika sätt för Per att försöka ändra sitt betyg.

A: En attackerare sniffar passivt en okrypterad ftp-session, på en dator där användaren är root. I och med detta får han tag i lösenord och användarnamn för denna användare.

B: En attackerare scannar aktivt en dator för nätverkstjänster som lyssnar på inkommande trafik, ex en webserver.

B: Attackeraren upptäcker en lyssnande tjänst och "fingerprintar" den för att ta reda på version av servern och os:et.

B: Attackeraren exekverar en nätverksbaserad overflow-attack för att

tvinga webservern att starta ett kommandoskal åt attackeraren.

B: Attackeraren installerar en nätverkssniffare och lyssnar efter lösenord i klartext

A & B: Attackeraren laddar upp sina exploits och kompilerar dem i /tmp. Attackeraren hittar ett exploit som funkar mot en binär som är suid root och får root-access. Attackeraren skapar ett kommandoskal som är suid root, så att varje gång det exekveras blir attackeraren root.

A & B: Nu är attackeraren root på systemet. Attackeraren startar administrationsprogrammet för betygsdatabasen och ändrar betyget för lämplig student.

A & B: Attackeraren loggar ut.

6.1 Lösning på Scenario

Hur tar man reda på vilken elev som varit inne och ändrat på betygen. En given lösning är att ta de elever som fått betyg ändrade och prata med dom för att se vem som gjorde det. Men det kan vara så att ingen av dessa elever gjorde ändringen. En människa är oskyldig tills motsatsen har bevisats. Så hur bevisar man att en elev har gjort en ändring? I detta scenario finns det en del saker som kan vara till hjälp. Det finns inom nätverket olika loggfiler som kan vara till hjälp att ta fast den skyldigt. Det finns loggar för nätverket och applikationer. Om nätverket hade konfiguerat en brandvägg och ett IDS system hade loggar från dessa också kunnat utnyttjas.

I detta scenario hade skolan installerat ett IDS system och skolan hade en bra konfiguerad brandvägg. Givet detta kan man hitta följande i loggarna:

Nätverksloggar: Datum och tid för inloggning, samt source IP. Om kommunikationen är okrypterad, även attackerarens exploit i klartext om de är i källkod, annars åtminstone strängar om de är kompilerade redan.

Applikationsloggar: Inloggning och utloggning för användare resp root. Historiefil för de kommandoskal som attackeraren använt. Sannolikt loggas också in och utloggning ur betygsprogrammet. Betygsprogrammet visar antagligen också de transaktioner som gjorts, och man kan säkert se att ett betyg ändrades. Om detta gjordes på natten ser man att det är en ovanlig tid att ändra betyg på.

Brandväggs: IDS-loggar. Det är möjligt att en signatur för attackerarens overflow attack finns tillgänglig i en IDS-regeldatabas. Då kan man se på alerten när något hände. Det som skulle kunna ha gjorts med hjälp av IDS systemet var att stänga ner kopplingen mellan nätverket och databasen som angriparen är inne i och ändrar. Alternativt göra en sökning i nätet för att se vart kopplingen kommer ifrån.

Tyvärr är det så att i de flesta fall när man arbetar med analys av spår vid incidenter blir svaren väldigt mycket "Det beror på X.", där X kan vara exempelvis "vilket/vilka operativsystem som är inblandade.". Detta gör att för att kunna bygga ett exakt scenario är väldigt svårt. Man måste ha all inforamtion ett system och kontakta flera olika system administratörer för att få reda på exempelvis hur deras loggar ska tolkas. Utan alla undersökningar formas av den miljö som incidenten har skett i. Ofta sammanställer man och jämför uppgifter från flera olika system, inte bara från datorer, utan det kan vara brandväggs- och nätverkstrafikloggar och till och med loggar för passerkort för dörrar.

Så en lösning på detta scenario skulle kunna vara att man får reda på att Per var den enda som var i en linux sal vid den tid som intrånget skedde och att det hände från Per´s konto. Oftast på skolor registreras elever när de loggar på och av. Denna information finns i applikationsloggar och har en betydande del i Per´s avslöjande.

7 Slutsats

Huvuduppgiften till denna uppsats var att undersöka vilka säkerhetsåtgärder som innehöll spårbarhet eller som hade spårbarhet som följd. För att göra detta behövdes objekt att undersöka hot mot. För att sedan ta fram säkerhetsåtgärder för hoten. I början på kapitel 3 togs det fram fyra stycken objekt som skulle undersökas närmare. Dessa fyra objekt var: arbetsstation, server, nätverk och databas. Anledningen till att just dessa fyra objekt valdes för undersökning var att dessa objekt finns inom de flesta företags informationssystem. Under bilagorna A, B och C finns en tabell per hot och i varje tabell finns det ett antal säkerhetsåtgärder för att lösa hotet. Vissa säkerhetsåtgärder blir tekniska lösningar och ibland kan den tekniska lösningen behöva skyddas från andra hot. När en teknisk lösning behöver skydd blir den tekniska lösningen ett sekundärobjekt. Säkerhetsåtgärder för sekundärobjekt finns listade i en tabell under Bilaga D.

I kapitel 3 har några av dessa tabeller från bilagorna A, B och C beskrivits lite mer ingående. Anledningen var att försöka identifiera olika huvudområden inom spårbarhet. Under kapitel 3 framträdde tre stycken huvudområden. Loggning, övervakningsprogram/system och IDS. Dessa huvudområden fick en mer detaljerad förklaring i kapitel 4.

Varje huvudområde beskrevs för att framhäva om spårbarhet fanns eller om spårbarhet blev en följd av införd åtgärd.

Spårbarheten inom loggning ligger i att i efterhand kunna gå bakåt i tiden för att ta reda på vad som hade hänt. Loggning innehåller alltså spårbarhet. Övervakningsprogram/system genererar de spår som senare kan undersökas. Övervakningsprogram/system har alltså spårbarhet som följd när dessa säkerhetsåtgärder har blivit införda. IDS är väldigt likt övervakningsprogram/system skillnaden är att IDS läser av trafik i nätverket eller till och från objekt. I denna trafik försöker IDS hitta onormal trafik. Spårbarheten i IDS liknar mycket spårbarheten för övervakningsprogram/system, men IDS lagrar även information om attacker som vid ett senare tillfälle kan användas som underlag för spårning av hur det skedde, varför det skedda och vem det kunde ha varit. Detta gör att IDS klassificeras som säkerhetsåtgärder med spårbarhet inbyggt och spårbarhet som följd. Detta gäller även utveckling av IDS, IPS. IPS har samma spårbarhet som IDS men IPS klarar av att ta egna beslut utan yttre påverkan.

Problemställningen för denna uppsats var tre stycken frågor.

1. Finns spårbarhet?
2. Är spårbarhet en följd av denna åtgärd?
3. I vilken form finns spårbarhet?

Dessa frågor skulle besvaras för varje säkerhetsåtgärd. Om en säkerhetsåtgärd fick svar ”ja” på någon av frågorna 1 och 2 ingick åtgärderna i kategorin: säkerhetsåtgärder som tillämpar spårbarhet. Under denna uppsats har jag kommit fram till ett antal säkerhetsåtgärder som ligger inom kategorin: säkerhetsåtgärder som tillämpar spårbarhet. De säkerhetsåtgärder som lagts in i den kategorin under arbetet är:

1	Account management
2	Antivirus program
3	Användar ID
4	Autentisering
5	Brandvägg
6	DMZ
7	E-post filtrering
8	Honeypot
9	IDS, HIDS, NIDS
10	Loggning
11	Manuell säkerhetskopiering
12	Network management
13	Proxy
14	System management
15	Uppdatering av antivirus pattern
16	Webb filter
17	Övervakning av objekt

Tabell 8.1 Säkerhetsåtgärder

I vilken form finns spårbarhet?

För att en säkerhetsåtgärd ska innehålla spårbarhet eller ha spårbarhet som följd måste antingen loggning vara en tillämpning i säkerhetsåtgärden. Eller så måste säkerhetsåtgärden innehålla stöd för spårgenerering.

Om en säkerhetsåtgärd innehåller stöd för loggning eller spårgenerering klassificeras säkerhetsåtgärden att den ingår i kategorin säkerhetsåtgärder som tillämpar spårbarhet.

I denna uppsats har säkerhetsåtgärder som tillämpar loggning fått betyg 2 och säkerhetsåtgärder som genererar spår har fått betyg 1. Dessa betyg kan ses i bilagorna A, B, C och D.

8 Referenser

[1] Robert Malmgren, *Praktisk nätsäkerhet*, INTERNET ACADEMY, 2002, ISBN: 91-85035-01-7

[2] Nationalencyklopedins hemsida, [WWW] http://0-www.ne.se.biblos.kau.se/jsp/search/article.jsp?i_art_id=211471&i_word=Information

[3] SS-ISO/IEC 17799:2005

[4] Wikipedia, [WWW] http://sv.wikipedia.org/wiki/Alexander_Graham_Bell

[5] David Kahn, *The codebreakers: The story of secret writing*, SCRIBNER, 1996, ISBN: 9780684831305

[6] Wikipedia, [WWW], http://sv.wikipedia.org/wiki/Datas%C3%A4kerhet

[7] SIS HB 550, *Terminologi för informationssäkerhet*, SIS – Ledningssystem, 2003, ISBN: 9171625763

[8] Veriscans PowerPoint presentations dokument

[9] Matt Bishop, Introduction to computer security, ADDISON-WESLEY, 2004, ISBN 0-321-24744-2

[10] BITS, Basnivå för informationssäkerhet, KBM, 2006, http://www.krisberedskapsmyndigheten.se/templates/EntryPage____677.aspx

[11] Nationalencyklopedin, [WWW] http://www.ne.se.biblos.kau.se/jsp/search/article.jsp?i_art_id=211494&i_word=informationssystem

[12] DatorMagazin nummer 1/2007, Artikel: *Säkerhet eller funktionalitet*, sid. 92-96

[13] Säkerhet och sekretess nummer 2/2006, Artikel: *Antiforensiska verktyg undanröjer bevisen?*, sid. 28-31

[14] CIO Sweden 2, Mars 2006, Artikel: Alla dessa mobila maniker – hur du undviker att bli galen, sid. 32-37

[15] Stadskontoret, *Hantering av IT-incidenter - vem gör vad och hur?*, 2001, http://www.statskontoret.se/Statskontoret/Templates/PublicationPage____1047.asp

[16] Nagios, [WWW], http://nagios.org/

[17] Big Brother, [WWW], http://bb4.com/

[18] Wikipedia, [WWW] http://sv.wikipedia.org/wiki/Code_Red_%28internetmask%29

[19] Wikipedia, [WWW], http://sv.wikipedia.org/wiki/Brandv%C3%A4gg

[20] Wikipedia, [WWW], http://sv.wikipedia.org/wiki/DMZ_%28Internet%29

[21] Wikipedia, [WWW], http://en.wikipedia.org/wiki/Proxy_server

[22] Wikipedia, [WWW], http://en.wikipedia.org/wiki/Intrusion_detection_system

[23] Wikipedia, [WWW], http://en.wikipedia.org/wiki/Oracle_database

[24] Jack Koziol, *Intrusion Detection with Snort*, HOWARD W SAMS, 2003, ISBN: 9781578702817

[25] LogAnalysis.org, [WWW], http://www.loganalysis.org/

[26] Dieter Gollmann, *Computer security*, JOHN WILEY & SONS LTD, 2006, ISBN: 0-470-86293-9

[27] IT-säkerhetshandboken, [WWW], https://itsakhandbok.irt.kth.se/susec/

[28] Wikipedia, [WWW], http://en.wikipedia.org/wiki/Group_Policy_Object

[29] Wikipedia, [WWW], http://en.wikipedia.org/wiki/Honeypot_%28computing%29

[30] DatorMagazin nummer 2/2007, Artikel: *Analys av intrång*, sid. 92-95

[31] DeamonNews, [WWW], http://ezine.daemonnews.org/200111/syslog.html

[32] EventReporter, [WWW], http://www.eventreporter.com/en/product/product-tour.php

Bilaga A Arbetsstation och server

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
Skadlig kod	Filtrering	Brandvägg	2	Brandvägg
		Antivirus	2	AV program
		Webbfilter	2	
		Proxy	2	Proxy
		E-post filtrering	2	

Tabell A.1: Skadlig kod

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
Intrångsförsök	Filtrering	Brandvägg	2	Brandvägg
		Proxy	2	Proxy
	Säkerhetskopiering	Manuell säkerhetskopiering	1	Lagringsmedia
		Backuprobot	0	Lagringsmedia
	Kryptering	Krypteringsteknik	0	
	Övervakning	System management	1	Management programmet
	BKS	ACL i NTFS	0	
		Anv.ID och lösen	2	

Tabell A.2: Intrångsförsök

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
Hårdvarufel	Systemunderhåll	Rutiner för uppdatering	0	
		Konfigurering	0	Övervakningsstation
	Övervakning av objekt	System Management	1	Management programmet
	Avtal	Hårdvaruutbyte via avtalspartner	0	
	Rutin för felavhjälpning		0	
	Systemdokumentation	Användarhandledning till system	0	Dokument
	Driftdokumentation	Användarbeskrivning till objekt	0	Dokument
	Säkerhetskopiering	Manuell säkerhetskopiering	1	Lagringsmedia
		Backuprobot	0	Lagringsmedia

Tabell A.3: Hårdvarufel

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
Mjukvarufel	Metoder	Metod för utveckling	0	
		Test innan produktionssättning	0	Testnät med testutrustning
		Metod för systemimplementation	0	
	Systemdokumentation	Användarhandledning till system	0	Dokument
	Driftdokumentation	Användarbeskrivning till objekt	0	Dokument
	Säkerhetskopiering	Manuell säkerhetskopiering	1	Lagringsmedia
		Backuprobot	0	Lagringsmedia
	Övervakning av objekt	System Management	1	Manager programmet
	Avtal med leverantörer		0	
	Garantier		0	

Tabell A.4: Mjukvarufel

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
Utnyttjande av standardinställningar	Installationshantering	Mallar för uppsäkring, script	0	Policy
		Kompetent personal	0	

Tabell A.5: Utnyttjande av standardinställningar

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
Incidenter inom företaget	Övervakning av trafik	Host Intrusion Detection System	2	
	Rättigheter/Åtkomst	Konfigurering via GPO (group policy)	0	
	Regler för användning	Policys	0	
	Inloggning	Unika ID	2	
		Lösenordsdesign	0	
	Kontohantering	Account management	1	Management programmet
	Övervakning av objekt	System Management	1	Management programmet
	Säkerhetskopiering	Manuell säkerhetskopiering	1	Lagringsmedia
		Backuprobot	0	Lagringsmedia
	Rutin för översyn av utgiven åtkomst		0	
	Interaktivt skydd mot annan användare	CTRL-ALT-DEL (Ny inlogg)/Lås maskin	0	
	Kontroll av använda programvaror		0	
	Program för inventering av program		0	

Tabell A.6: Incidenter inom företaget

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
Trådlös kommunikation	Säkra protokoll	WPA, WPA-TSK, WEP	0	
	Kryptering	Krypteringstekniker, algoritmer	0	
	Övervakning av trafik	Host Intrusion Detection System	2	
		Network Management	1	Management programmet
	Rutin för uppsäkring av datorinställningar		0	
	Kontroll av okända nät		0	

Tabell A.7: Trådlös kommunikation

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
DoS	Redundans	Redundans i kommunikation	0	Avtal med ISP
		Redundans i applikation	0	
	Incidenthantering	Policy för incedenthantering	0	Dokument
	Övervakning av objekt	System Management	1	Management programmet
	Övervakning av trafik	Network Management	1	Management programmet
	Säkerhetskopiering	Manuell säkerhetskopiering	1	Lagringsmedia
		Backuprobot	0	Lagringsmedia

Tabell A.8: DoS

Bilaga B Nätverk

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
Skadlig kod	Filtrering	Brandvägg	2	Brandvägg
		Antivirus	2	AV program
		Proxy	2	Proxy
		E-postsystem filtrering	2	
		DMZ	1	

Tabell B.1: Skadlig kod

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
Intrångsförsök	Filtrering	Brandvägg	2	Brandvägg
		Proxy	2	Proxy
		DMZ	1	
	Kryptering	Krypteringsteknik	0	
	Övervakning av trafik	HIDS, NIDS, IDS	2	
		Network management	1	Manager programmet
	BKS	ACL i NTFS	0	
		Anv.ID och lösen	2	
	Lurar attackerare	Honeypot	2	

Tabell B.2: Intrångsförsök

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
Hårdvarufel	Systemunderhåll	Rutiner för uppdatering	0	
		Konfigurering	0	Övervakningsstation
	Övervakning av object	System Management	1	Manager programmet
	Avtal	Hårdvaruutbyte via avtalspartner	0	
	Rutin för felavhjälpning		0	
	Systemdokumentation	Användarhandledning till system	0	Dokument
	Driftdokumentation	Användarbeskrivning till objekt	0	Dokument
	Säkerhetskopiering	Manuell säkerhetskopiering	1	Lagringsmedia
		Backuprobot	0	Lagringsmedia

Tabell B.3: Hårdvarufel

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
Mjukvarufel	Metoder	Metod för utveckling	0	
		Test innan produktionssättning	0	Testnät men testutrustning
		Metod för systemimplementation	0	
	Systemdokumentation	Användarhandledning till system	0	Dokument
	Driftdokumentation	Användarbeskrivning till object	0	Dokument
	Säkerhetskopiering	Manuell säkerhetskopiering	1	Lagringsmedia
		Backuprobot	0	Lagringsmedia
	Övervakning av objekt	System Management	1	Manager programmet
	Avtal med leverantörer		0	
	Garantier		0	

Tabell B.4: Mjukvarufel

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
Utnyttjande av standard-inställningar	Installationshantering	Mallar för uppsäkring, script	0	Policy
		Kompetent personal	0	

Tabell B.5: Utnyttjande av standarinställningar

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
Incidenter inom Företaget	Övervakning av trafik	Host Intrusion Detection System	2	
		Network management	1	Manager programmet
	Rättigheter/Åtkomst	Konfiguering via GPO (group policy)	0	
	Regler för användning	Policys	0	
	Inloggning	Unika ID	2	
		Lösenordsdesign	0	
	Kontohantering	Account management	1	Manager programmet
	Övervakning av objekt	System Management	1	Manager programmet
	Säkerhetskopiering	Manuell säkerhetskopiering	1	Lagringsmedia
		Backuprobot	0	Lagringsmedia

Tabell B.6: Incidenter inom företaget

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
Trådlös kommunikation	Säkra protokoll	WPA, WPA-TSK, WEP	0	
	Kryptering	Krypteringstekniker, algoritmer	0	
	Övervakning av trafik	Network Intrusion Detection System	2	
		Network Management	1	Manager programmet
	Rutin för uppsäkring av datorinställningar		0	
	Kontroll av okända nät		0	

Tabell B.7: Trådlös kommunikation

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
DoS	Redundans	Redundans I kommunikation	0	Avtal med ISP
		Redundans i applikation	0	
	Incidenthantering	Policy för incedenthantering	0	Dokument
	Övervakning av objekt	System Management	1	Management programmet
	Övervakning av trafik	Network Management	1	Management programmet
		Host Intrution Detection System	2	
	Säkerhetskopiering	Manuell säkerhetskopiering	1	Lagringsmedia
		Backuprobot	0	Lagringsmedia

Tabell B.8: DoS

Bilaga C Databas

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
Skadlig kod	Filtrering	Antivirus	2	AV program

Tabell C.1: Skadlig kod

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
Intrångsförsök	Kryptering	Krypteringsteknik	0	
	Övervakning av trafik	Host Intrution Detection System	2	
		Network management	1	Manager programmet
	BKS	ACL i NTFS	0	
		Anv.ID och lösen	2	

Tabell C.2: Intrångsförsök

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
Programvarufel	Metoder	Metod för utveckling/upgradering	0	
		Test innan produktionssättning	0	Testnät men testutrustning
		Metod för systemimplementation	0	
	Systemdokumentation	Användarhandledning till system	0	Dokument
	Driftdokumentation	Användarbeskrivning till objekt	0	Dokument
	Säkerhetskopiering	Manuell säkerhetskopiering	1	Lagringsmedia
		Backuprobot	0	Lagringsmedia
	Övervakning av objekt	System Management	1	Manager programmet
	Avtal med leverantörer		0	
	Garantier		0	

Tabell C.3 Programvarufel

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
Utnyttjande av standardinställningar	Installationshantering	Mallar för uppsäkring, script	0	Policy
		Kompetent personal	0	
	Administratör konto	Lösenordsdesign	0	
	Systemkonton	Unika ID	2	
		Lösenordsdesign	0	

Tabell C.4: Utnyttjande av standardinställningar

Hot	Skyddsåtgärd	Lösning/ teknisklösning	Spårbarhet	Sekundärobjekt
Incidenter inom företaget	Rättigheter/Åtkomst		0	
	Regler för användning	Policys	0	
	Inloggning	Unika ID	2	
	Säkerhetskopiering	Lösenordsdesign	0	
		Manuell säkerhetskopiering	1	Lagringsmedia
		Backuprobot	0	Lagringsmedia

Tabell C.5: Incidenter inom företaget

Bilaga D Sekundärobjekt

Sekundärobjekt	Hot	Skyddsåtgärd	Spårbarhet
Proxy	Obehörig person loggar in	Autentisering	2
		Loggning	2
	Mjukvarufel	Övervakning av objekt	1
Brandvägg	Obehörig person loggar in	Autentisering	2
		Loggning	2
	Mjukvarufel	Övervakning av objekt	1
AV program	Gammal version	Uppdatering av pattern	1
	Mjukvarufel	Övervakning av AV systemet	1
		Larmfunktion virusskydd	1
Lagringsmedia	Mjukvarufel	Övervakning av objekt	1
	Fysiska hot	Fysiska skyddsåtgärder	1
Dokument	Stöld, modifiering	Skyddad lagringsplats	2
Management program	Obehörig person loggar in	Autentisering	2
		Loggning	2
	Mjukvarufel	Övervakning av objekt	1
Övervakningsstation	Mjukvarufel	Övervakning av objekt	1
Testnät med testutrustning	Hårdvarufel	Övervakning av objekt	1
	Mjukvarufel	Övervakning av objekt	1
Policy	Fysiska hot	Fysiska skydd	2
Avtal med ISP			0

Tabell D.1: Sekundär objekt

Bilaga E Sisco switch loggfil

*** Loggfil för Alsters Förskola Switch_30 (Cisco), 17.00 070425 ***

AlstersFS-Sw.030#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0 flushes, 0 overruns)
  Console logging: disabled
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 445 messages logged
  Exception Logging: size (4096 bytes)
  File logging: disabled
  Trap logging: level warnings, 89 message lines logged
    Logging to 192.36.20.24, 89 message lines logged

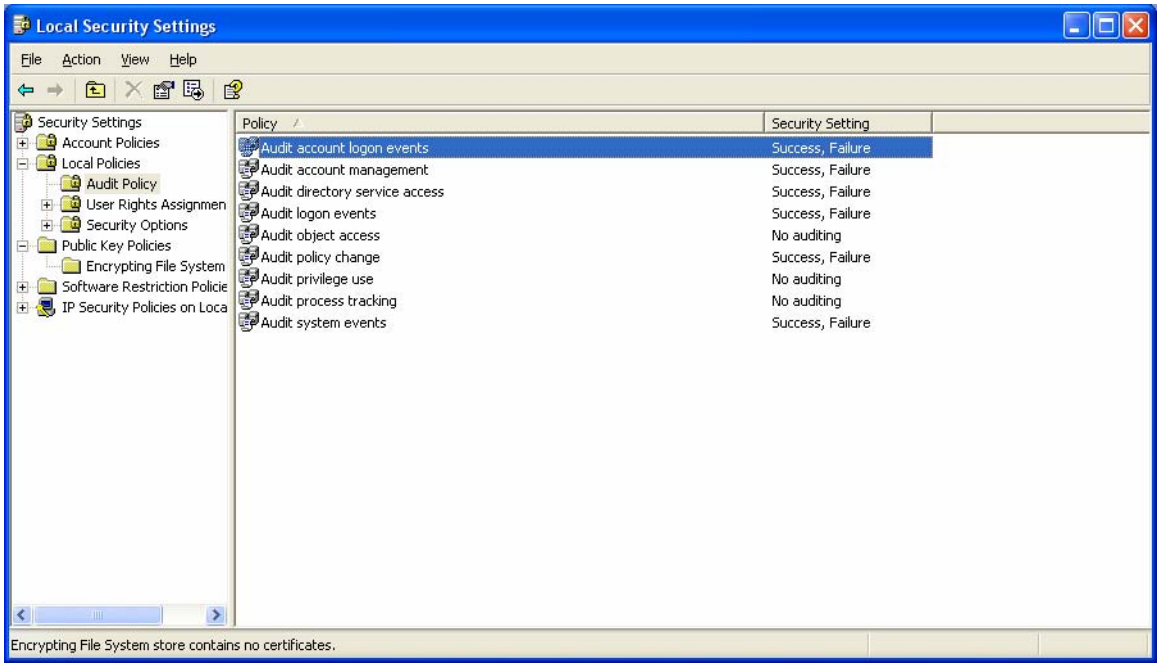
Log Buffer (16384 bytes):
 changed state to up
Mar 29 15:47:49.351 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Mar 29 15:47:50.355 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to down
Mar 29 15:47:52.551 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to up
Mar 29 15:47:53.551 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Mar 30 08:46:51.719 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Mar 30 08:46:53.731 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Mar 30 08:47:14.719 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Mar 30 08:47:16.723 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Mar 30 12:06:44.666 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
Mar 30 12:06:46.670 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Mar 30 15:26:00.818 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to down
Mar 30 15:26:01.822 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to down
Mar 30 15:26:25.419 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Mar 30 15:26:26.423 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to down
Mar 30 15:26:28.619 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to up
Mar 30 15:26:29.619 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 2 09:25:55.726 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 2 09:25:57.730 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 2 09:26:18.527 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 2 09:26:20.531 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 2 13:17:56.962 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to up
Apr 2 13:17:57.962 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to up
Apr 2 15:40:29.017 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 2 15:40:30.021 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to down
Apr 2 15:40:32.217 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to up
Apr 2 15:40:33.217 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 3 09:42:34.706 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 3 09:42:36.710 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up

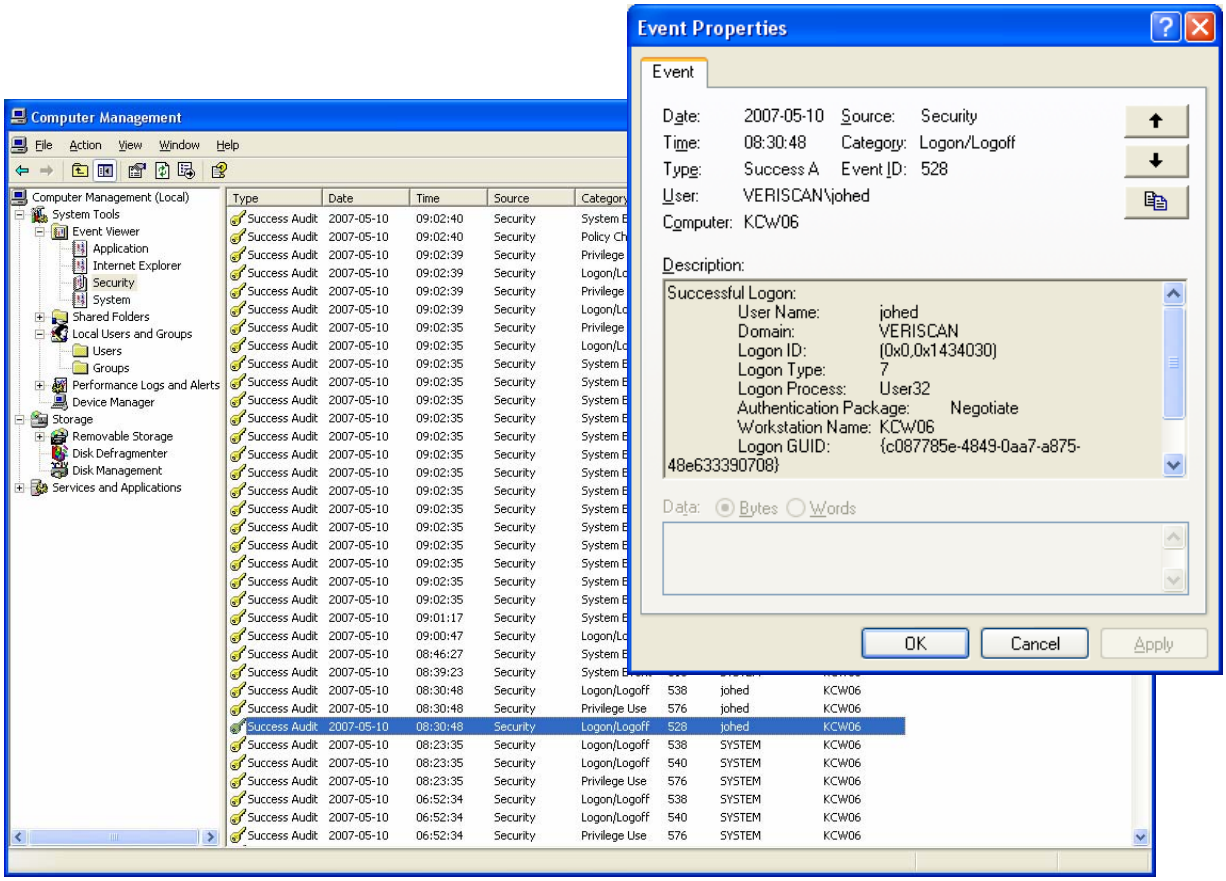
Apr 3 09:42:57.314 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 3 09:42:59.318 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 3 09:48:03.558 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 3 09:48:08.363 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 3 09:48:30.759 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 3 09:48:31.763 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to down
Apr 3 12:55:26.822 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
Apr 3 12:55:28.826 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Apr 3 15:54:59.586 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to down
Apr 3 15:55:00.590 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to down
Apr 4 16:16:37.151 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to up
Apr 4 16:16:38.151 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to up
Apr 5 13:52:03.543 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to up
Apr 5 13:52:04.543 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 5 13:53:22.360 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 5 13:53:24.364 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 5 13:53:28.160 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 5 13:53:30.172 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 5 14:26:46.650 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 5 14:26:47.654 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to down
Apr 5 14:26:49.850 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to up
Apr 5 14:26:50.850 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 5 14:44:20.008 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to down
Apr 5 14:44:21.012 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to down
Apr 10 07:29:21.255 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 10 07:29:23.259 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 10 07:29:27.255 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 10 07:29:27.655 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to up
Apr 10 07:29:28.655 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to up
Apr 10 07:29:29.259 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 10 14:16:13.625 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 10 14:16:15.637 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 10 14:16:19.425 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 10 14:16:21.429 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 10 14:16:25.225 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 10 14:16:27.229 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 10 15:32:41.884 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 10 15:32:43.896 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 11 08:45:32.772 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 11 08:45:34.776 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 11 08:45:38.572 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 11 08:45:40.584 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 11 15:06:36.319 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 11 15:06:37.323 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to down
Apr 11 15:06:39.519 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to up
Apr 11 15:06:40.519 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 12 07:24:54.905 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 12 07:24:56.917 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 12 07:25:00.905 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 12 07:25:02.910 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 12 14:53:08.038 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down

Apr 12 14:53:09.042 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to down
Apr 12 14:53:11.238 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to up
Apr 12 14:53:12.238 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 13 12:09:07.631 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 13 12:09:09.635 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 13 12:09:13.631 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 13 12:09:15.635 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 13 13:55:06.160 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 13 13:55:07.164 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to down
Apr 13 13:55:09.360 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to up
Apr 13 13:55:10.360 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 16 08:52:35.995 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 16 08:52:37.999 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 16 08:52:41.796 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 16 08:52:43.800 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 16 15:34:27.535 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 16 15:34:29.547 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 17 09:06:43.394 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 17 09:06:45.398 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 17 09:06:49.194 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 17 09:06:51.198 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 17 15:50:48.345 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 17 15:50:50.357 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 18 07:46:42.534 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
Apr 18 07:46:44.538 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Apr 18 09:29:34.037 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 18 09:29:36.049 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 18 09:29:40.037 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 18 09:29:42.041 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 18 14:57:37.519 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 18 14:57:39.531 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 19 09:05:45.079 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 19 09:05:47.091 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 19 09:05:51.079 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 19 09:05:53.083 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 19 15:33:37.697 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 19 15:33:39.709 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 19 16:38:44.269 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to down
Apr 19 16:38:45.273 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to down
Apr 20 10:44:25.804 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 20 10:44:27.816 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 20 10:44:31.804 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 20 10:44:33.808 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 20 10:46:03.413 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to up
Apr 20 10:46:04.413 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to up
Apr 20 10:53:02.874 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
Apr 20 10:53:04.878 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Apr 20 14:18:16.677 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to down
Apr 20 14:18:17.681 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to down
Apr 20 15:52:12.694 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 20 15:52:13.698 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to down

Apr 20 15:52:15.894 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to up
Apr 20 15:52:16.894 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 23 09:03:57.175 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 23 09:03:59.179 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 23 09:04:02.975 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 23 09:04:04.987 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 23 09:12:20.845 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to up
Apr 23 09:12:21.845 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to up
Apr 23 15:54:37.377 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 23 15:54:38.381 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to down
Apr 23 15:54:40.577 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to up
Apr 23 15:54:41.577 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 24 08:50:57.299 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 24 08:50:59.303 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 24 08:51:03.107 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 24 08:51:05.111 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 24 15:13:31.462 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 24 15:13:33.474 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 25 08:58:05.011 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 25 08:58:07.023 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
Apr 25 08:58:11.011 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
Apr 25 08:58:13.015 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
AlstersFS-Sw.030#

Bilaga F Login/logoff loggar i Windows





Bilaga G Logg från en brandvägg

Apr 28 15:41:38

mindator kernel: IN=eth0 OUT=

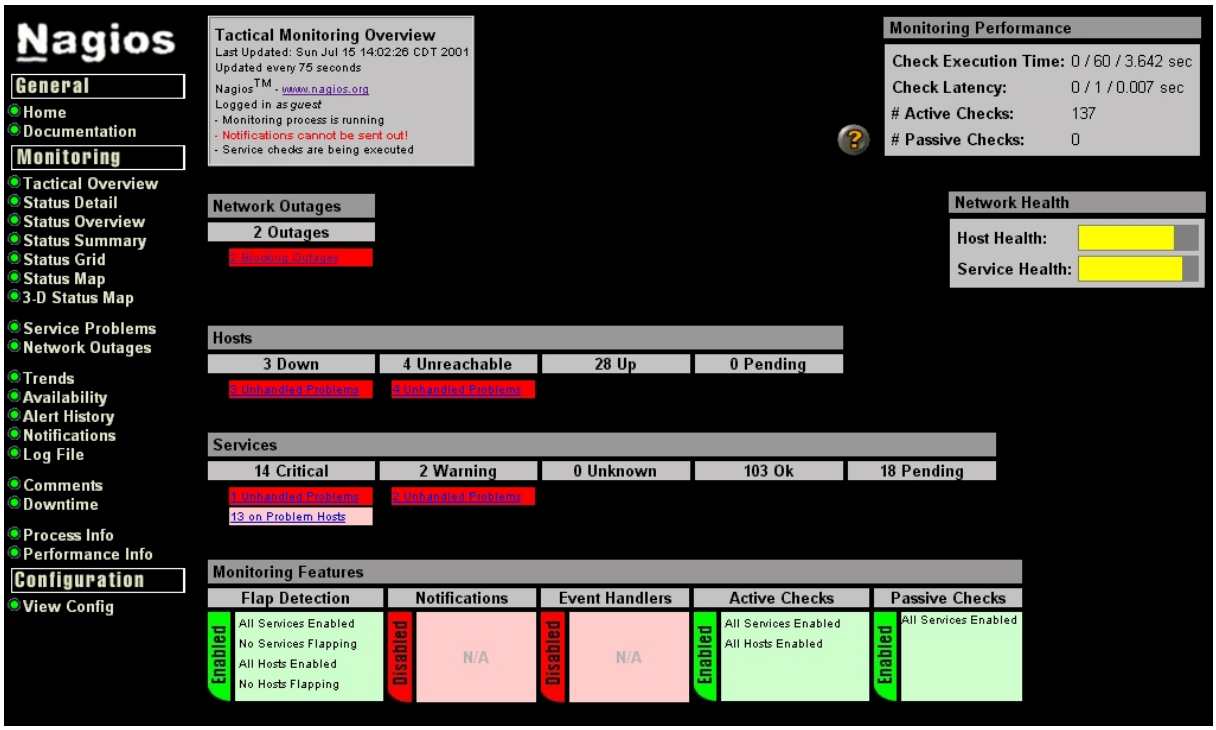
MAC=00:10:a4:6f:73:5e:00:80:3f:57:eb:f7:08:00 SRC=10.17.18.19

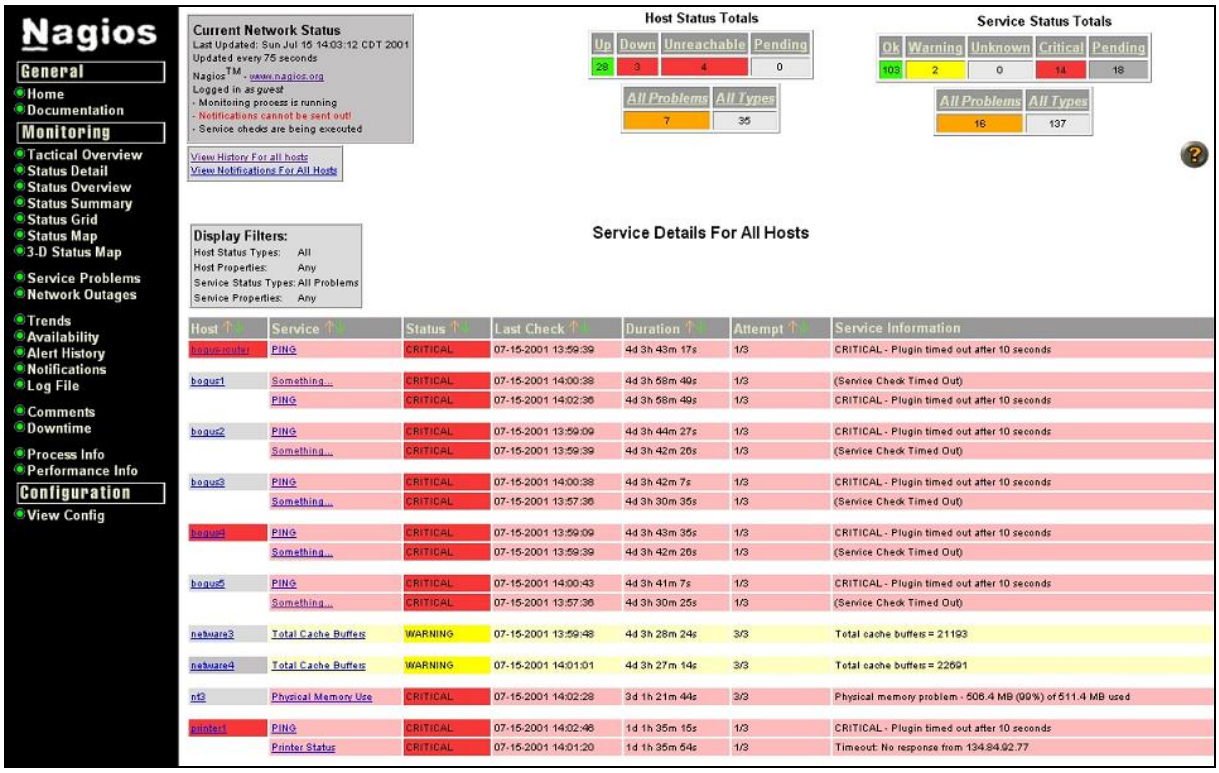
DST=10.10.10.42 LEN=40 TOS=0x00 PREC=0x00 TTL=253 ID=16146 DF

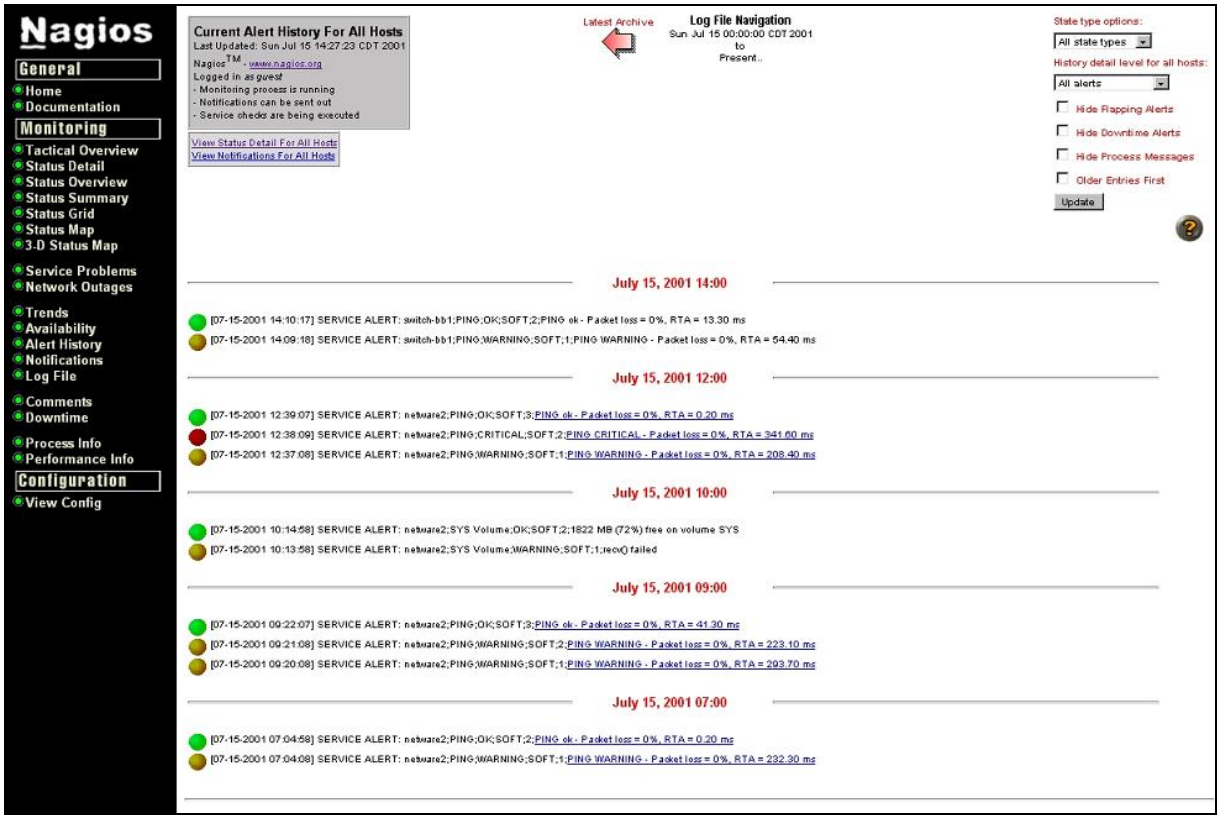
PROTO=TCP SPT=46801 DPT=80 WINDOW=8760 RES=0x00 ACK FIN URGP=0

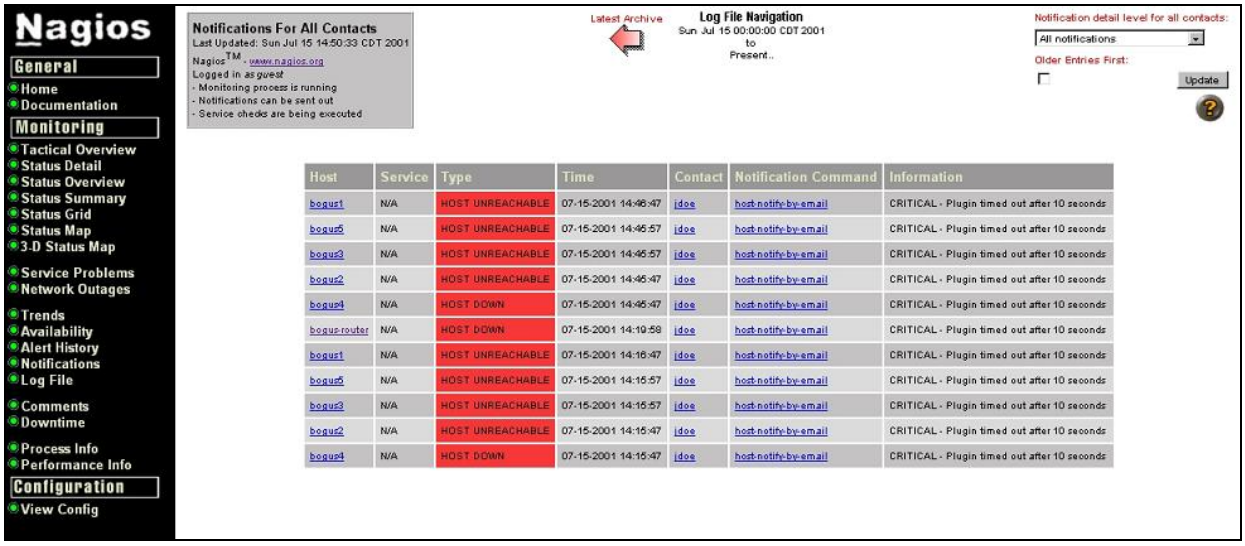
Del av loggrad	Vad den innebär
Apr 28 15:41:38	Datum och tid för det aktuella paketet.
mindator kernel:	mindator är datorns namn, kernel talar om att loggraden kommer från linuxkärnan (brandväggsskyddet i linuxkärnan).
IN=eth0	Talar om att trafiken kom in på nätverksinterfacet eth0 .
OUT=	Om trafiken går ut via något interface kommer OUT att visa vilket interface det går ut via.
MAC=00:10:a4:6f:73:5e:00:80:3f:57:eb:f7:08:00	Den första delen, 00:10:a4:6f:73:5e:, är mindator:s MAC-adress. Den andra delen är den avsändande dators MAC-adress om den finns på samma nät, annars är det defaultrouterns MAC-adress.
SRC=10.17.18.19	Är avsändande dators IP-adress.
DST=10.10.10.42	Är mottagande dators IP-adress
LEN=40	Längden på paketet.
TOS=0x00	TOS är Type Of Service-fältet i IP-paketet.
PREC=0x00	-
TTL=253	Paketets Time To Live
ID=16146	TCP-paketets sekvensnummer
DF	Don't Fragment-flaggan är satt, det vill säga paketet får inte fragmenteras (delas upp i flera delar).
PROTO=TCP	Vilket protokoll det rör sig om. I detta exempel är det TCP-trafik.
SPT=46801	Avsändarport
DPT=80	Mottagarport
WINDOW=8760	Fönsterstorleken för TCP.
RES=0x00	-
ACK FIN URGP=0	Flaggorna ACK, FIN är satta och Urgentflaggan är 0.

Bilaga H Övervakningsprogram Nagios






Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Status Detail
Status Overview
Status Summary
Status Grid
Status Map
3-D Status Map
Service Problems
Network Outages
Trends
Availability
Alert History
Notifications
Log File
Comments
Downtime
Process Info
Performance Info
Configuration
View Config
Current Alert History For All Hosts
Last Updated: Sun Jul 15 14:27:23 CDT 2001
Nagios™ - www.nagios.org
Logged in as guest
- Monitoring process is running
- Notifications can be sent out
- Service checks are being executed
View Status Detail For All Hosts
View Notifications For All Hosts
Latest Archive
Log File Navigation
Sun Jul 15 00:00:00 CDT 2001
to
Present..
State type options:
All state types
History detail level for all hosts:
All alerts
Hide Flapping Alerts
Hide Downtime Alerts
Hide Process Messages
Older Entries First
Update
July 15, 2001 14:00
[07-15-2001 14:10:17] SERVICE ALERT: switch-bb1;PING;OK;SOFT;2;PING ok - Packet loss = 0%, RTA = 13.30 ms
[07-15-2001 14:09:18] SERVICE ALERT: switch-bb1;PING;WARNING;SOFT;1;PING WARNING - Packet loss = 0%, RTA = 54.40 ms
July 15, 2001 12:00
[07-15-2001 12:39:07] SERVICE ALERT: netware2;PING;OK;SOFT;3;PING ok - Packet loss = 0%, RTA = 0.20 ms
[07-15-2001 12:38:09] SERVICE ALERT: netware2;PING;CRITICAL;SOFT;2;PING CRITICAL - Packet loss = 0%, RTA = 341.60 ms
[07-15-2001 12:37:08] SERVICE ALERT: netware2;PING;WARNING;SOFT;1;PING WARNING - Packet loss = 0%, RTA = 208.40 ms
July 15, 2001 10:00
[07-15-2001 10:14:58] SERVICE ALERT: netware2;SYS Volume;OK;SOFT;2;1822 MB (72%) free on volume SYS
[07-15-2001 10:13:58] SERVICE ALERT: netware2;SYS Volume;WARNING;SOFT;1;recvQ failed
July 15, 2001 09:00
[07-15-2001 09:22:07] SERVICE ALERT: netware2;PING;OK;SOFT;3;PING ok - Packet loss = 0%, RTA = 41.30 ms
[07-15-2001 09:21:08] SERVICE ALERT: netware2;PING;WARNING;SOFT;2;PING WARNING - Packet loss = 0%, RTA = 223.10 ms
[07-15-2001 09:20:08] SERVICE ALERT: netware2;PING;WARNING;SOFT;1;PING WARNING - Packet loss = 0%, RTA = 293.70 ms
July 15, 2001 07:00
[07-15-2001 07:04:58] SERVICE ALERT: netware2;PING;OK;SOFT;2;PING ok - Packet loss = 0%, RTA = 0.20 ms
[07-15-2001 07:04:08] SERVICE ALERT: netware2;PING;WARNING;SOFT;1;PING WARNING - Packet loss = 0%, RTA = 232.30 ms


Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Status Detail
Status Overview
Status Summary
Status Grid
Status Map
3-D Status Map
Service Problems
Network Outages
Trends
Availability
Alert History
Notifications
Log File
Comments
Downtime
Process Info
Performance Info
Configuration
View Config
Notifications For All Contacts
Last Updated: Sun Jul 15 14:50:33 CDT 2001
Nagios™ - www.nagios.org
Logged in as guest
- Monitoring process is running
- Notifications can be sent out
- Service checks are being executed
Latest Archive
Log File Navigation
Sun Jul 15 00:00:00 CDT 2001
to
Present..
Notification detail level for all contacts:
All notifications
Older Entries First:
Update
Host | Service | Type | Time | Contact | Notification Command | Information
bogus1 | N/A | HOST UNREACHABLE | 07-15-2001 14:46:47 | jdoe | host-notify-by-email | CRITICAL - Plugin timed out after 10 seconds
bogus5 | N/A | HOST UNREACHABLE | 07-15-2001 14:46:57 | jdoe | host-notify-by-email | CRITICAL - Plugin timed out after 10 seconds
bogus3 | N/A | HOST UNREACHABLE | 07-15-2001 14:46:57 | jdoe | host-notify-by-email | CRITICAL - Plugin timed out after 10 seconds
bogus2 | N/A | HOST UNREACHABLE | 07-15-2001 14:46:47 | jdoe | host-notify-by-email | CRITICAL - Plugin timed out after 10 seconds
bogus4 | N/A | HOST DOWN | 07-15-2001 14:46:47 | jdoe | host-notify-by-email | CRITICAL - Plugin timed out after 10 seconds
bogus-router | N/A | HOST DOWN | 07-15-2001 14:19:58 | jdoe | host-notify-by-email | CRITICAL - Plugin timed out after 10 seconds
bogus1 | N/A | HOST UNREACHABLE | 07-15-2001 14:16:47 | jdoe | host-notify-by-email | CRITICAL - Plugin timed out after 10 seconds
bogus5 | N/A | HOST UNREACHABLE | 07-15-2001 14:15:57 | jdoe | host-notify-by-email | CRITICAL - Plugin timed out after 10 seconds
bogus3 | N/A | HOST UNREACHABLE | 07-15-2001 14:15:57 | jdoe | host-notify-by-email | CRITICAL - Plugin timed out after 10 seconds
bogus2 | N/A | HOST UNREACHABLE | 07-15-2001 14:15:47 | jdoe | host-notify-by-email | CRITICAL - Plugin timed out after 10 seconds
bogus4 | N/A | HOST DOWN | 07-15-2001 14:15:47 | jdoe | host-notify-by-email | CRITICAL - Plugin timed out after 10 seconds