Anders Berndt

Arena College
Vårterminen 2003

Analys av IT-säkerheten i

Advokatfirma
Rosén och Lagerbielke

med förslag till
riskreducerande åtgärder och införande
av informationssäkerhetspolicy.

Konsultfirma
IT - Security

Innehållsförteckning

Inledning

I den här rapporten redovisar vi våra tankar kring Advokatfirma Rosén och Lagerbielke ur ett informationssäkerhetsperspektiv. Det innebär att vi har tittat på informationshanteringen i firman med hjälp av dessa tre ledord:

1. Sekretess – att information är tillgänglig endast för dem som har behörighet.
2. Riktighet – att information förblir korrekt och fullständig.
3. Tillgänglighet – att behöriga användare har tillgång till information när de behöver den.

Detta är grunden i allt informationssäkerhetsarbete, och kan verka vara självklarheter. Men det är lätt hänt att säkerheten brister. Har det inte hänt något allvarligt på länge är det lätt att slå sig till ro och tänka att allt fungerar som det ska.

Det är ett stort och ständigt pågående arbete att hålla hög säkerhet i ett företag, men absolut nödvändigt om det är ett företag som förfogar över så dyrbara resurser som Advokatfirma Rosén och Lagerbielke. Inget företag eller organisation har råd att förlora sina investeringar på grund av brister i säkerhetsarbetet.

Advokatfirman är välmående, åtnjuter stort förtroende hos kunder i Sverige såväl som utomlands, och bedriver sin verksamhet i ett vackert sekelskifteshus i centrala Malmö. På senare tid har man expanderat med nyanställningar och upprättande av kontor i Köpenhamn. Denna utveckling är naturligtvis till glädje, men innebär också nya och viktiga utmaningar för de som arbetar med informationssäkerheten i firman.

Vi på konsultfirma IT-Security vill peka på vad vi anser är brister i säkerheten som behöver åtgärdas. En första riskanalys presenteras, och en åtgärdskalender för det mest akuta föreslås.

Säkerhetsarbete går hand i hand med allt annat arbete på ett företag, och därför måste alla anställda vara involverade. Därför kommer vi att föreslå hur en säkerhetspolicy kan utformas, som alla anställda får ta del av och bekräfta att de ställer upp på.

En säkerhetsorganisation för att administrera det hela måste också finnas, och vi föreslår hur den bör vara sammansatt.

Riskanalys

Riskanalysen är ett centralt dokument. Det ligger till grund för beslut om vilka åtgärder som kommer att vidtas för att säkra firmans resurser, och i vilken ordning detta ska ske. Vad man vill få fram är vad det kostar att skydda sig, jämfört med vad det kostar att inte ha skyddat sig när olyckan är framme.

Advokatfirman Rosén och Lagerbielke förfogar över resurser som överlag representerar mycket stora värden, både ekonomiskt och förtroendemässigt. Detta är naturligtvis värt att skydda. Dock kan dessa skyddsåtgärder vara olika kraftfulla och ha olika kostnader, och det gäller att komma fram till en bra balans mellan funktion och pris.

Detta är en preliminär och förenklad riskanalys. De faktiska värdena på Advokatfirma Rosén och Lagerbielkes resurser är naturligtvis för oss okända, och den ovannämnda balansen mellan funktion och pris uppnår vi under gemensamma diskussioner. Dock ger tabellen redan nu en fingervisning om var i firman säkerhetsarbetet bör ta sin början.

I tabellen nedan har ställts upp en del av firmans resurser, vilka hot som föreligger mot dessa, hur troligt det är att dessa hot realiseras, och vilka de negativa konsekvenserna i så fall blir. Skalan löper från 1 (ingen eller ringa) till 5 (total eller mycket stor). I den sista kolumnen står ett värde som är summan av sannolikheten och konsekvensen, och ger ett mått på total risk. Ju högre total risk, desto större förlust vid olycka.

Resurs	Hot	Sannolikhet	Konsekvens	Summa
Personal	Brand	4	5	20
	Rån	4	5	20
Byggnader, rum	Brand	4	5	20
	Vattenskada	4	4	16
Arkiv	Stöld	3	4	12
Kassavalv	Stöld	4	4	16
Dokument	Stöld	4	4	16
Datorer	Stöld	3	2	6
	Intrång	5	4	20
	Korruption	5	4	20
Data	Stöld	4	4	16
	Korruption	5	4	20
Backup	Stöld	3	5	15
	Korruption	4	5	20
Nätverk	Intrång	5	4	20
	Korruption	5	4	20

Åtgärdskalender

I riskanalysen har framkommit vilka resurser som måste skyddas och vilka hot de förr eller senare riskerar att utsättas för. Det är en stor uppgift att säkra allt, det måste göras, men vissa saker är det mer bråttom med än andra.

Vi redovisar här en kalender över de viktigaste åtgärderna, de som vi anser måste vidtas utan dröjsmål för att minimera riskerna för snara incidenter. De listas i prioriteringsordning, med en kort förklaring och beräknad tid för utförande.

Åtgärd		Beskrivning	Uppskattad arbetstid
1.	Backup på server och klienter, samt verifiering av återställningsfunktion.	Då viktig data finns lagrad på i stort sett alla datorer i företaget, och det inte är säkert att backup har blivit gjord eller fungerar för återställning, måste detta säkras innan något annat.	5 dagar
2.	Installation av enkel brandvägg och antivirusprogram.	Det lokala nätverket är helt oskyddat mot intrångsförsök och virusspridning. Det måste stängas för åtkomst utifrån och genomsökas efter eventuella virus. Då arkitekturen på nätverket troligen kommer att ändras senare, räcker det med en enkel och billig brandväggskonfiguration nu, som går snabbt att installera.	3 dagar
3.	Låsning av dörrar och flytt av kassaskåp.	Olåsta dörrar och kassaskåp i gatuplanet inbjuder till rånförsök, varvid personalens hälsa och viktiga dokument riskeras. Dessutom skulle en flytt till en mer central och säker plats vara ett första steg ifrån vanan att spara dokument på klientdatorerna.	En timme

Under arbetet med riskanalysen har det framkommit att el- och teleinstallationer samt vattenstammar uppvisar stora brister, och att det inte finns några som helst larmanordningar. Det har förekommit störningar och läckage tidigare och detta kan enligt vår bedömning inträffa igen, i stort sett när som helst.

Vi vill understryka att för att säkerhetsarbetet i Advokatfirma Rosén och Lagerbielke ska vara verkningsfullt, och att firman inte ska riskera att förlora sina värdefulla resurser är det av största vikt att dessa brister åtgärdas. Dessa arbeten ligger utanför vår verksamhet och är därför inte med i åtgärdskalendern ovan, men vi rekommenderar gärna företag som vi har haft gott samarbete med tidigare.

Säkerhetspolicy

För att få en heltäckande grund att stå på i säkerhetsarbetet formuleras en informationssäkerhetspolicy. Detta arbete sker i samarbete med Advokatfirma Rosén och Lagerbielkes ledning och ska hela tiden återspegla firmans verksamhetspolicy. Hela organisationen omfattas och genomsyras av detta dokument, som måste läsas och bekräftas av alla, inte minst nyanställda.

Vi visar här ett exempel på hur en sådan säkerhetspolicy kan se ut. Den riktiga kommer alltså att utarbetas av hela säkerhetsorganisationen i samarbete.

Informationssäkerhetspolicy för Advokatfirma Rosén och Lagerbielke

Daterad 2003-03-19
Personal ska tilldelas ett personligt exemplar av informationssäkerhetspolicyn.
Policyn kommer att presenteras vid interna möten under hösten.

Motiv
Anställda på Advokatfirma Rosén och Lagerbielke använder IT för att stödja, utveckla och effektivisera verksamheten. Vårt företag är beroende av informationsbehandlingen. Kraven på snabb och relevant information inom olika funktioner av Advokatfirma Rosén och Lagerbielkes verksamhet ökar. Att säkerställa hög tillgänglighet och samtidigt innehålla nödvändiga krav på sekretess är väsentligt ur affärssynpunkt och för att skydda våra klienter.

Definition
Informationssäkerhet inbegriper all säkerhet kring Advokatfirma Rosén och Lagerbielkes totala informationsbehandling av uppdrag från klienter. Såväl organisatoriska åtgärder som fysiska och logiska skyddsåtgärder inbegrips.
Exempel på säkerhetsrelaterade åtgärder är en fastställd säkerhetspolicy, ansvarsfördelning, utbildning, riskanalys, katastrofplan, behörighetsregler, informationsklassning, säkrad driftmiljö, åtkomstskydd i datorer, regler för hantering av datamedia, behörighetsadministration, säkerhetskopiering, regler för extern kommunikation och modemuppkopplingar etc. och kontroll av uppgiven identitet vid till exempel påloggning med hjälp av aktiva kort (förstärkt autentisering).
För att tillgodose kraven som ställs på informationssystemen, där så gott som all Advokatfirma Rosén och Lagerbielkes information hanteras på ett eller annat sätt, är det nödvändigt att hanteringen av information sker på ett så tillförlitligt sätt som möjligt. Informationssäkerheten ska motverka risker för såväl obehörig läsning och förändring av data som för förlust av data. Informationssäkerheten syftar även på informationens kvalitet, riktighet och tillgänglighet.
Nyckelord för informationssäkerheten är att säkra informationens

- *sekretess,*
- *tillgänglighet,*
- *riktighet,*
- *spårbarhet.*

Informationssäkerhetspolicyn utgör ett komplement till Advokatfirma Rosén och Lagerbielkes målbeskrivning och IT-strategi, som anger inriktningen för den totala informationsbehandlingen. Policyn är det grundläggande underlaget för informationssäkerhet och berör samtliga anställda, samarbetspartners och konsulter.
Informationssäkerhetspolicyn ger inriktningen och de övergripande målen för hur informationssäkerhetsarbetet ska bedrivas inom företaget - för verksamheten, personalen, kunderna och samarbetspartners.

Policy för godtagbart bruk
Policy för godtagbart bruk anger vad anställda i Advokatfirma Rosén och Lagerbielke får och inte får göra med firmans informationsresurser.

Det är inte tillåtet att:

- använda Internet för icke-godkänt bruk
- öppna bifogade filer i e-post
- installera icke-godkänd programvara
- använda disketter eller annan flyttbar media som inte viruskontrollerats
- använda telefon och fax för icke-godkänt bruk

För undantag från policyn för godtagbart bruk ska ansvarig i säkerhetsorganisationen lämna tillåtelse. Övervakning av firmans informationsresurser kan ske, och anställda kan inte räkna med att någon information är att betrakta som privat.
Brott mot policyn för godtagbart bruk kan leda till omedelbar uppsägning.

Mål för informationssäkerheten
Målsättningen med denna policy är att säkerställa sekretess, tillgänglighet och spårbarhet för verksamhetens information och data, samt att reducera risken för skador på verksamheten oavsett orsak och angripare.

- Avsikten med denna policy är att skydda organisationens informationstillgångar mot alla typer av hot - interna eller
  externa, avsiktliga eller oavsiktliga.

Säkerhetspolicy

- Det ska finnas skyddsmekanismer som utifrån nedanstående punkter säkerställer informationens

– sekretess,
– tillgänglighet,
– riktighet,
– spårbarhet.

- Informationssäkerhetsarbetet ska bedrivas enligt standarden SS ISO/IEC 17799.
- Alla anställda inom organisationen som i sina arbetsuppgifter berörs av IT ska vara medvetna om informationssäkerhetsfrågornas betydelse samt ha kunskaper om vad som gäller för att bevara och utveckla en säker och stabil IT-miljö.
- Informationssäkerheten ska vara en integrerad del i Advokatfirma Rosén och Lagerbielkes ordinarie verksamhet och stödja verksamheterna i att uppnå de uppsatta målen för kvalitet och effektivitet.
- Till grund för informationssäkerhetsåtgärder ska föreligga dokumenterade bedömningar eller genomförda riskanalyser.

- Skydden för kända hot ska vara uppbyggda till rätt nivå med hänsyn till skyddskostnad och konsekvens för Advokatfirma Rosén och Lagerbielkes verksamhet vid eventuellt tillfogad skada.
- Alla säkerhetsincidenter, konstaterade eller misstänkta, ska rapporteras till och utredas av informationssäkerhetschefen.
- Uppföljning av riskanalyser, skyddsåtgärder och utbildningsinsatser ska ske kontinuerligt.
- En kontinuerlig drift ska garanteras genom att säkerställa driftmiljön för samtliga datordriftställen.
- Advokatfirma Rosén och Lagerbielke ska ha egen IT-personal, det vill säga anställda med rätt kompetens och som fortlöpande utbildas i takt med att datorsystemen utökas och förändras.
- Känslig data ska skyddas mot otillbörlig åtkomst inom och utom företaget med hjälp av behörighetskontroll och i vissa fall kryptering.
- Säkerhetsarbetet ska skydda personalen i dess tjänsteutövning.
- Kommunikationslösningar ska vara gjorda så att resursdatorer och nätverk skyddas mot driftsstörningar och intrång. Driftstörningar och intrång ska kunna följas upp med hjälp av dokumenterad historik (loggar).
- Man ska leva upp till gällande lagar och kommersiell sekretess. Exempelvis ska personuppgiftslagen (PUL) följas så att den personliga integriteten beaktas i användningen av personregister. Bokföringslagen ska följas vad gäller ansvarsfördelning och behandlingshistorik för att uppnå en tillförlitlighet och en god intern kontroll av redovisningen.

Omfattning
Informationssäkerhetspolicyn rör all informationsbearbetning oavsett driftmiljö, alltså oberoende av om datorbearbetningen sker i resursdator (stor-, minidator, eller server) eller persondator. Policyn gäller även om datorbearbetningen sker externt och via datakommunikation eller motsvarande. Med datorbearbetning menas hela informationssystemet: system-/programutveckling, källdataframställning, registrering, dataöverföring, bearbetning, datalagring, utdatahantering, arkivering och makulering.

Genomförande
För att nå de uppsatta målen ska resurser avdelas för att systematisk genomföra
- riskbedömningar och konsekvensanalyser
- riktlinjer och handlingsplan
- informationssäkerhetshöjande åtgärder
- utbildning och information

Årligen ska en plan för säkerhetsarbetet inom varje avdelning upprättas. Planen ska innehålla en beskrivning av säkerhetsläget samt de planerade åtgärderna som ska vidtas för att höja säkerhetsnivån. Planerna sammanställs till en handlingsplan och en budget för informationssäkerheten för hela Advokatfirma Rosén och Lagerbielke.
Ledningen fattar beslut om planen, dess genomförande och budget.

Övergripande ansvar
Företagsledningen är ytterst ansvarig för mål och ramar för informationssäkerhetsarbetet och bär det yttersta ansvaret för skador som kan inträffa. Ledningen följer upp informationssäkerhetsläget genom att ta del av säkerhetsplanen.

Ansvarsfördelning
Informationssäkerhetschefen sammanställer avdelningarnas säkerhetsplaner och upprättar en säkerhetsplan för hela Advokatfirma Rosén och Lagerbielke samt svarar för initiering och uppföljning av informationssäkerhetsarbetet enligt planen.
Informationssäkerhetssamordnaren är ansvarig för att informationssäkerhetsåtgärder genomförs enligt ledningens och informationssäkerhetschefens beslut. Samordnaren ska leda informationssäkerhetsarbetet inom respektive tilldelat ansvarsområde och är även registeransvarig för avdelningens personregister.
Den system-/driftansvarige har det operativa ansvaret för att beslutade åtgärder genomförs. Ansvaret kan gälla ett eller flera IT-system. Den ansvarige är skyldig att omgående meddela säkerhetsproblem och misstanke om eller redan inträffade incidenter till informationssäkerhetssamordnaren eller informationssäkerhetschefen.

Klassificering av information och ansvar
Informationen i firman klassificeras i olika nivåer, beroende på känslighet. En ansvarig utses att förvalta respektive nivå.

Känslighetsnivå	Exempel	Skyddskrav	Dataförvaltare
Hemlig	Strategiska planer t.ex. företagsfusioner, utredningar, personal, lönelistor, prissättning och kunder.	Måste etiketteras, datafiler måste vara skyddade med lösenord och kryptering. Dokument måste förstöras när de kastas.	Högre chefer eller personer som de utsett.
Offentlig	Alla annan information	Inga	Annan personal

Säkerhetspolicy
Användaren ska verka för en god informationssäkerhet inom sitt område och följa de regler och riktlinjer som gäller inom Advokatfirma Rosén och Lagerbielke. Nivån på informationsskyddet inom företaget beror på hur varje enskild person hanterar verktygen för informationsbehandling såsom datorer, disketter, datakommunikation, cd-roms, cd-rw, e-post, fax, etc.

Dotterbolag/partners
I enlighet med företagsägarnas enhälliga beslut vid fastställandet av denna policy år 2003, gäller samma informationssäkerhetspolicy för dotterbolag och partners.

Policyns giltighet
Planering av framtida IT-strategier ska ske i samarbete med respektive företagsledning. Informationssäkerhetschefen ska arbeta för att informationssäkerheten i samtliga bolag uppnår jämlika nivåer till det fjärde kvartalet 2003. Revidering av informationssäkerhetspolicyn samt riktlinjerna kommer att göras därefter för att i ny upplaga börja gälla from 2004.

Säkerhetsorganisation

För att administrera säkerheten i firman inrättas en säkerhetsorganisation, som bör bestå av personer från ledningen och samtliga avdelningar. Finns säkerhetsmässig och teknisk kompetens bland kandidaterna är det naturligtvis bra, men övergripande administrativt ansvar är det viktigaste. Vi erbjuder support i många former, och en av dem kan vara som säkerhetsteknisk rådgivare och kontaktperson till Advokatfirma Rosén och Lagerbielkes säkerhetsorganisation.

IT-Security har även olika sorters utbildning inom IT på sitt program. Om behov visar sig finnas, föreslår vi därför att vi får förtroendet att hålla i ett par specialanpassade kurser för Advokatfirma Rosén och Lagerbielkes medarbetare. Det är viktigt att all personal genomgår en grundkurs i IT-säkerhet, dels för att lära sig nya rutiner men kanske framförallt för att få ett delvis nytt säkerhetstänkande med sig.

Det vore dock önskvärt att någon i personalen fick mer teknisk utbildning för att kunna axla det operativa ansvaret i säkerhetsorganisationen. Det är denna person som blir IT-Securitys kontaktperson i den vardagliga driften av Advokatfirma Rosén och Lagerbielkes datornätverk. Alternativet är att en systemtekniker anlitas, och om önskemål finns kan det arbetet naturligtvis utföras av en av våra tekniska konsulter.

Advokatfirma Rosén och Lagerbielke har i sin organisation mycket värdefullt kapital: kunskapsmässigt, förtroendemässigt såväl som ekonomiskt. Att skydda detta kapital är självklart oerhört viktigt, men att se och hålla reda på alla faror som hotar och att prioritera, bedöma och bestämma om åtgärder mot dem, är något som de flesta firmor inte har tid eller möjlighet att klara av på egen hand.

IT-Security har många års erfarenhet av att ta hand om företags informationssäkerhetsskydd. Vi gör det effektivt, vi gör det heltäckande, och vi gör det på era villkor. IT-security blir ett tryggt val för Advokatfirma Rosén och Lagerbielke.