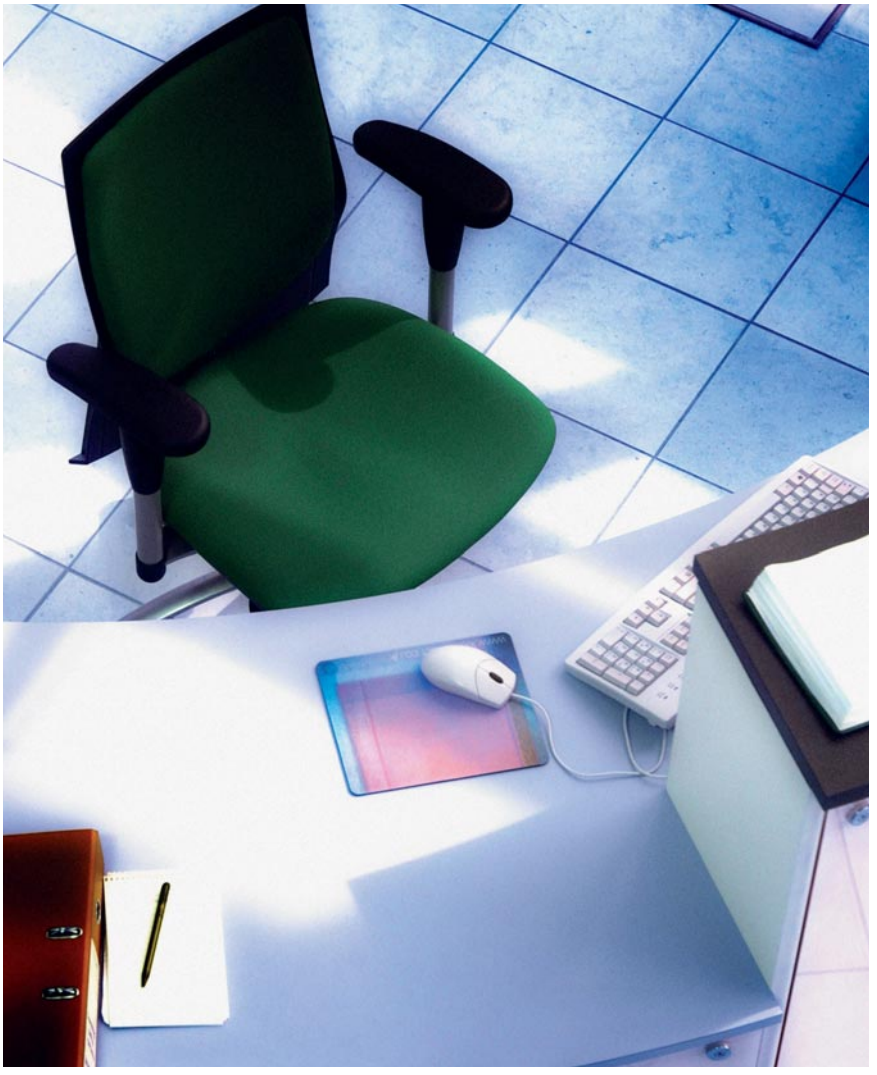
De digitala **spåren avslöjar** stölderna

Före detta anställda tar med sig företagshemligheter i form av kundregister, utvecklingsdokumentation eller affärsplaner. Med hjälp av ett USB-minne kan en illojal anställd tömma företagets datorer på hemligheter i digital form på femton minuter och få en flygande start i en konkurrerande verksamhet. Ofta finns det misstankar men det kan vara svårt att finna konkreta bevis. I den här artikeln beskriver **Göran Fornbrandt** och **Henrik Bengtsson** de tekniska och juridiska metoder de framgångsrikt har använt för att hjälpa företag som råkat ut för angrepp.



Beroende på verksamhetsinriktning kan ett företags hemligheter, i form av digitalt sparad data, vara en av de största tillgångarna. Några exempel på röjande av företagshemligheter som kan få ödesdigra konsekvenser är röjande av ritningar till en ny produkt som kan innebära att konkurrentens utvecklingstid kan halveras, röjande av kundregister som gör det enkelt för en konkurrent att approchera rätt kunder och kontaktpersoner eller röjande av priser vilket gör att en konkurrent lätt kan lägga sina priser strax under företagets prislista. Just kundregister är den hemlighet som det oftast tvistas om i domstolarna.

Numera kan en illojal anställd eller konsult tömma ett helt IT-system på information under en timme. Få företag stänger av USB-portarna på sina datorer och det gör det lätt att ansluta externa minnen eller lagringsmedia. Och förvånansvärt många anställda är medvetna om vilka allvarliga rättsliga konsekvenser ett röjande av företagshemligheter kan få.

SVERIGE HAR SEDAN 1990 en särskild lag om skydd för företagshemligheter, (FHL). Lagen tillämpas numera ganska ofta av företag som råkat ut för att anställda, konsulter, samarbetspartners eller konkurrenter röjt eller utnyttjat företagshemligheter.

FÖRUTSÄTTNINGEN för att information i rättslig mening skall vara en företagshemlighet är

- att det är information i näringsidkarens rörelse
- att informationen hållits hemlig
- att den som innehar information kan skadas om informationen kommer ut till tredje part

NÅGRA EXEMPEL på information som domstolarna ansett vara företagshemligheter är

- Affärsplaner
- Ritningar
- Kundregister
- Konsultregister
- Offerter, pris och kalkylunderlag
- Kundakter

ANLEDNINGEN till att en computer forensisk undersökning inleds, är oftast att företaget har fattat misstanke om att en före detta anställd har tagit med sig någon form av företagshemligheter och som sedan dyker upp inom ett konkurrerande bolag. Vid upptäckten infinner sig ofta panik och företaget vill omedelbart reda ut vad som hänt. I ett sådant skede är det viktigt att företaget agerar rätt.

ALL TEKNISK UTRUSTNING som innehåller någon form av minnesfunktion lagrar i någon form information om hur utrustningen använts. Information lagras i datorer, handdatorer, mobiltelefoner, SIM-kort i telefoner och USB-minnen, men kan också lagras i faxar och kopiatorer. Normalt fungerar all lagringsmedia på så vis att den information som användaren raderar inte är försvunnen för gott förrän det aktuella området är helt överskriven med ny data. Eftersom lagringsmedia idag ofta är stora (en standardhårddisk rymmer idag allt från 100 GB upp till 1 TB) innebär det att det kan gå lång tid fram till tidpunkten då operativsystemet skriver över just det område som användaren raderade.

När en användare raderar information i papperskorgen i Windows eller sitt e-postprogram innebär det inte alltid att informationen raderas permanent. Effekten av en radering av en fil är att länken mellan filnamnet och ursprunglig lagringsplats klipps av vilket kan liknas med att ta bort innehållsförteckningen ur en bok. Det innebär att det i normalfallet är fullt möjligt att återskapa raderad information. När det gäller e-post finns det dessutom ofta backupkopior på e-postservern som gör att användarens radering kan vara betydelselös.

VILKA DIGITALA SPÅR kan man då finna i exempelvis en dator? Några exempel på information som normalt kan hittas är

- när en fil sparats, kopierats, raderats eller skrivits ut
- hur länge en fil har redigerats
- ögonblicksbilder av webmail
- vilka externa enheter som varit anslutna till en dator, vid vilken tidpunkt de varit anslutna och enhetens serienummer
- sökhistoria på google med enskilda sökord
- Internethistorik, vilka sidor som användaren har surfat mot

EN COMPUTER FORENSICS analys av en dator är en personuppgiftsbehandling i personuppgiftslagens

FORTS.

Ett typiskt ”case”

Det här är ett fiktivt fall som belyser en typsituation där ett företag råkar ut för anställda som tar med sig information när de lämnar sin anställning. Tidningen Båtsommar, som är en annonsfinansierad gratistidning, har under de senaste tre åren ökat sina annonsintäkter med 5 miljoner om året. Företaget går bra men det finns en konflikt mellan vice VD:n och VD:n som inte går att lösa. En dag meddelar vice VD:n att han tänker lämna tidningen för att börja arbeta i sin hustrus familjeföretag, ett charkuteri.

Några dagar efter att vice VD:n sagt upp sig säger två av bolagets annonssäljare upp sig. En månad efter att de lämnat Båtsommar märker annonssäljarna på tidningen att det börjar gå trögt med annonsförsäljningen. Annonsörer som tidigare köpt dubbeluppslag i varje nummer är inte längre intresserade. En månad därefter dyker det första numret av den nya tidningen Båtfantasten upp.

Det visar sig att vice VD:n inte alls börjat i familjeföretaget utan har startat en konkurrerande tidning där Båtsommars tidigare annonssäljare ingår i ledningen. Alla annonsörer i Båtfantasten är Båtsommars gamla kunder. VD:n får en stark misstanke att vice VD:n och annonssäljarna har tagit med sig tidningens register över annonsörer och kontaktar en advokat för att se om det går att göra något åt situationen.

Bolaget har bytt datorer i samband med att vice VD:n och annonssäljarna hoppade av och därför finns deras gamla datorer i Båtsommars källare. Advokaten frågar om det finns några konkreta bevis på att avhopparna tagit med sig information. Eftersom det inte finns rekommenderar han att avhopparnas datorer skall lämnas till computer forensics analys för att se om det finns några digitala spår av vad avhopparna haft för sig innan de lämnade sin anställning. Analysföretaget gör en spegel av avhopparnas datorer och går igenom dem. Resultatet av datoranalysen visar:

- Bland de raderade dokumenten på vice VD:ns dator finns ett power point dokument som heter ”Affärsplan Investerare Båtsommar.ppt” som skapats fem månader innan vice VD:n sade upp sig.
- vice VD:n har raderat ett e-brev som han har skickat till sin privata hotmailadress. I bilagan till e-brevet finns dokumentet ”Annonspriser.xls” som innehåller samtliga annonspriser som Båtsommar haft de senaste tre åren.
- en av annonssäljarna har ”accessat” 660 dokument på bolagets server mellan 01.15 och 02.09 en söndag natt två veckor innan han lämnade tidningen. Mellan 00.54 och 02.11 har en extern hårddisk av märket X varit ansluten till annonssäljarens dator. Bland de ”accessade” dokumenten finns två excelfiler, en som innehåller alla tidningens annonsörer.

NÅGRA DAGAR SENARE mailar en av Båtsommars annonsörer en skannad kopia av ett annonserbjudande från Båtfantasten. Adressen till annonsören är felstavad och skriven med versaler. När VD:n kontrollerar mot Båtsommars annonsregister innehåller registret samma felstavning och adressen i registret är också skriven med versaler vilket inte andra adresser i registret är.

Advokaten förbereder en ansökan om intrångsundersökning och interimistiskt förbud utan motpartens hörande. Västmanlands tingsrätt bifaller yrkandena och två dagar senare gör Kronofogden ett tillslag i Båtfantastens nya kontor. På datorerna återfinns dokumentet Annonspriser.xls och de 660 dokument som annonssäljaren hade ägnat söndag natt att kopiera. Båtfantasten överklagar beslutet om vitesförbud och intrångsundersökning men hovrätten ändrar inte tingsrättens beslut. Båtfantastens advokat hör av sig och meddelar att vice VD:n vill förlika tvisten.

Båtfantasten får betala 1,2 miljoner i skadestånd och accepterar att skicka ett pressmeddelande där man ber Båtsommar om ursäkt för att man tagit med sig bolagets företagshemligheter. Båtfantastens annonsörer vill inte fortsätta annonsera i tidningen och ett halvår senare går Båtfantasten i konkurs. ●

(PUL) mening. Det innebär att behandlingen för att vara tillåten måste inrymmas under något av undantagen i PUL.

Datainspektionens uppfattning är att en arbetsgivare normalt får ta del av arbetstagares privata elektroniska kommunikation för att kontrollera och övervaka anställdas användning av Internet och e-postsystem genom loggning av tekniska eller säkerhetsmässiga skäl eller vid allvarlig misstanke om illojalt eller brottsligt beteende.

Däremot är en arbetsgivare alltid skyldig att informera om att man gör sådana kontroller. Informationen kan lämnas i ett anställningsavtal, personalhandbok, IT-policy eller inom fyra veckor efter att analysen är genomförd. Det är inte tillåtet att analysera anställdas privata datorer eller hem-PC eftersom det kan betraktas som dataintrång eller egenmäktigt förfarande.

VAD GÖR MAN om företaget råkat ut för ett angrepp på företagshemligheter? Den första åtgärden bör alltid vara att ta hand om före detta anställdas datorer och förvara dem säkert så att datorn inte används. Man bör absolut inte på egen hand leta efter bevis om att information förts ut eftersom det påverkar tidsstämplar på hårddisken och det kan göra att de digitala spåren försvinner eller får ett sämre bevisvärde.

Därefter får man ta ställning till om man vill ta till kraftfulla rättsliga åtgärder i form av så kallad intrångsundersökning (en razzia där man får söka efter bevisning bland annat i motpartens datorer som genomförs av kronofogden efter domstolsbeslut) eller interimistiskt förbud (ett summariskt förbud som kan meddelas av domstolen efter en relativt kort prövning) mot att angripa företagshemligheter.

DET BÄSTA SÄTTET att skydda företagshemligheter är naturligtvis att begränsa informationen till endast de medarbetare som har ett direkt behov av den för att klara sina arbetsuppgifter, uppdrag eller andra avtalsåtaganden. Ett vanligt sätt är att anställda tilldelas unika konton och användarprofiler som innebär att de endast har tillgång till de områden på servern som är nödvändiga för att utföra arbetsuppgiften.

Företaget kan också använda sig av programvara som övervakar vilka filer som flyttas över till externa lagringsmedia genom datorernas USB-portar genom att installera programvara som USB Monitor. De anställda bör informeras om att programvaran har installerats och där effekten förmodligen blir att de anställda inser att angrepp på företagshemligheterna direkt kan spåras.

INFORMATION som kundregister eller utvecklingsritningar kan dock behöva spridas till en större del av personalen. I sådana fall bör man se till

- att all personal skrivit under sekretessavtal där det framgår att sekretessen även gäller när anställningen har upphört (omkring 1,5 år är den längsta skyddstid man kan avtala om)
- att det på intranät eller i personalhandbok finns en sekretesspolicy som anger vilken information som är bolagets företagshemligheter och hur anställda får handskas med sådan information genom att maila den till sig själva, till tredje part eller ladda ned informationen på lagringsmedia
- att vd eller personalchef har ett avslutningssamtal med anställda som sagt upp sig där man gör klart (i) att ingen information får tas med (ii) att alla externa lagringsmedia återlämnats och (iii) att det inte finns någon information på den anställdes privata datorer eller annars hos den anställde. Ofta får anställda ta med sig egna mallar eller kursdokumentation. I sådana fall bör det dokumenteras skriftligen, exempelvis genom ett e-mail till den anställde, vilken information den anställde få ta med sig. Ibland får anställda köpa företagets gamla datorer när de slutar. Informationen på sådana datorer bör raderas genom programvara som hindrar återskapande av raderad information.

Göran Fornbrandt är ansvarig för affärsområdet Computer Forensics inom Ibas. Göran har lång erfarenhet av kvalificerat utredningsarbete, både från sitt tidigare arbete som polis, samt inom Ibas och Ernst & Young där inriktningen har varit utredningar inom computer forensics och ekonomiska oegentligheter.

Henrik Bengtsson är advokat och delägare vid Advokatfirman Delphi. Han är expert i utredningen om översyn av lagen om skydd för företagshemligheter och har bland annat skrivit boken *Åtgärder vid immaterialrättsintrång* och artikeln *Interimistiska förbud och bevissäkring vid angrepp på företagshemligheter* i Juridisk tidskrift.

I ETT ANTAL rättsfall har det visat sig att felstavningar i kundregister är ett effektivt bevis om att en före detta anställd tagit med sig företagshemligheter. Om den nya verksamheten gjort utskick med samma oförklarliga stavfel eller redigeringsfel som den gamla arbetsgivaren hade i sina register, blir det svårt för angriparen att förklara sig. En annan metod som förekommer är att den som vill skydda ett kundregister lägger in adresser till någon förtrogen bekant som kommer att få utskick om en anställd olovligen för med sig kundregistret. ●