



Säkerhetspolisen

# FÖRETAGSSPIONAGE

Juni 2005

Rapportserie  
2005:3

<b>1</b>	<b>INLEDNING</b> .....	<b>3</b>
<b>2</b>	<b>SVERIGE</b> .....	<b>4</b>
2.1	ATT SKYDDA SVENSK BIOTEKNIK .....	4
2.2	SKYDD FÖR FÖRETAGSHEMLIGHETER .....	4
2.3	BRISTANDE IT-SÄKERHET HOS MYNDIGHETER OCH NÄRINGSLIV .....	4
2.4	SKATTEVERKET RÄTT TILL FÖRETAGSINFORMATION .....	4
2.5	MYNDIGHET TVINGAS LÄMNA UT KUNDLISTA .....	5
2.6	DATAHACKARE DÖMD FÖR FÖRETAGSSPIONERI .....	5
2.7	MISSTÄNKT STÖLD AV AFFÄRSHEMLIGHETER .....	5
2.8	MISSTÄNKT FÖRETAGSSPIONAGE INOM RESEBRANSCHEN .....	5
2.9	MEDIEBYRÅ STÄMMER FÖRE DETTA ANSTÄLLD .....	5
2.10	KONKURRENT ANKLAGAS FÖR STÖLD AV FÖRETAGSHEMLIGHETER .....	5
2.11	KVARGLÖMDA DATORER I TAXIBILAR .....	6
2.12	KÄNSLIG FÖRSVARSSINFORMATION SPREDS VIA INTERNET.....	6
<b>3</b>	<b>EUROPA</b> .....	<b>6</b>
3.1	DANSKT FÖRETAG UTSATT FÖR MISSTÄNKT FÖRETAGSSPIONAGE .....	6
3.2	RADERADE HÅRDDISKAR INNEHÅLLER FÖRETAGSINFORMATION .....	6
3.3	GÄSTSTUDENT MISSTÄNKT FÖR FÖRETAGSSPIONAGE .....	6
3.4	FRANKRIKE STÖDER INHEMSK INDUSTRI .....	7
<b>4</b>	<b>USA</b> .....	<b>7</b>
4.1	AMERIKANSKA FARHÅGOR OM KINESISKT FÖRETAGSSPIONAGE.....	7
4.2	MILJARDSKADESTÅND FÖR STÖLD AV FÖRETAGSHEMLIGHETER .....	7
4.3	FÖRETAGSSPIONAGE INOM AMERIKANSK BILINDUSTRI.....	7
4.4	FÖRE DETTA ANSTÄLLD DÖMD FÖR DATAINTRÅNG .....	7
4.5	INFORMATIONSFÖRETAG UTSATT FÖR DATAINTRÅNG .....	8
4.6	BRISTANDE SÄKERHET VID AMERIKANSKA SKATTEVERKET .....	8

## 1 Inledning

Rapporten bygger på ett urval av artiklar kopplade till informations säkerhet eller företagsspionage. Artiklarna är publicerade i svensk och internationell press under vintern och våren 2005.

Det har förekommit ett flertal fall av misstänkt företagsspionage eller stöld av företagshemligheter både i Sverige och utomlands. Svenska företag utsätts för företagsspionage av både utländska och inhemska konkurrenter i syfte att vinna tekniska och ekonomiska fördelar. Det förekommer också att informationsinhämtning understöds av utländska underrättelsetjänster. Mörkertalet gällande företagsspionage är dock stort och flertalet företag väljer att inte offentliggöra när de blivit utsatta av risk för negativ publicitet.

Bristande IT-säkerhet kopplat till informationsförlust är fortsatt ett av de mest omskrivna problemen och antalet dataintrång utifrån bedöms öka. Samtidigt utgör personal och före detta anställda som gått över till en konkurrent eller startat upp en liknande verksamhet och tagit med sig kritisk information ett allt större hot mot verksamheten.

## 2 Sverige

### 2.1 Att skydda svensk bioteknik

Säkerhetspolisen bedriver ett informativt arbete mot svenskt näringsliv och myndigheter gällande spionage. I samarbete med Inspektionen för strategiska produkter har en serie seminarier genomförts för att uppmärksamma hot riktade mot svensk bioteknik. För att visa hur man med relativt enkla medel kan vidta åtgärder för att skydda sin forskning har Säkerhetspolisen tagit fram broschyren *Att skydda svensk bioteknik*. Broschyren finns tillgänglig på Säkerhetspolisens hemsida, [www.sakerhetspolisen.se](http://www.sakerhetspolisen.se)

### 2.2 Skydd för företagshemligheter

Riksdagen har tillstyrkt en motion om att se över lagen om skydd för företagshemligheter. Svenskt Näringsliv har vid upprepade tillfällen påpekat att lagen har stora brister och att företagen därmed inte har ett tillräckligt rättsligt skydd på området. Bland annat saknas regler om bevissäkring, hantering av hemlig information för inhyrd personal och straffansvar för anställda som lämnar ut eller utnyttjar företagshemligheter.

Under hösten 2005 kommer Svenskt Näringsliv att hålla ett antal kurser för att öka kunskapen om hur man skyddar hemlig affärsinformation och på hemsidan finns information om företagshemligheter och hur de skyddas i svensk rätt.<sup>1</sup>

### 2.3 Bristande IT-säkerhet hos myndigheter och näringsliv

Krisberedskapsmyndigheten har genomfört en lägesbedömning av samhällets informationssäkerhet. I rapporten beskrivs bland annat att det finns ett stort utländskt underrättelseintresse för Sverige. Intresset rör områden som telekommunikation, medicin, försvarsindustrin och Sveriges politiska agerande.

Krisberedskapsmyndigheten har också uppmärksammat bristande IT-säkerhet hos både myndigheter och den privata sektorn. Spridning av virus, skräppost och spionprogramvara är växande hot. Antalet attacker riktade mot finansiella institutioner och deras kunder där användaren luras att lämna ifrån sig konfidentiell finansiell information uppges öka. Trots ett ökat antal upptäckta riktade angrepp utifrån utgör anställda eller andra av företaget anlitade personer fortfarande det största hotet mot verksamheten.<sup>2</sup>

### 2.4 Skatteverket rätt till företagsinformation

Ett bolag inom Bonnierkoncernen har vägrat att lämna ut avtal till Skatteverket för granskning med hänvisning till att avtalen har betydande skyddsintresse. Handlingar som innehåller företagshemligheter kan undantas från granskning av Skatteverket. Länsrätten har dock beslutat att informationen skall lämnas ut varpå företaget har överklagat domen till Kammarrätten. Tidigare i år beslutade Länsrätten att ett statligt skogsbolag skulle lämna ut handlingar till Skatteverket i ett liknande fall.<sup>3</sup>

---

<sup>1</sup> [www.svensktnaringsliv.se](http://www.svensktnaringsliv.se)

<sup>2</sup> Krisberedskapsmyndigheten "Samhällets informationssäkerhet" Lägesbedömning 2005

<sup>3</sup> Svenska Dagbladet "Bonniers redo ta skattestrid" 050311

## **2.5 Myndighet tvingas lämna ut kundlista**

Företag och branschorganisationer uppges vara kritiska till att Försvarets radioanstalt bedriver kommersiell verksamhet. Under hösten 2004 begärdes uppgifter ut om vilka myndigheter och företag FRA utför IT-konsulttjänster åt. Myndigheten nekade till att lämna ut uppgifterna med hänvisning till att risken för angrepp skulle öka. Kammarrätten har dock beslutat att informationen skall lämnas ut.<sup>4</sup>

## **2.6 Datahackare dömd för företagsspioneri**

I april 2005 dömdes en hackare med ungerskt medborgarskap av Stockholms tingsrätt till tre års fängelse för grovt företagsspioneri och olovlig befattning med hemlig handling. Hackaren hade tagit sig in på Ericssonkoncernens nätverk och kommit över företagshemligheter med bäring för det svenska försvaret. Mannen avslöjades genom att bjuda ut hemliga källkoder till försäljning på Internet.<sup>5</sup>

## **2.7 Misstänkt stöld av affärshemligheter**

Två före detta anställda vid ett svenskt byggvaruhus har stämts av sin tidigare arbetsgivare misstänkta för att ha kopierat kund- och leverantörsinformation samt förberett ny konkurrerande verksamhet på företagets datorer medan de fortfarande var anställda. En av de misstänkta medger att han angripit företagshemligheter medan den andra personen nekar. De båda männen hade tillsammans med ett flertal medarbetare tagit anställning vid ett konkurrerande industriföretag som etablerat verksamhet på samma ort. Detta företag uppger sig dock inte ha tagit emot någon form av hemlig företagsinformation.<sup>6</sup>

## **2.8 Misstänkt företagsspionage inom resebranschen**

Konkurrensen inom resebranschen har ökat och VD:n för ett svenskt reseföretag uppger sig ha märkt av att utländska konkurrenter bevakar deras verksamhet. Konkurrenter skall bland annat ha dumpat priser och försökt ta över samarbeten med utvalda hotell.<sup>7</sup>

## **2.9 Mediebyrå stämmer före detta anställd**

Ett svenskt medieföretag har stämt en före detta anställd anklagad för att ha röjt företagshemligheter i syfte använda dem i konkurrerande verksamhet. Enligt företaget skall kvinnan ha spridit falska uppgifter om att företaget skulle lägga ner delar av sin verksamhet, raderat filer med avtal och tagit med sig flertalet av företagets kunder till en ny mediebyrå. Kvinnan nekar till anklagelserna och uppger att kunderna själva valt att byta byrå. Förhandlingar i Tingsrätten är att vänta.<sup>8</sup>

## **2.10 Konkurrent anklagas för stöld av företagshemligheter**

Ett svenskt elektroniktillverkningsföretag har stämt en konkurrent för att ha stulit företagshemligheter. Det konkurrerande företaget skall ha köpt över två anställda vilka uppges ha tagit med sig information om företagets tekniska system, maskiner och tillverkning. Informationen skall ha bidragit till att ge konkurrensfördelar och som bevis

<sup>4</sup> Computer Sweden "FRA tvingas ge ut kundlista" 050211

<sup>5</sup> TT "Fängelse för spion som drömde om Ericssonjobb" 050404

<sup>6</sup> Vestmanlands Läns Tidning "Avhoppare stal affärshemligheter" 041221, "Inga hemligheter till Arvid Svensson Pro?" 050120

<sup>7</sup> Dagens Industri "STS-uppstickaren i charterkriget" 041221

<sup>8</sup> Dagens Media "Mediacom stämmer RSM-avhoppare på 6 miljoner" 050326

åberopas e-postkorrespondens mellan företaget och de två anställda. Det konkurrerande företaget bestrider dock anklagelserna.<sup>9</sup>

### **2.11 Kvarglömda datorer i taxibilar**

Enligt en svensk undersökning glöms ett stort antal mobiltelefoner och datorer kvar i taxibilar. Flertalet av dessa kan innehålla företagshemligheter som vid ett försvinnande kan komma att röjas om information inte skyddas genom användning av lösenord och kryptering. Företag och myndigheter vars anställda arbetar på distans är av förklarliga skäl särskilt drabbade av denna form av informationsförlust.<sup>10</sup>

### **2.12 Känslig försvarsinformation spreds via Internet**

Försvarsförbundets medlemstidning skall ha publicerat utdrag från intervjuer genomförda av en konsultfirma med personer inom försvarsmakten. Anteckningarna från intervjuerna skall ha gått att ladda ner från Internet efter att en konsult sparat ner dessa på en hemdator ansluten till ett fildelningsprogram.<sup>11</sup>

## **3 Europa**

### **3.1 Danskt företag utsatt för misstänkt företagsspionage**

Ett danskt industriföretag har anklagat en tysk konkurrent för företagsspionage. En anställd vid företagets forsknings- och utvecklingsavdelning uppges redan i slutet av nittioalet ha sålt produktritningar och andra dokument till konkurrenten. Inga ytterligare uppgifter om den anställda eller det misstänkta företaget har påträffats.<sup>12</sup>

### **3.2 Raderade hårddiskar innehåller företagsinformation**

Brittiska universitetsforskare köpte via Internet in 100 hårddiskar från gamla datorer. Hårddiskarna kom från företag och organisationer som anlitat andra företag för att få informationen på dessa förstörd. Vid analys av hårddiskarna fann forskarna att information som personalregister, e-post och finansiell information fortfarande var intakt, information som om den hamnade i orätta händer skulle kunna orsaka stor skada.<sup>13</sup>

### **3.3 Gäststudent misstänkt för företagsspionage**

En kinesisk student som arbetar vid ett franskt tillverkningsföretag inom bilbranschen har arresterats misstänkt för företagsspionage. Polisen skall ha funnit hårddiskar med hemlig information om produkter som ännu inte släppts på marknaden hemma hos kvinnan som arbetade vid företagets forsknings- och utvecklingsavdelning. Hon uppges ha väckt misstankar genom att gå runt med sin bärbara dator på kontoret och tillbringa mer tid än nödvändigt framför datorn.<sup>14</sup>

<sup>9</sup> Dagens Industri "Partnertech stäms av konkurrent" 041229

<sup>10</sup> Aktuell Säkerhet "Glömda datorer i taxibilar kan röja företagshemligheter", nummer 1 2005

<sup>11</sup> PC hemma "Fildelning fällde försvaret" 050228

<sup>12</sup> AP Worldstream "Danish company FLSmidth claims to be victim of German industrial espionage

<sup>13</sup> www.nok.idg.se "Dåligt raderade hårddiskar kan äventyra säkerheten" 050217

<sup>14</sup> Agence France Presse "French police investigate Chinese woman accused of industrial espionage" 050503

### **3.4 Frankrike stöder inhemsk industri**

Den franska regeringen har startat en organisation som skall investera i små innovativa företag för att förhindra utländska uppköp av värdefull teknik. Syftet är att stärka landets industriella utveckling och internationella konkurrenskraft. Det har ifrågasatts huruvida det är regeringens uppgift att bedriva riktade satsningar mot enskilda branscher och företag.<sup>15</sup>

## **4 USA**

### **4.1 Amerikanska farhågor om kinesiskt företagsspionage**

Amerikanska IBM skall sälja delar av verksamheten till ett företag i Kina, delvis ägt av den kinesiska staten. I samband med köpet har det förekommit spekulationer kring kinesiskt företagsspionage i USA. Amerikanska myndigheter ser efter utredning dock inga hinder till att försäljningen skall kunna genomföras.<sup>16</sup>

### **4.2 Miljardskadestånd för stöld av företagshemligheter**

En amerikansk minneskorttillverkare har erhållit närmare 2,7 miljarder kronor i skadestånd från en japansk konkurrent för stöld av företagshemligheter. Det japanska företaget kunde genom att investera pengar och placera en styrelseledamot i bolaget få tillgång till hemlig företagsinformation. Informationen skall ha använts för att vinna konkurrensfördelar och ingå nya samarbetsavtal. Den amerikanska tillverkaren avser nu kräva att den japanska konkurrentens produkter dras in från den amerikanska marknaden.<sup>17</sup>

### **4.3 Företagsspionage inom amerikansk bilindustri**

Två före detta anställda anklagas för att ha stulit företagshemligheter från en leverantör till ett amerikanskt biltillverkningsföretag. Informationen var avsedd för ett kinesiskt företag och företagsspionaget utfördes för att komma över uppgifter om företagets teknologi, priser och samarbetspartners. Det drabbade företaget fick reda på att information läckt ut genom underleverantörer som blivit kontaktade av det kinesiska företaget.<sup>18</sup>

### **4.4 Före detta anställd dömd för dataintrång**

En IT-chef i Kalifornien har dömts till fem månaders fängelse för ett dataintrång utfört i början av 2003. Mannen använde datorer vid företaget där han var anställd för att ta sig in i datasystemet till ett konkurrerande företag där han också arbetade extra. Mannen ifråga var missnöjd med sin tillfällige arbetsgivare och skall ha läst e-post, stulit data och raderat filer för att hämnas. Företaget där mannen är anställd uppger sig inte ha något med intrånget att göra.<sup>19</sup>

<sup>15</sup> The Business "France invests to keep IT from foreign firms" 050327

<sup>16</sup> Computer Sweden "Oro för spionage hindrar inte IBM" 050311

<sup>17</sup> Dagens Industri "Toshiba döms till miljardskadestånd" 050324

<sup>18</sup> The Detroit News "FBI: Local execs stole secrets for Chinese" 050202

<sup>19</sup> Svenska Dagbladet "IT-chef döms för dataintrång" 050317

#### **4.5 Informationsföretag utsatt för dataintrång**

Hackare har stulit användarnamn och lösenord vid ett internationellt informationsföretag och därigenom kommit över ett stort antal personuppgifter. Företaget tillhandahåller juridisk och ekonomisk information samt samlar även in och säljer persondata. De säger sig nu se över företagets säkerhetsrutiner och hjälpa eventuellt drabbade personer.<sup>20</sup>

#### **4.6 Bristande säkerhet vid amerikanska skatteverket**

Att få tillgång till hemlig information genom så kallad *social engineering* har blivit allt mer uppmärksammat. Ett exempel på detta är dataintrång där man istället för att hacka sig in i datasystemet helt enkelt använder sig av personer i företaget för att ta sig in. I USA genomförde revisorer vid finansdepartementet en rundringning till skatteverket och utgav sig för att behöva hjälp med att lösa ett tekniskt problem. På så sätt lyckades de få 35 av 100 tjänstemän att lämna ut sina användarnamn och ändra lösenord och därmed få tillgång till sekretessbelagd information gällande privatpersoners och företags ekonomi.<sup>21</sup>

---

<sup>20</sup> Ny Teknik "Datatjuvar kom över personuppgifter" 050413

<sup>21</sup> www.idg.se "Var tredje skattmas lämnar ut hemliga lösenord" 050418