



Säkerhetspolisen

# FÖRETAGSSPIONAGE



Rapportserie  
2005:1

<b>1</b>	<b>INLEDNING.....</b>	<b>3</b>
<b>2</b>	<b>SVERIGE.....</b>	<b>4</b>
2.1	BIOTEKNIK MÅL FÖR FÖRETAGSSPIONAGE.....	4
2.2	MOBILTELEFON EN SÄKERHETSRIKSK.....	4
2.3	KARTLÄGGNING AV INTERNETRELATERADE HOT.....	4
<b>3</b>	<b>INTERNATIONELLT.....</b>	<b>5</b>
3.1	EUROPA.....	5
3.1.1	<i>Företagsspionage står tyska företag dyrt.....</i>	5
3.1.2	<i>Bristande IT-säkerhet hos brittiska företag.....</i>	5
3.2	SYDAMERIKA.....	5
3.2.1	<i>IAEA tillåts inspektera kärnbränsleanläggning i Brasilien.....</i>	5
3.2.2	<i>Misstänkt företagsspionage i Brasilien.....</i>	6
3.3	NORDAMERIKA.....	6
3.3.1	<i>Israel nekar till företagsspionage i USA.....</i>	6
3.3.2	<i>Tillverkningsföretag utsatt för informationsförlust.....</i>	6
3.3.3	<i>Fortsatt tvist mellan konkurrerande flygbolag.....</i>	6
3.4	ASIEN.....	7
3.4.1	<i>Före detta anställd misstänkt för företagsspionage.....</i>	7
3.4.2	<i>Sydcoreansk IT-industri utsatt för företagsspionage.....</i>	7
3.4.3	<i>Misstänkt företagsspionage vid mässa.....</i>	7
3.4.4	<i>Silicon Valley föremål för otillåten informationsinhämtning.....</i>	8
3.4.5	<i>Anställd laddade ner hemlig företagsinformation.....</i>	8
3.4.6	<i>Försök till företagsspionage hos europeiskt företagskonsortium.....</i>	8
3.4.7	<i>Japanska industrin utsatt för informationsläckage.....</i>	8
3.5	MELLANÖSTERN OCH AFRIKA.....	8
3.5.1	<i>Israelisk man dömd för företagsspionage frisläppt.....</i>	8
3.5.2	<i>Försök till korruption vid upphandling.....</i>	9

## **1 Inledning**

Den här rapporten visar ett urval av artiklar med anknytning till företagsspionage publicerade i svensk och internationell press under sommaren och hösten 2004. Få konkreta fall där personer har dömts för företagsspionage finns publicerade men säkerhetsrisker och olika former av informationsförlust fortsätter att vara aktuella ämnen. Företagsspionage är inte begränsat till en viss bransch eller ett visst företag. De inhämtningsätt som används beror både på vilken slags information som eftersöks och hur tillgänglig informationen är. Det är svårt att skilja på statlig informationsinhämtning och företagsspionage då myndigheter i flertalet länder både i Asien och västvärlden har ett väl utvecklat samarbete med, och stödjer respektive lands näringsliv. Oavsett om spionaget utförs av främmande makt eller om utövaren är ett företag med renodlat kommersiella intressen kan dock konsekvenserna för drabbade företag bli stora. Säkerhetspolisen bedriver därför ett informativt arbete mot svenskt näringsliv och myndigheter gällande spionage.

## 2 Sverige

### 2.1 Bioteknik mål för företagsspionage

Det finns ett stort internationellt intresse för svensk bioteknik och branschen riskerar att utsättas för spionage både av konkurrerande företag och utländska underrättelsetjänster. Spionage kan utföras för att stärka konkurrenskraften men också för att inhämta information användbar för utveckling av massförstörelsevapen.

För att visa hur man med relativt enkla medel kan vidta åtgärder för att skydda sin forskning genomför Säkerhetspolisen, i samarbete med Inspektionen för strategiska produkter, en serie seminarier inom bioteknikbranschen. Säkerhetspolisen har även sammanställt en broschyr, *Att skydda svensk bioteknik*, som under våren 2005 kommer att finnas tillgänglig på hemsidan.

### 2.2 Mobiltelefon en säkerhetsrisk

I föregående rapport beskrevs mobiltelefoner med inbyggd kamera kunna utgöra en säkerhetsrisk då de skulle kunna användas för att kopiera hemlig företagsinformation. Diskussionerna kring risker med mobiltelefoner har fortsatt. En del företag har valt att helt förbjuda användning av mobiltelefoner i närheten av tillverknings- och produktionsanläggningar medan andra är mindre restriktiva och tillåter dem så länge inga foton tas. Ett problem är dock att flertalet mobiltelefoner inte bara innehåller en kamera utan också funktioner som röstinspelning och Internetuppkoppling vilket ökar möjligheterna att både hämta in och skicka vidare information.<sup>1</sup>

### 2.3 Kartläggning av Internetrelaterade hot

Krisberedskapsmyndigheten och Post- och telestyrelsen har på regeringens uppdrag påbörjat ett arbete med att kartlägga Internetrelaterade hot som virus, intrångsförsök, spionage och sabotage mot svenska myndigheter och näringsliv. Kartläggningen bygger på att företag och myndigheter samarbetar och delar med sig av information om den egna Internettrafiken. Krisberedskapsmyndigheten vill inte tala om vilka som redan deltar i kartläggningen men uppger att den kommer att pågå under en längre tid och att man efterfrågar fler medverkande.<sup>2</sup>

---

<sup>1</sup> St. Louis Post-Dispatch "Camera phones pose problems for workplace privacy and security" 040830

<sup>2</sup> www.krisberedskapsmyndigheten.se "KBM kartlägger Internetrelaterade hotbilder" 041022, Ny Teknik "Myndigheter försöker kartlägga internethot" 040901

## 3 Internationellt

### 3.1 Europa

#### 3.1.1 Företagsspionage står tyska företag dyrt

En tysk studie visar att företag riskerar att förlora stora summor på grund av informationsförlust i samband med företagsspionage. I undersökningen, som omfattar 400 företag i regionen Baden-Wuerttemberg, uppges redan två tredjedelar av de undersökta företagen ha varit utsatta för någon form av informationsförlust.<sup>3</sup>

#### 3.1.2 Bristande IT-säkerhet hos brittiska företag

Enligt en brittisk undersökning utsätter sex av tio anställda sitt företag för risker i samband med Internetanvändning. Anställda lämnar ut sin e-postadress till kommersiella webbsidor, diskussionsforum eller nyhetsbrev vilket ökar risken att utsättas för olika former av hacking och spam. För att komma tillrätta med problemet krävs att företagen har en väl utvecklad policy kring IT-säkerhet och att framtagna rutiner följs av samtliga anställda. Flertalet företag har trots uppmärksammade risker inte prioriterat IT-säkerhet då det betraktas som en kostnad istället för en investering. Militären, IT-leverantörer och företag inom den finansiella sektorn uppges ha den högsta medvetenheten gällande IT-säkerhet.<sup>4</sup>

Liknande studier har genomförts i Sverige där det framkommit att flertalet svenska företag saknar en strategi för hantering av Internetrelaterade hot. Försvarets radioanstalt har också uppgett att flera av de myndigheter och statliga bolag de samarbetar med riskerar att utsättas för dataintrång på grund av bristande säkerhet.<sup>5</sup>

### 3.2 Sydamerika

#### 3.2.1 IAEA tillåts inspektera kärnbränsleanläggning i Brasilien

Brasilien har byggt en ny anläggning för anrikning av uran. Anrikat uran kan användas både som bränsle i kärnkraftsverk och till att producera kärnvapen. I mitten av oktober 2004 inspekterades anläggningen av IAEA. Inspektörerna nekades dock tillträde till själva centrifugerna med förklaringen att Brasilien vill skydda den inhemskt tillverkade tekniken mot företagsspionage. Enligt IAEA misstänks inte Brasilien ha för avsikt att tillverka massförstörelsevapen genom anrikning av uran, men ett nekande av inspektioner kan ge felaktiga signaler till omvärlden. I november kom ett besked att IAEA tillåts utföra inspektioner och även ges tillträde till delar av centrifugerna.<sup>6</sup>

<sup>3</sup> Riskwire "Alert- Industrial espionage costing billions of euros" 041019

<sup>4</sup> Computer Weekly "Take control of your staff" 041109

<sup>5</sup> Svenska Dagbladet "Dataattacker mot myndigheter" 040922, SvD 040927

<sup>6</sup> National Public Radio "Brazil faces scrutiny from the International Atomic Energy Agency over its nuclear program" 041019, DN "Brasilien utmanar USA och FN. IAEA tillåts inte inspektera anläggningen för anrikning av uran" 041023, AP Online "IAEA says deal reached with Brazil on inspection for uranium enrichment" 041125

### 3.2.2 Misstänkt företagsspionage i Brasilien

Den brasilianska regeringen tillsatte i somras en utredning för att undersöka huruvida de varit utsatta för någon form av övervakning och informationsläckage. Händelsen har kopplats till företagsspionage inom telekombranschen och informationen skall ha inhämtats via ett internationellt analysföretag. Det finns misstankar att företaget använt sig av statligt anställda för att inhämta information och flertalet anställda vid företaget uppgavs i slutet av oktober 2004 ha arresterats misstänkta för korruption.<sup>7</sup>

## 3.3 Nordamerika

### 3.3.1 Israel nekar till företagsspionage i USA

USA har under hösten 2004 anklagat Israel för att bedriva spionage mot amerikanska intressen. FBI har undersökt huruvida israeler som besökt fabriker och utställningar i landet försökt att samla in hemlig teknisk information. Israel har förnekat att de skulle utöva företagsspionage mot USA och hävdar att händelsen är ett missförstånd som bygger på kulturella olikheter mellan länderna.<sup>8</sup>

### 3.3.2 Tillverkningsföretag utsatt för informationsförlust

En internationell tillverkare av hydrauliska pumpar anklagar ett konkurrerande företag för företagsspionage. Tillverkaren har lämnat in en stämningsansökan som skall förbjuda konkurrenten att använda sig av den stulna företagsinformationen. Informationsförlusten skall ha orsakat tillverkaren affärsproblem i Europa. Händelsen uppdagades i och med att en tidning rapporterade att det konkurrerande företaget planerade att öppna en ny anläggning för pumpar i närheten av tillverkaren. En före detta anställd misstänks via e-post ha försett konkurrenten med tillverknings-, pris-, och kundinformation. Representanter för det konkurrerande företaget skall också ha fotograferat maskiner och införskaffat ritningar och annan information vid besök hos tillverkaren.<sup>9</sup>

### 3.3.3 Fortsatt tvist mellan konkurrerande flygbolag

I föregående rapport beskrevs hur ett kanadensiskt flygbolag anklagat ett konkurrerande bolag för företagsspionage. Konkurrenten skall ha använt sig av hemlig företagsinformation i syfte att erhålla konkurrensfördelar gällande prissättning, flygrutter och expansionsmöjligheter. Tvisten mellan flygbolagen fortsätter och det företag som tidigare stämde har nu lämnat in en egen stämningsansökan. I den hävdar man att flygbolagets ursprungliga stämningsansökan inte gjordes för att skydda konfidentiell information utan för att misskreditera konkurrenten och på sikt försätta dem i konkurs.<sup>10</sup>

<sup>7</sup> Intelligence Online "Kroll's Overseas Woes" 040827, EFE Ingles "Consulting firm's execs arrested for espionage in Brazil" 041028

<sup>8</sup> Jerusalem Post "US is mistaking our hutzpa for industrial espionage" 041209

<sup>9</sup> PR Newswire Europe "Portage County Company Sues Over International Industrial Espionage Plot" 041214

<sup>10</sup> AP "WestJet files \$30-million lawsuit against Air Canada and three top executives" 041215

## 3.4 Asien

### 3.4.1 Före detta anställd misstänkt för företagsspionage

En före detta teknisk chef vid ett kemiföretag i Taiwan har arresterats misstänkt för företagsspionage. Mannen misstänks ha sparat ner konfidentiell information från företagets databas innan han slutade och använt sig av denna för att starta upp egna företag i Kina. Databasen skall bland annat ha innehållit information gällande företagets forskning och utvecklingsplaner.<sup>11</sup>

### 3.4.2 Sydkoreansk IT-industri utsatt för företagsspionage

Sydkorea har en ledande IT-industri men konkurrensen är hård. De främsta konkurrenterna är Kina och Taiwan och anställda inom sydkoreanska företag lockas genom ekonomisk kompensation att stjäla och sälja vidare företagshemligheter.<sup>12</sup> I föregående rapport beskrevs hur Sydkoreanska företag står inför ett ökat hot av industrispionage. Den Sydkoreanska regeringen uppger att ett femtiotal fall av företagsspionage har rapporterats sedan 1998. En före detta anställd vid ett företag som tillverkar LCD-skärmar står anklagad för företagsspionage efter att ha försökt sälja teknisk information till ett taiwanesiskt företag. Ytterligare ett exempel är en före detta anställd vid ett läkemedelsföretag i Sydkorea som uppges ha sålt information till ett kinesiskt företag. Informationen skall ha använts för att tillverka produkter som sedan såldes tillbaka till Sydkorea.<sup>13</sup>

I mitten av maj 2004 arresterades en anställd vid ett mobiltelefonleverantörsföretag i Hongkong, anklagad för industrispionage. Mannen skall ha försökt få forskare vid ett sydkoreanskt företag som tillverkar mobiltelefoner att avsluta sina anställningar vid företaget och spara ner hemlig företagsinformation mot ekonomisk ersättning. Informationen skulle sedan säljas vidare till mobiltelefonföretag i Europa, Kina och Ryssland.<sup>14</sup> Sedan det blivit känt att teknisk information gällande mobiltelefoni läckt till Kina skall ett flertal företag ha börjat se över sin säkerhet. Bland annat installeras mjukvara som förhindrar nedladdning eller överföring av företagsinformation. Regeringen i Sydkorea avser att ge skattelättnader till företag som investerar i olika former av säkerhetssystem som brandväggar och lås. De planerar också att se över lagstiftningen på området. Syftet är att skydda näringsliv och forskning mot otillåten informationsinhämtning.<sup>15</sup>

### 3.4.3 Misstänkt företagsspionage vid mäs

Ett kinesiskt systemleverantörsföretag anklagades 2003 för upphovsrättsligt intrång hos ett stort amerikanskt nätverksföretag. I augusti 2004 rapporterades att en anställd vid samma kinesiska företag skall ha inhämtat hemlig företagsinformation hos en japansk konkurrent. Mannen skall under en mäs

<sup>11</sup> Channel News Asia "Former Taiwan Dow Chemical executive arrested on industrial spying charges" 040814

<sup>12</sup> The Korea Herald "IT industry threatened by espionage; Potential losses from industrial spying estimated at W38 trillion over past 6 years" 040603

<sup>13</sup> The Korea Herald "Technology theft" 041030, WNC "Koreans Indicted for Trying to Sell 6th-Generation LCD Secrets to Taiwan" 041206

<sup>14</sup> Yonhap English News "Employee of Hong Kong Firm Arrested for Industrial Espionage" 040519

<sup>15</sup> AsiaPulse News "S Korean govt to offer corporate security investment tax breaks" 040917, S Korean hi-tech firms beef up security against tech leakage" 041027

<sup>16</sup> Fiber Optics Weekly Update "A spy from Huawei?" 040813, Fiber Optics Weekly Update "A spy from Huawei?" 040813

#### **3.4.4 Silicon Valley föremål för otillåten informationsinhämtning**

En kinesisk medborgare, verksam vid ett amerikanskt mjukvaruföretag i Kalifornien, har dömts till två års fängelse för dataintrång och försök till bedrägeri. Mannen var anställd vid ett statligt kinesiskt oljebolag och uppges ha blivit placerad vid det amerikanska företaget för att lära sig företagets produkter.<sup>17</sup>

#### **3.4.5 Anställd laddade ner hemlig företagsinformation**

Ett amerikanskt företag som tillverkar mjukvara för tryckindustrin öppnade under våren 2004 ett kontor i Indien. I augusti rapporterades att en anställd laddat ner källkoder och information gällande designen av företagets produkter.<sup>18</sup>

#### **3.4.6 Försök till företagsspionage hos europeiskt företagskonsortium**

Anställda hos en europeisk tillverkare av höghastighetståg uppges ha uppmärksammat ett misstänkt fall av företagsspionage. Ett okänt antal kinesiska ingenjörer skall ha filmats när de tagit sig in i företagets lokaler i Shanghai och försökt inhämta hemlig information om tågen. Den lokala chefen för projektet skall dock ha uppgett att händelsen snarare är kopplad till forskning och utveckling än försök till företagsspionage.<sup>19</sup>

#### **3.4.7 Japanska industrin utsatt för informationsläckage**

Japanska myndigheter avser att stärka landets konkurrenslagstiftning och öka skyddet av information. Syftet är att förhindra inhemska ingenjörer från att läcka information till andra länder vilket kan medföra att landet dräneras på teknisk kompetens. Japanska ingenjörer uppges under veckoslutsresor och semestrar till närliggande länder hjälpa lokala företag med teknisk expertis, något som på sikt kan komma att försämra Japans internationella konkurrenskraft.<sup>20</sup>

### **3.5 Mellanöstern och Afrika**

#### **3.5.1 Israelisk man dömd för företagsspionage frisläppt**

I december 2004 släpptes en israelisk affärsman efter att i åtta år ha suttit fängslad för företagsspionage i Egypten. Mannen som arbetade vid en textilfabrik arresterades 1996 anklagad för att ha lämnat information till Israel om egyptiska fabriker. Året därpå dömdes han till 15 års fängelse men släpptes i utbyte mot sex egyptiska studenter som anklagats för att illegalt ha tagit sig över gränsen och planerat att kidnappa israeliska soldater. Frisläppandet ses som ett tecken på en politisk vilja till enighet mellan Egypten och Israel.<sup>21</sup>

<sup>17</sup> Monterey County Herald "Chinese man sentenced for Silicon Valley fraud" 041218

<sup>18</sup> Computer Sweden "Indier stal källkod från amerikanskt företag" 040806

<sup>19</sup> AFX Asia "Transrapid films Chinese engineers on suspicion of espionage" 041203

<sup>20</sup> Daily Yomiuri "Business spies could face prison terms" 041019

<sup>21</sup> AP Online "Israeli prime minister welcomes accused spy home after eight years in Egyptian prison" 041206

### **3.5.2 Försök till korruption vid upphandling**

Två företag inom den sydafrikanska guldgruvsindustrin anklagar varandra för oömsbördig konkurrens. Bland annat har ett av företagen anklagat det andra för försök till korruption. En anställd vid ett av företagen skall ha blivit tillfrågad om att mot ersättning lämna ut information om budgivning vid upphandlingar. Båda företagen nekar till anklagelserna.<sup>22</sup>

---

<sup>22</sup> Guardian “Gold miners clash over spy claim: Harmony’s accusation of industrial espionage dismissed as nonsense by targeted rival” 041116