



## Kinas internationella expansion och informationsinhämtning

Kina bedriver en omfattande informationsinhämtning internationellt i syfte att utveckla forskning och utveckling och därigenom stärka landets konkurrenskraft. En betydande del av inhämtningen sker i USA, vilket ses som ett hot mot den nationella säkerheten. Det finns farhågor att det amerikanska immigrations-systemet och landets utbildningsväsen utnyttjas för att bedriva spionage. Kinesiska studenter, forskare och personer placerade på kinesiska frontföretag uppges hämta in information som sedan förmedlas tillbaka till Kina. Kinesiska företag uppges också inleda affärskontakter med amerikanska bolag enbart i syfte att komma över känslig teknologi. Företag står inför dilemmat att vilja expandera i Asien samtidigt som de måste kunna skydda både företagets teknik och immateriella tillgångar. Utifrån detta har FBI etablerat samarbete med ledande bolag inom försvarsindustrin som Lockheed Martin, General Dynamics och Raytheon för att diskutera den teknik de utvecklar och vilka hot som företagen och dess anställda kan möta. Det stora antal kineser som besöker, arbetar eller studerar i USA gör det dock svårt för amerikanska myndigheter att kontrollera syftet med deras vistelse i landet. För att kunna möta hotet mot ekonomiskt spionage uppges företrädare för amerikansk underrättelsetjänst att det finns ett behov av att öka kunskapen om vilken forskning och utbildning som utländska medborgare bedriver i USA.

Kina har också uppmärksammats för att bedriva ekonomiskt spionage i Australien och Kanada. Uppgifterna framkom efter att kinesiska underrättelseagenter hoppat av och sökt asyl i dessa länder. I Kanada riktas spionaget främst mot nyckelsektorer som bioteknik- och läkemedelsindustrin. I syfte att stärka den nationella säkerheten och förhindra att utländska intressenter får för stor kontroll över Kanadas ekonomi och naturtillgångar har landets regering lämnat ett lagförslag som skall ge möjlighet att förhindra utländska uppköp av företag.

Det finns också information att Kina bedriver ett omfattande spionnätverk i Europa. Enligt uppgifter från en kinesisk avhoppare som sökt asyl i Belgien skall det röra sig om hundratals kineser verksamma i Nordeuropeiska industri-företag. Det är dock oklart

### Nytt nyhetsbrev ersätter rapporter

Det här är det första numret av Säkerhetspolisens nyhetsbrev Företagsspionage. Tidigare har urvalet av artiklar om informationssäkerhet och företags-spionage presenterats i rapportform.

Under 2005 har två rapporter publicerats:

- Företagsspionage (rapport 2005:3) Publicerad den 28 juni
- Företagsspionage (rapport 2005:1) Publicerad den 27 januari

Du hittar rapporterna på Säkerhetspolisens webbplats:  
[www.sakerhetspolisen.se](http://www.sakerhetspolisen.se)

### HACKARPROGRAM ANVÄNDES FÖR ATT SAMLA IN FÖRETAGS-INFORMATION

se sidan 2

### TYSKLAND SÄKRAR IT-SYSTEM

se sidan 2

### MOBILTELEFON MED INBYGGD KAMERA EN SÄKERHETSRISK

se sidan 2

### MP3-SPELARE KAN ANVÄNDAS FÖR FÖRETAGSSPIONAGE

se sidan 2

### STAL FÖRETAGSINFORMATION FRÅN KONKURRENT

se sidan 2

### BILTILLVERKARE UTSATT FÖR INFORMATIONSLÄCKAGE

se sidan 2

### ANKLAGELSER OM FÖRETAGS-SPIONAGE INOM DETALJHANDLNINGEN

se sidan 3

### STULNA AFFÄRSHEMLIGHETER SÅLDES TILL TAIWAN

se sidan 3

### SYDKOREA UPPMÄRKSAMMAR INDUSTRI-SPIONAGE

se sidan 3

Nyhetsbrevet baseras på information från ett urval av artiklar som handlar om informationssäkerhet eller företags-spionage. Artiklarna är publicerade i svensk och internationell press under sommaren och hösten 2005.

*Fortsättning från s. 1 ...*

huruvida denna massinhämtning av information bidragit till att stärka Kinas tekniska utveckling och konkurrensförmåga eller vilken information som kan ha vidarebefordrats till kinesisk under rättelsetjänst.

I Säkerhetspolisens nyhetsbrev i juni 2005 rapporterades att en kinesisk praktikant vid ett tillverkningsföretag i bilbranschen arresterats i Frankrike misstänkt för att ha laddat ner hemlig företagsinformation. Det franska justitiedepartementet har i samband med detta varnat för att det förekommer industrispionage i Frankrike.

*Källa: The Wall Street Journal "FBI sees big threat from Chinese spies" 2005-08-10*

*Inside US-China Trade vol.5 no 40, 2005-10-05*

*Agence France Press "Canada government acts to nix foreign takeovers of companies" 2005-06-20*

## Hackarprogram användes för att samla in företagsinformation

Ett stort antal personer häktades i somras misstänkta för att genom dataintrång ha kommit över hemlig företagsinformation från konkurrerande bolag. Ett flertal företag i olika branscher utsattes för intrång genom att en trojan, som spreds via e-post, infekterade företagets datorer. Programmet hade sitt ursprung i Israel och såldes bland annat till detektivbyråer som utförde spionage åt andra företag. Händelsen har kommit att betraktas som ett av de mest omfattande fallen av företagsspionage under senare tid.

*Källa: Computer Sweden "Trojansk häst för utbrett spionage" 2005-06-10*

## Tyskland säkrar IT-system

Den tyska regeringen avser att öka skyddet av kritiska IT-system inom bland annat flygtrafikledning, bankväsen och myndigheter. Detta är ett resultat av ökad internationell uppmärksamhet mot Internetrelaterade hot som virus, dataintrång och företagsspionage genom så kallad phishing.

*Källa: Associated Press Newswires "Germany outlines plan to stop criminal, terrorist attacks on IT systems" 2005-08-18*

## Mobiltelefon med inbyggd kamera en säkerhetsrisk

I Australien har en tekniker som reparerade hushållsmaskiner avskedats för att vid upprepade tillfällen ha fotograferat konfidentiell företagsinformation. Bilderna togs med mannens mobiltelefon och bedömdes kunna vara av värde för eventuella konkurrenter. Mannen som ertappades av två medarbetare uppgav själv att fotograferingen endast var en hobby.

*Källa: Dominion Post "Appeal against industrial espionage dismissal fails" 2005-08-27*

## MP3-spelare kan användas för företagsspionage

Bärbara musikspelare uppges kunna utgöra en potentiell säkerhetsrisk för företag. MP3-spelare eller andra mobila enheter som USB-minnen ger möjlighet att på kort tid ansluta och spara ner stora mängder information, så kallade pod-slurping. Personer som besöker eller utför arbete hos ett företag och bär med sig en MP3-spelare kan se ut att lyssna på musik medan de i själva verket laddar ner hemlig information.

*Källa: The Australian "Pod slurping hits a sour note" 2005-06-28*

## Stal företagsinformation från konkurrent

En anställd vid ett elektronikföretag som säljer navigeringsutrustning har hackat sig in på ett konkurrerande företag och stulit information om kunder och återförsäljare. Syftet uppges ha varit att kunna erbjuda lägre priser än konkurrenten och därmed öka försäljningen vid det egna företaget.

*Källa: Associated Press Newswires "Executive charged with corporate espionage against rival firm" 2005-05-26*

## Biltillverkare utsatt för informationsläckage

En stor internationell biltillverkare har uppgett att en av företagets underleverantörer läckt information om en ny bilmodell till en kinesisk biltillverkare. Konkurrenten skall bland annat ha fått tillgång till testresultat på motorer. Det drabbade företaget har avbrutit samarbetet med underleverantören men uppger samtidigt att andra samarbetspartners skall ha försökt sälja företagets tekniska lösningar till olika kinesiska företag.

*Källa: World News Connection "Hyundai falls victim to industrial espionage" 2005-10-25*

## Anklagelser om företagsspionage inom detaljhandeln

Ett amerikanskt företag anklagas för att ha bedrivit företagsspionage för att komma över affärshemligheter och på så sätt kunna utveckla sin försäljning av sportartiklar. En marknadsansvarig vid det drabbade företaget skall innan han sa upp sig ha övertalat anställda att gå över till konkurrenten samt kopierat pris-, kostnads- och försäljningsinformation från företaget. En representant för det utpekade företaget uppger att anklagelserna helt saknar grund.

*Källa: Boston Herald "New Balance gets slashed" 2005-05-27*

## Stulna affärshemligheter såldes till Taiwan

En före detta anställd vid ett amerikanskt glas-tillverkningsföretag anklagas för att ha stulit företagshemligheter och sålt dessa till ett företag i Taiwan. Företaget uppges ha fått tillgång till och fotograferat skisser på tillverkningsprocessen och sedan laddat ner dessa på en diskett. Händelsen uppmärksammades i och med att företaget visade upp ritningar i samband med köp av utrustning från ett annat företag. Det taiwanesiska företaget har erbjudit tillverkningsföretaget ekonomisk kompensation för det inträffade samt gått med på att inte använda sig av den stulna informationen.

*Källa: Lexington Herald-Leader "Ex-worker charged with selling trade secret" 2005-10-21*

## Sydkorea uppmärksammar industrispionage

Den sydkoreanska underrättelsetjänsten har uppmärksammat en ökning av antalet anmälda händelser av industrispionage i landet. Under 2004 rapporterades 26 händelser och under de första sju månaderna 2005 har 19 fall av industrispionage uppdagats. Underrättelsetjänsten uppger att det krävs förändringar i lagstiftningen för att förhindra industrispionage. Det framkommer dock inte inom vilka områden eller av vem spionaget har utförts.

*Källa: Yonhap News Agency of Korea "Industrial spy cases in S. Korea surged in 2004" 2005-09-21, "S. Korea's intelligence agency seeks bill on industrial espionage" 2005-10-21*

Säkerhetspolisens vision är att framgångsrikt skydda Sveriges säkerhet mot brottsliga angrepp. Vi värnar därmed den svenska demokratin och dess institutioner, medborgarnas grundläggande fri- och rättigheter samt den nationella säkerheten.

Säkerhetspolisen tar tacksamt emot information, frågor eller iakttagelser om spionage.

Ansvarig:  
Informationschef Christina Fornell

Säkerhetspolisen  
Box 8304  
104 20 Stockholm

Tfn: 08-401 26 00  
Fax: 08-401 48 85

E-post:  
sakerhetspolisen@sakerhetspolisen.se

Vill du prenumerera på *Företagsspionage* skicka ett e-brev med din e-postadress till [foretagsspionage@sakerhetspolisen.se](mailto:foretagsspionage@sakerhetspolisen.se).

[www.sakerhetspolisen.se](http://www.sakerhetspolisen.se)