



Manual för ekonomisk underrättelsetjänst publicerad i Frankrike

Den franska näringslivsorganisationen Le mouvement des entreprises de France (MEDEF) har tagit fram en manual innehållande praktiska rekommendationer för de franska företagsledningar som vill utveckla sitt företags förmåga att bedriva ekonomisk underrättelsetjänst och samtidigt skydda sin egen information från främmande intressen.

Den 52 sidor långa publikationen består av fem huvudkapitel vilka handlar om hur en företagsledning bättre kan arbeta för att förstå och följa utvecklingen i omvärlden, hur man kan skapa ett system för ekonomiska underrättelser, hur man vidareutvecklar organisationens inhämtning, vidare hur man skyddar sin information samt avslutningsvis hur inflytelseaktioner kan bedrivas.

Boken är ett resultat av observationer och intervjuer med företagsledare.

Sammanfattningsvis kan publikationen betraktas som syftandes till att väcka intresset för ekonomiska underrättelser och metodik för detta.

Källa: L'intelligence économique Guide pratique pour les PME, MEDEF Paris, 2007-03-30

Kina stört av anklagelser om ekonomiskt spionage

Efter en artikel i Financial Times Deutschland (se artikel i detta nyhetsbrev) där anklagelser om kinesiskt industrispionage framkom uttryckte den kinesiska ambassaden sin frustration över att den federala tyska regeringen i sina officiella kontakter inte nämnt någonting om detta. Kinesiska studenter och trainees lider nu av anklagelserna och betraktas med mistänksamhet av tyska företag.

Efter tyska anklagelser om industrispionage uppger Kinas före detta ambassadör i Tyskland Mei Zharong att man ser på anklagelserna med irritation. Vidare uppges att Kina upplever en allmänt ökad distans till Tyskland som politisk och ekonomisk partner.

Källa: Hamburg Financial Times, 2007-03-12

Nyhetsbrevet baseras på information från ett urval av artiklar som handlar om informationssäkerhet, företags- eller industrispionage. Artiklarna är publicerade i svensk och internationell press från december 2006 till och med mars 2007.

**TYSKA BOLAG UPPMANAR
MYNDIGHETER ATT AGERA
MOT VÅG AV KINESISK
IT-BROTTLIGHET**

se sidan 2

**RYSKT INDUSTRISPIONAGE I
TYSKLAND**

se sidan 2

**MULTINATIONELLA BOLAG
– ETT MÅL FÖR INDISKA
UNDERRÄTTELSETJÄNSTEN?**

se sidan 2

TEKNIKSPIONAGET ÖKAR

se sidan 2

**NY AMERIKANSK STRATEGI
FÖR ATT BEMÖTA SPIONAGE,
INKLUSIVE FÖRETAGSSPIO-
NAGE**

se sidan 3

**TYSKT MJUKVARUFÖRETAG
MOTSÄGER SIG ANKLAGELSER
OM INDUSTRISPIONAGE**

se sidan 3

**TELEKOMSKANDALEN SOM
SKÅKADE ITALIEN**

se sidan 3

**INGENJÖR DÖMS TILL LIVS-
TIDS FÄNGELSE FÖR INDU-
STRISPIONAGE I QATAR**

se sidan 3

**SPIONEN SOM FÖRSÖKTE
SÄLJA COCA COLAS HEMLIG-
HETER SKYLDIG**

se sidan 4

**KINESISK INGENJÖR ANKLA-
GAD FÖR INDUSTRISPIONAGE
I USA**

se sidan 4

**DNA-DATABAS UTSATT FÖR
INDUSTRISPIONAGE**

se sidan 4

Tyska bolag uppmanar myndigheter att agera mot våg av kinesisk IT-brottslighet

Förbundet för tyska industrier – Bundesverband der Deutschen Industrie (BDI) – har uppmanat tyska myndigheter att i ökad utsträckning anstränga sig för att skydda tyska företag från främmande intressen. Tyska företag klagar över ett ökat antal intrångsförsök och IT-attacker från privata kinesiska hackers. Små och medelstora företag förefaller vara mest utsatta eftersom de sällan har sofistikerade elektroniska skyddssystem.

Ordföranden för BDI Jurgen Thumann har efterlyst ett bättre samarbete mellan det tyska näringslivet och landets säkerhetsorganisationer. "Företag och myndigheter måste bli bättre på att utbyta information. I det avseendet kan Frankrike lyftas fram som ett bra exempel. I Frankrike är det vanligare att säkerhetsexperten under en kortare period kan tjänstgöra i myndigheter och vice versa. Det borde vara möjligt även i Tyskland."

Enligt den tyska säkerhetstjänsten BfV är det framförallt ryska samt kinesiska intressen som aktivt bedriver industrispionage i Tyskland. Medan Ryssland vanligen försöker att infiltrera agenter in i tyska företag, strävar Kina istället efter att komma över känslig information med hjälp av elektroniska intrång.

Källa: *Financial Times Deutschland*, 2007-02-09

Ryskt industrispionage i Tyskland

500 ryska agenter bedöms vara verksamma i Tyskland, enligt Erich Schmidt-Eenbom, chef för Research Institute for Peace Policy. Tyskland och Frankrike uppges utgöra huvudintresse för ryska underrättelseoperationer. Aktiviteterna består främst av industrispionage och riktas exempelvis mot exportförhandlingar i syfte att förse ryska företag med konkurrensfördelar. Även tyska myndigheter har uttalat sig om ryska underrättelseaktiviteter i Tyskland. I sin årsrapport skriver BfV att även om den politiska relationen mellan Tyskland och Ryssland under flera år utvecklats positivt, är ryska underrättelseaktiviteter i Tyskland förekommande och oförminskade.

Källa: *Hamburg Bild am Sonntag*, 2006-12-17

Multinationella bolag – ett mål för indiska underrättelsetjänsten?

Industrispionage i Indien förekommer framförallt inom området informationsteknologi. De nationella säkerhets- och underrättelseorganisationerna IB och RAW påstås även genomföra fysisk övervakning av västerländska diplomater och affärsmän. Elektronisk avlyssning är lagligt i Indien och metoden anses vara vanligen förekommande. De flesta fall av industrispionage i Indien involverar insiders som stjälar källkoder och annan affärsinformation.

Risken att utsättas för industrispionage förekommer över hela världen men högteknologiska företag löper större risk i vissa länder, särskilt i Indien eftersom en stor del av företagets utvecklingsarbete är lokaliserat där. IB och RAW uppges vara mer aggressiva än motsvarande organisationer i andra länder beträffande inhämtning av skyddad och känslig information från främmande företag för att främja Indiens egna intressen.

Källa: *InfosecToday (Ursprungligen publicerat av Stratfor)*, 2007-03-12

Teknikspionaget ökar

Nu ökar spionattackerna mot den högteknologiska försvarsindustrin i USA. En rapport visar också att det är fler länder än tidigare som står för intrångsförsöken.

I USA är det huvudsakligen olika former av dataintrång som används för att komma åt känslig information. Målet är framförallt industrier för utveckling och tillverkning av laser, missiler och sensorer.

Amerikanska myndigheter har sett en 43 procentig ökning av misstänkta attacker mot landets försvarsindustri. Totalt noterades 971 misstänkta händelser. Dessa har skett från 106 olika länder vilket är en ökning från året innan då motsvarande siffra var 90. Enligt Reuters härstammar drygt 30 procent av attackerna från Östasien och Stilla havsregionen. USA har tidigare pekat ut Kina, Ryssland och Iran som de största hoten mot den amerikanska försvarsindustrin. Uppgifterna i denna artikel gäller redovisning fram till september 2005.

Källa: *Ny Teknik*, 2007-01-04

Ny amerikansk strategi för att bemöta spionage, inklusive företagsspionage

En ny amerikansk nationell strategi för kontraspionage har godkänts av President George Bush. Ett av de framträdande budskapen i strategin är behovet att med agenter eller på elektronisk väg penetrera främmande länders underrättelsetjänster, regeringar och utländska grupper.

Ur ett skyddsperspektiv framhävs datorbaserade skyddsåtgärder som försvar mot främmande staters och privata aktörers försök till spionage. Privata sektorn beskrivs som en fertil grogrund för teknisk utveckling och forskning och utgör alltså ett mjukt mål för främmande underrättelseintressen. I strategin betonas att allmänheten bättre bör informeras att de datornätverk som används varje dag är föremål för attacker från främmande aktörer och bör skyddas därefter.

I dokumentet uppmuntras underrättelse- och säkerhetsrelaterade myndigheter att effektivisera informationsutbytet med externa organisationer, inklusive intresserade företag i den privata sektorn.

Källa: The National Counterintelligence Strategy of the United States of America, 2007-03-28

Tyskt mjukvaruföretag motsäger sig anklagelser om industrispionage

Henning Kagermann, ordförande för det tyska mjukvaruföretaget SAP tillbakavisar anklagelser från den amerikanska konkurrenten Oracle, som hävdar att SAP har stulit information från företaget. Enligt Oracle ska SAP ha skaffat sig otillåten access till Oracles lösenordsskyddade webbsida för kundförfrågningar. SAP ska ha kopierat mängder av känslig information inklusive mjukvaruprodukter till sin egen server. Oracle har anmält ärendet till en amerikansk domstol.

Källa: Financial Times Deutschland, 2007-03-27

Telekomskandalen som skakade Italien

Företaget Telecom Italia är misstänkt för att ha använt olagliga metoder och spionerat på konkurrenter och politiker. Listan över personer som varit mål för det påstådda spionaget är omfattande, bland annat uppges personer associerade med RCS Mediagroup, som publicerar *Il Corriere della Serra* finnas bland underrättelsemålen. Kritiska artiklar om Telecom Italia, i kombination med misstankar att artiklarna förmedlats av konkurrenter uppges ha motiverat spionaget.

Totalt ska 6 000 dossier ha lagts upp på kända italienska politiker, affärsmän, finansmän, bankmän, konkurrenter i affärer och kärlek, fotbollsspelare och artister, journalister och åklagare. 2 000 av akterna berör personer som är anställda på Telecom Italia.

En rad olika metoder påstås ha använts, bland annat ska tidningens VD lurats att använda en säkerhetsmjukvara som i själva verket sög ut allt innehåll ur datorn. En annan person lockades med hjälp av en vacker kvinna att ge ut sin e-postadress. Via e-postadressen skulle därefter ett elektroniskt intrångsförsök riktas.

Personer som anlitats för spionaget är privatdetektiver och dataexperter för att nämna några exempel. Betalning har utbetalats via en amerikansk bank i Annandale i Virginia, USA. Vissa arvoden har Giuliano Tavaroli, Telecom Italias före detta säkerhetschef som avsändare men inte alla. Tavaroli pekas ut som en av huvudmännen i skandalen.

Källa: Dagens Industri, 2007-02-09

Ingenjör döms till livstids fängelse för industrispionage i Qatar

En domstol i Qatar har dömt en amerikansk ingenjör till livstids fängelse för industrispionage. Ingenjören, 51 år gammal, som arbetade för regeringsägda Qatar Petroleum, togs på bar gärning då han försökte sälja viktig information om ett oljefält till personal från ett icke-namngivet lands ambassad. Mannen kunde gripas efter att polisen genomfört en operation där en polisman spelat representant från ett främmande lands ambassad. En CD med den känsliga informationen uppges ha påträffats i ingenjörens hem.

Källa: Upstream, 2007-02-23

Spionen som försökte sälja Coca Colas hemligheter skyldig

En jury i Coca Colas hemstad Atlanta, USA har funnit att den 41-åriga kvinnliga administratör som misstänkts ha koordinerat ett försök till industrispionage är skyldig. Hon dömdes till 10 års fängelse.

Administratören och två medarbetare ska ha kontaktat konkurrenten Pepsi och erbjudit att mot 100 000 dollar förmedla känsliga uppgifter om Coca Colas senaste produkter. Pepsis ledning larmade FBI direkt efter kontakttagandet. FBI organiserade därefter en hemlig operation som slutade med att de tre förövarna greps i ett fingerat möte.

Administratören hävdar fortfarande att hon är oskyldig och att de två medförövarna, som bägge erkänt sig skyldiga, ska ha lurat henne och stulit informationen och kontaktat Pepsi utan hennes vetskap.

Källa: The Guardian, 2007-02-03

Kinesisk ingenjör anklagad för industrispionage i USA

En kinesisk ingenjör anklagades i San Jose, USA för att ha stulit affärshemligheter från ett företag i Silicon Valley som tillverkar mjukvaror för militär utbildning. Mannen, en 42-årig kines med kanadensiskt medborgarskap, dömdes bland annat för ekonomiskt spionage i syfte att främja utländsk regering. Åklagarna uppgav att ingenjören stal mjukvarukoden från företaget Quantum 3D Inc., som används för att träna militära stridsflygare. Mannen ska därefter ha försökt sälja informationen till det thailändska respektive det malaysiska flygvapnet samt till ett företag med kopplingar till den kinesiska försvarsmakten.

Källa: AP, 2006-12-15

DNA-databas utsatt för industrispionage

Fem personer anställda vid brittiska Forensic Science Service, FSS har stängts av från sina befattningar på grund av misstanke om industrispionage. De fem, alla verksamma i området kring Birmingham, uppges olovligt ha kopierat känslig information i syfte att starta en konkurrerande verksamhet. Samtliga personer var engagerade av FSS för att bistå med driften och utvecklingen av en omfattande databas med DNA-prov från fyra miljoner personer, den största i världen i sitt slag. De fem ska ha kopierat mjukvara såväl som annan känslig information.

Ärendet kommer oundvikligen att väcka debatten kring sårbarheter och etiska utmaningar att registrera genetisk information.

Källa: USA Defence Security Service, 2007-02-12

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.

www.sakerhetspolisen.se