

SÄKERHETSPOLISEN



Företagsspionage

Rapport 2 /2004

1	INLEDNING	4
2	INTERNATIONELLT	5
2.1	KINESISK INGENJÖR DÖMD FÖR SPIONAGE	5
2.2	KINESISKA MILITÄRER ANKLAGAS FÖR SPIONAGE	5
2.3	JAPAN VÄGRAR ÖVERLÄMNA FORSKARE TILL USA	5
2.4	SYDKOREANSK IT-INDUSTRI UTSATT FÖR SPIONAGE	5
2.5	FN AVLYSSNAT	6
2.6	FLYGBOLAG ANKLAGAR KONKURRENT FÖR SPIONAGE	6
2.7	SPIONAGE INOM BILINDUSTRIEN	6
2.8	HOTBILD MOT DEN PRIVATA SEKTORN	6
3	SVERIGE	7
3.1	ANSTÄLLD KOPIERADE FÖRETAGSINFORMATION	7
3.2	STÄMNINGANSÖKAN GAV TILLGÅNG TILL FÖRETAGSINFORMATION	7
3.3	MOBILTELEFONER EN SÄKERHETSRISK	7
3.4	AFFÄRSPLANER DISKUTERADES ÖPPET PÅ FLYGPLAN	8

1 Inledning

Den här rapporten syftar till att spegla hur företagsspionage rapporterats i svensk och internationell media under våren 2004. Det har förekommit relativt få konkreta fall av företagsspionage i media vilket dock inte är att betrakta som ett mått på den faktiska förekomsten av spionage eller informationsförluster hos företag. Företagsspionage uppfattas ofta som ett yttre hot medan stora delar av den informationsförlust som sker möjliggörs genom bristande intern säkerhet, brister som företag inte alltid vill dela med sig av. Flera av de händelser som uppmärksammas i denna rapport påvisar att anställda eller före detta anställda utgör en av de främsta säkerhetsriskerna för företag. I flera fall hamnar dock inte företeelser som säkerhet och spionage på företagens agenda förrän det blivit uppmärksammat och omdebatterat i media.

Ur ett internationellt perspektiv fortsätter asiatiska länder, företrädesvis Kina, att förekomma i media kring företagsspionage. Det bedrivs inte nödvändigtvis mer spionage i denna region jämfört med övriga länder utan uppmärksamheten i media beror snarare på den industriella utvecklingen i området. Den asiatiska marknaden växer och fler företag förlägger sin verksamhet där samtidigt som asiatiska företag och gästforskare verkar utomlands. Det gör det både nödvändigt och högst intressant för både myndigheter och näringsliv att följa utvecklingen inom det affärsrättsliga området i denna region.

2 Internationellt

2.1 Kinesisk ingenjör dömd för spionage

En ingenjör vid ett kinesiskt ståltillverkningsföretag har dömts till 18 års fängelse för företagsspionage. Mannen som arbetade på företagets utvecklingsavdelning ertappades med att sälja hemlig företagsinformation till ett utländskt bolag som deltog i upphandlingen av ett affärsprojekt. I samband med att ingenjören blivit arresterad drog sig det utländska bolaget ur upphandlingen.¹

2.2 Kinesiska militärer anklagas för spionage

Kina har arresterat flera militärer som bedrivit spionage för Taiwan. De skall enligt uppgift ha sålt försvarsuppgifter gällande det kinesiska flygvapnet. Kina skall också tidigare i år ha arresterat taiwanesiska affärsmän som bedrivit spionage mot försvarsmakten.² Detta utgör inte ett konkret fall av företagsspionage, men är intressant då det påvisar spionage mellan två asiatiska länder. Rapportering av företagsspionage i Asien är fortfarande relativt begränsat i västerländska källor.

2.3 Japan vägrar överlämna forskare till USA

En japansk forskare åtalades 2001 för spionage i USA. Enligt beslut i japansk domstol behöver mannen dock inte återvända till USA. Domstolen ansåg att forskaren inte brutit mot amerikansk lag om företagsspionage då han inte haft uppsåt att tjäna på händelsen. Forskaren stod anklagad för ekonomiskt spionage kopplat till medicinsk forskning inom Alzheimer.³ Enligt uppgift skall det vara första gången som Japan nekar ett liknande utlämnande. En orsak kan vara det faktum att Japan ligger långt fram inom Alzheimers-forskning och att forskaren därmed bedöms som en viktig resurs för landet.

2.4 Sydkoreansk IT-industri utsatt för spionage

Sydkorea har en ledande IT-industri men konkurrensen är hård och landets företag står inför ett ökat hot av företagsspionage. De främsta konkurrenterna är Kina och Taiwan och anställda inom sydkoreanska företag lockas genom ekonomisk kompensation att stjäla och sälja vidare företagshemligheter.⁴

I mitten av maj arresterades en anställd vid ett mobiltelefonleverantörsföretag i Hong-Kong, anklagad för företagsspionage. 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.⁵

¹ Xinhua Financial Network News "Chinese engineer jailed 18 years for industrial espionage" 040423

² Vancouver Sun "Top Chinese officers accused of espionage: Four generals are among those arrested for selling secrets to Taiwan" 040417

³ Chicago Tribune "Court rejects extradition request from U.S." 040329

⁴ The Korea Herald "IT industry threatened by espionage; Potential losses from industrial spying estimated at W38 trillion over past 6 years" 040603

⁵ Yonhap English News "Employee of Hong Kong Firm Arrested for Industrial Espionage" 040519

2.5 FN avlyssnat

I början av 2004 rapporterades att Kofi Annan och andra ledande politiska aktörer varit utsatta för avlyssning genom övervakningssystemet Echelon inför kriget i Irak. Det är rimligt att anta att det inte är ovanligt att diplomater och andra strategiskt viktiga personer utsätts för avlyssning och annan form av elektronisk övervakning. Det bästa skyddet är helt enkelt att vara medveten om var och hur känslig information behandlas.⁶

2.6 Flygbolag anklagar konkurrent för spionage

Ett kanadensiskt flygbolag anklagar ett konkurrerande bolag för företagsspionage. Detta skall ha skett genom otillåten användning av konfidentiell information. Informationen skall ha använts för att erhålla konkurrensfördelar gällande prissättning, flygrutter och expansionsmöjligheter. Konkurrenten skall enligt uppgift ha kommit över informationen genom en före detta anställd vid flygbolaget som hade kvar en personlig inloggningskod för att boka flygbiljetter vilken gav access till det interna nätverket.⁷ Flygbranschen har tidigare varit drabbad av företagsspionage vilket kan vara en följd av de ekonomiska svårigheter och den ökade konkurrens som branschen drabbats av.

2.7 Spionage inom bilindustrin

En biltillverkare misstänks för spionage mot ett konkurrerande företag. En anställd som tidigare arbetat för det drabbade företaget misstänks ligga bakom händelsen. Tekniker på företaget skall också via ett annat företag ha försökt sälja hemlig information om bilarnas konstruktion. Det företag som utsatts för spionaget har själva kritiserats för att ha fotograferat konkurrenters bilar för att vinna konkurrensfördelar. Båda företagen satsar stora pengar på att utveckla konkurrenskraftiga tävlingsfordon vilket medför en ökad risk för företagsspionage.⁸

2.8 Hotbild mot den privata sektorn

Den 27 maj 2004 hölls en konferens i London på temat hur den privata sektorn hanterar hotet från terrorism. Under konferensen presenterades en undersökning som visar att tillfrågade företag upplever terrorism som ett hot mot verksamheten. Det framkom också att företagsspionage bedöms komma att påverka den egna verksamheten liksom hot från cyberbrottslighet. Det finns därmed en riskmedvetenhet hos företag och privata organisationer inför ovanstående hot. Samtidigt finns en diskrepans mellan den upplevda hotbilden och de säkerhetsåtgärder som företag faktiskt vidtar.⁹

⁶ Svenska Dagbladet "Annan drabbades av Echelon" 040228

⁷ Financial Post 040407 "Air Canada accuses WestJet of espionage: Blames ex-employee", Calgary Herald "WestJet CEO silent on suit" 040420

⁸ Aftonbladet "Toyotas F1-bil en spionaffär?" 031103

⁹ CIOS/FHS

3 Sverige

3.1 Anställd kopierade företagsinformation

En anställd på ett företag inom fordonsindustrin åtalades i början av 2004 för dataintrång och företagsspionage efter att ha kopierat hemliga uppgifter. Informationen gällde bland annat sekretessbelagd leverantörsinformation.¹⁰ I slutet av maj 2004 friades mannen från misstankarna. Enligt domen finns inget underlag för att bedöma hurvida informationen som mannen haft tillgång till är att betrakta som företagshemligheter. Tingsrätten påpekar också att det inte stod klart vilken information de anställda på företaget hade rätt att ta del av.¹¹

Dataintrång utfört av anställda eller anställda som använder sig av känslig företagsinformation på ett felaktigt sätt är ett fortsatt stort hot mot företagets säkerhet. Händelsen visar på vikten av att skydda känslig information i interna nätverk och att dokumentera vilken slags information personal har rätt att ta del av. Har information väl läckt ut är det svårt att bevisa att det rör sig om företagshemligheter som kan skada företaget.

3.2 Stämningsansökan gav tillgång till företagsinformation

Ett svenskt IT-företag har stämt ett konkurrerande företag för intrång i upphovsrätten. En tidigare anställd skall ha tagit med sig ett dataprogram han utvecklat hos sin tidigare arbetsgivare. I och med stämningsansökan har Kronofogdemyndigheten beslagtagit material i form av offerter och källkoder hos det konkurrerande företaget som det aktuella IT-företaget sedan fick tillgång till. Detta utan att invänta företagets svar på anklagelserna. Tingsrätten har nu beslutat att upphäva beslutet om intrångsundersökning och konstaterar att upphovsrätten till dataprogrammet inte tillfaller mannens före detta arbetsgivare. Det företag som blivit stämt räknar med att kräva skadestånd i och med att företagshemligheter läckt ut. Tvisten är därmed ännu inte avgjord.¹²

Artikeln är ytterligare ett exempel på före detta anställda som tar med sig information till nya arbetsgivare. I det här fallet har också det företag som stämt sin konkurrent kommit över hemlig information genom att ta del av handlingar som blivit offentliga.

3.3 Mobiltelefoner en säkerhetsrisk

Få företag har en säkerhetspolicy gällande användning av mobiltelefoner. Affärsresenärer, militärer och diplomater är exempel på personer som riskerar att bli avlyssnade. I och med uppmärksam avlyssning av FN framförs nu krav på att svenska ministrar bör använda krypterade telefoner för att säkra sin kommunikation. Hackerverktyg för avlyssning är lätt att tillgå och finns att köpa över Internet. Det är därför viktigt att se över inte bara tekniken man använder utan också vilken information som diskuteras över mobiltelefonen.¹³

Enligt uppgifter i Aftonbladet har en svensk kommunpolitiker polisanmälts och blivit avstängd från sin arbetsplats för att ha avlyssnat kollegor genom en mobiltelefon. Mobiltelefonen hade placerats påslagen i en kopp i en bokhylla.¹⁴

¹⁰ Göteborgsposten "Tidigare anställd kopierade hemliga datafiler – åtalas" 040127

¹¹ TT "Friad från misstankar om företagsspioneri" 040602

¹² Svenska Dagbladet "Delseger för dataföretag i upphovsrättvist" 040519

¹³ Aftonbladet "Hans Blix buggad under FN-uppdrag" 040227, Computer Sweden "Mobilen osäker för affärssamtal". "Tekniken inget hinder för företagsspioneri" 040303

¹⁴ Aftonbladet "Politiker avlyssnade kollegor" 040610

Ytterligare en säkerhetsrisk som uppmärksammats är mobiltelefoner med inbyggd kamera och möjligheten att använda denna för att fotografera företagshemligheter. Fenomenet är relativt nytt och ännu har inga fall påträffats. Vissa företag har dock valt att förbjuda användning av mobiltelefoner med kamera.¹⁵

3.4 Affärsplaner diskuterades öppet på flygplan

Under en flygresa diskuterade två chefer för ett mobiloperatörsföretag öppet känslig företagsinformation. Bakom dem satt en koncernchef från ett konkurrerande bolag och överhörde samtalet. Händelsen har fått stark kritik internt på det aktuella företaget och ansågs extra problematisk då det rörde sig om företagets chefer vilka kan besitta kritisk information och också skall fungera som föredöme för övriga anställda. Att diskutera företagsinformation öppet kan medföra stora skador för ett företag.¹⁶

¹⁵ Computer Sweden "Volvo förbjuder kameramobil" 040310

¹⁶ Blekinge Läns Tidning "Toppchefer avslöjade hemliga affärsplaner" 040124