



Spioneri via internet och insiderstöder allt vanligare

Företagsspionage är ett kontroversiellt begrepp. Det dyker upp som skällsord när företag eller länder anklagas för att med tveklaktiga metoder ha tillskansat sig skyddad och känslig information om andra företags verksamheter, särskilt när det gäller forskning och utveckling. Andra menar att det är en ganska alldaglig och mestadels laglig företeelse för att hålla sig à jour med den industriella och tekniska utvecklingen inom en bransch. Gränsen mot "äkta" företagsspionage blir ibland otydlig och diffus. Utöver detta skiljer sig etik, moral och lagstiftning åt länder emellan, och vad som är tillåtet i ett land kan vara förbjudet i ett annat.

Vad man emellertid kan konstatera är att spionage och intrång via datorer och internet ökar och utvecklas, samt att allt mer av världen blir mobil. Exempelvis skaffar sig 13 miljoner indier mobiltelefon varje månad, och av världens 6,6 miljarder invånare har 4,4 miljarder en mobiltelefon. Kameror, USB-minnen, iPods och CD-skivor med mängder av information byter lätt ägare vilket, om de skulle hamna i konkurrentens händer, kan innebära att vi köper tillbaka vår egen teknologi i slutändan. Också det stigande beroendet av internetbaserade kommunikationsverktyg har ökat sårbarheten gentemot insiderstöder, hackers och spioner.

Intrångsförsöken via internet mot svenska företag har ökat markant, och mörkertalet bedöms som mycket stort då ingen vill skylta med bristfällig säkerhet. Detsamma gäller i många andra länder. Frågar man dock företagsledare anonymt, börjar man förstå vidden av problemet.

I en amerikansk studie utförd av Purdue's Krannert School of Management (finansierad av McAfee) uppgav 119 av närmare 800

BRITTISK DUO ÅTALAS FÖR FÖRETAGSSPIONAGE MOT AMERIKANSKA GOODYEAR
se sidan 2

RYSK DOMSTOL DÖMER AMERIKANSK-RYSKA BRÖDER FÖR FÖRETAGSSPIONAGE
se sidan 3

ESTNISKA ENTREPRENÖRER HOTAS AV RYSKT FÖRETAGSSPIONAGE
se sidan 3

SHERATONÄGARE STÄMMER HILTON FÖR FÖRETAGSSPIONAGE
se sidan 3

FERRARI & MASERATI VERSUS BENTLEY & ASTON MARTIN
se sidan 4

FRANSK ENERGIJÄTTE MISSTÄNKTS HA SPIONERAT PÅ GREENPEACE
se sidan 4

GIGANTISKT BOTNÄT STYRS FRÅN UKRAINA
se sidan 5

MISSTÄNKT FÖRETAGSSPIONAGE MOT AMERICAS CUP-VINNAREN ALINGHI
se sidan 5

TOPPHEMLIG TELEFON STULEN
se sidan 5

PENTAGONS JOINT STRIKE FIGHTER JET-PROJEKT UTSATT FÖR CYBERSPIONER
se sidan 6

USA:S ELNÄT ANGRIPET AV SPIONER
se sidan 6

RAZZIA MOT MISSTÄNKTA I PATRIAHÄRVAN
se sidan 7

ANGIE'S LIST STÄMMER KONKURRENTEN TRUSTYS.COM FÖR FÖRETAGSSPIONAGE
se sidan 7

Nyhetsbrevet baseras på information från ett urval av artiklar som handlar om informationssäkerhet eller företagsspionage. Artiklarna är publicerade i svensk och internationell press januari till och med maj 2009.

tillfrågade företagsledare att de hade blivit bestulna på företagshemligheter. Vidare uttryckte 42 procent ett upplevt ökat hot av insiderstödler som en följd av den globala konjunkturnedgången. Uppsagd personal tros bli mer benägen att sälja konfidentiella uppgifter till konkurrenter eller att erbjuda en ny potentiell arbetsgivare information för att bli mer attraktiv i en anställningssituation. Oron är berättigad då rapporterade insiderstölder ska ha fördubblats mellan 2007 och 2008. Vanligast förekommande var detta inom sektorn för finansiella tjänster vilken drabbats extra hårt av uppsägningar.

En annan studie bland 600 kontorsanställda i London, New York och Amsterdam visade att datastöld och företagsspionage är på väg uppåt. Det största hotet kommer inte från hackers utan från egna anställda som oroar sig för arbetslöshet. 56 procent av de tillfrågade kände oro över att bli av med sina jobb på grund av den nedåtgående ekonomin, och över hälften erkände att de redan nu laddar ner konkurrenskraftiga företagsdata i väntan på att eventuellt komma att behöva säkra nästa steg i yrkeslivet.

Bilden kompletteras av ytterligare en studie utförd av Ponemon Institute där 945 vuxna amerikaner ingick, vilka blivit avskedade, friställda eller bytt jobb det senaste året och som alla hade tillgång till kunduppgifter, finansiell information, konfidentiella data eller annat av värde. Studien visade att sex av tio anställda hade stulit företagsdata när de lämnat sina jobb.

De mest åtråvärda uppgifterna att ta med sig är lösenord, kund- och kontaktdatabaser, offerter, produktinformation och affärsplaner. HR- och rättsliga dokument är av lägst intresse.

Arbetsgivare behöver kontrollera användningen av sina IT-verktyg för att trygga både säkerhet och effektivitet inom företaget, och behovet av kontrollåtgärder ökar i takt med den tekniska utvecklingen. I Sverige tillåts arbetsgivare idag ta del av anställdas e-post och internetanvändande inom vissa ramar (såsom

PUL och straffbestämmelser), men sedan några år tillbaka har det utretts hur den enskildes personliga integritet i arbetslivet kan stärkas. Ett starkare skydd för den enskildes personliga integritet på bekostnad av arbetsgivares möjligheter att skydda sina hemligheter är dock ingen självklarhet. I Finland beslutades exempelvis nyligen att arbetsgivare ska ha rätt att utföra viss kontroll av anställdas e-brev om de misstänker att företagshemligheter läcker ut. Syftet med den nya regleringen är just att försöka förhindra företagsspionage.

Källor: e24.se, 2009-05-22; The Wall Street Journal, 2009-04-21; Computer World, 2009-04-11; Dagens Industri, 2009-04-02; Svenska Dagbladet, 2009-03-13; BBC News, 2009-02-23 och Forbes.com, 2009-01-29

Brittisk duo åtalas för företagsspionage mot amerikanska Goodyear

Två ingenjörer (46 och 38 år gamla) från Wyko Tire Technology Inc., ett ledande brittiskt däck-tillverkningsföretag, ska år 2007 under falska förespeglningar ha tagit sig in i en Goodyear-fabrik i Kansas och med en vanlig mobiltelefon smygfotoferat sju bilder av välbevakad topphemlig utrustning avsedd för en särskild typ av däcktillverkning. Den ene tog bilderna medan den andre agerade utkik. Bilderna skickades via e-post till två Wyko-kollegor i Storbritannien och användes som underlag för att tillverka en liknande utrustning åt Haohau South China Guilin Rubber Company i nordöstra Kina. Kontraktet med Kina uppges ha varit värt 1,2 miljoner US-dollar.

FBI kallades in för att utreda fallet och duon har nu åtalats för sammanlagt 12 brott i sammanhanget. Trots att de nekar till anklagelserna har de att förvänta sig ett maxstraff på 150 år i fängelse och böter på 2,75 miljoner US-dollar.

Källor: Lawiscool.com, 2009-03-27; www.news.webinida123.com, 2009-03-10; Times Online, 2009-03-09 och Associated Press, 2009-03-07

Rysk domstol dömer amerikansk-ryska bröder för företagsspionage

Den ryska federala säkerhetstjänsten meddelar att två bröder dömts till ett års villkorlig dom då de försökt samla in sekretessbelagda kommersiella uppgifter från det statsägda ryska energibolaget Gazprom. Bröderna, med dubbla amerikansk-ryska medborgarskap, försökte muta sig till insideinformation från Gazprom-anställda för att ge vidare uppgifterna till utländska bolag och på så sätt ge dem fördelar gentemot ryska företag.

Bröderna greps i mars 2008. Den ene var då anställd av TNK-BP, en stor rysk-brittisk energi-koncern, och den andre arbetade för en alum-niförening initierad av den brittiska ambassa-dens kulturella utskott i Moskva. Gripandet gav upphov till spekulationer som kretsade kring eventuella försämrade relationer mellan Stor-britannien och Ryssland pga ett antal tidigare spionskandaler, vilket det ryska utrikesministe-riet dock tillbakavisade.

Källa: Associated Press, 2009-05-07

Estniska entreprenörer hotas av ryskt företagsspionage

KAPO, estniska motsvarigheten till Säkerhets-polisen, har gått ut med en varning till före-tagare gällande ett ökat hot av ryskt företags-spionage. Det tilltagande intresset för Estland uppges bero på landets vetenskapliga utveck-ling och stegrande internationella samarbete.

Ryssland är enligt KAPO mycket intresserade av den estniska energisektorn, främst i samband med implementeringen av Nord Stream-projek-tet längs Östersjöns botten.

Källa: shaan.typepad.com, hänvisning Interfax, 2009-04-18

Sheratonägare stämmer Hilton för företagsspionage

Starwood – ägare av bland annat Sheraton, Le Meridien och lyxhotellkedjan W Hotels – har stämt Hilton och två Hiltonanställda för före-tagsspionage. Starwood hävdar att lanseringen av Hiltons senaste satsning, superlyxhotellked-jan Denizen Hotels i 13 storstäder världen över, har grundats på 100 000 dokument, presen-tationer och marknadsundersökningar som stulits av före detta Starwoodanställda.

Hilton har kritiserats av hotellbranschen för att ännu inte ha tagit plats inom det så kallade luxury lifestyle-segmentet på marknaden. I juni 2008 tog dock Hilton över två chefer från Starwood, vars nyckelbefattningar var just inom luxury and lifestyle brands respektive det segmentets utveckling. De fick i uppgift att arbeta med Denizen som skulle bli Hiltons svar på Starwoods lyxhotellkedja W. Den slående likheten med W ska ha påtalats vid en press-konferens.

Starwood påstår att de bägge männen sparade ned dokument till sina privata e-postkonton innan de gick över till konkurrenten Hilton. Dokumenten innehöll sammantaget en plan för lanseringen av W Hotels-kedjan, och Star-wood hävdar att Hilton omöjligt kan ha hunnit lansera Denizen inom loppet av mindre än ett år utan tillgång till all denna information.

I väntan på översyn arbetar för närvarande varken de två cheferna eller resten av luxury and lifestyle development-teamet bestående av flertalet före detta Starwoodanställda. En brottsutredning har inletts och en federal jury ska fatta beslut om åtal.

Hilton har tillkännagivit stämningen samt försening av Denizen-lanseringen. Dock förnekar Hilton och de bägge cheferna anklagelserna.

Källor: The New Zealand Herald, 2009-04-23 och Industry.bnet.com, 2009-04-21

Ferrari & Maserati versus Bentley & Aston Martin

Två ägare av Bentley- och Aston Martinåterförsäljaren Universal Autosports LLC, (43 och 42 år gamla) greps tillsammans med företagets 40-åriga creative director i sina hem i New York anklagade för olaglig avlyssning av Ferrari Maseratis e-post. Mellan februari och september 2008 ska de vid inte mindre än cirka 2 500 tillfällen ha tagit sig in på Ferrari Maseratis e-postserver, såväl från Universal Autosports som från sina egna hem.

Den ene ägaren var tidigare general manager på Ferrari Maserati, och 40-åringen var den webbansvarige som lade upp Ferrari Maseratis e-postkonton. 2007 byttes ledningen ut. I september 2008 upptäckte man plötsligt att anställdas e-post vidarebefordrades till en obehörig e-postadress på företagets server. Berörda e-brev innehöll bland annat information om kunder, lager och anställdas ersättning.

Informationen ska bland annat ha utnyttjats vid försök att ta över en potentiell Ferrari Maserati-kund som höll på att förhandla om en Ferrari Enzo värd över 1,3 miljoner US-dollar. Konkurrentens återförsäljare kontaktade kunden och frågade om Ferrari Maserati hade hittat en lämplig bil ännu, eller om han kunde hjälpa till och komma in i bilden på något sätt.

FBI engagerades i fallet, och straffet kan bli upp till fem års fängelse samt 250 000 US-dollar i böter.

Källa: Bloomberg.com, 2009-04-22

Fransk energijätte misstänks ha spionerat på Greenpeace

Två seniora säkerhetschefer vid den franska statliga elleverantören Électricité de France (ÉDF) har fått sina datorer konfiskerade av fransk polis. Ytterligare tre personer (chefen för privata utredningar på företaget Kargus Consultant, och två icke namngivna personer varav en uppges vara "datorexpert") har åtalats för medverkan till spionage mot Greenpeace genom olagligt intrång i organisationens servrar och nätverk.

Greenpeace har under senare år ingått i ett slags politisk vendetta mot ÉDF där de utövat påtryckningar mot energijätten för att minska dess omfattande nätverk av kärnkraftsreaktorer i Frankrike. ÉDF är numera även ägare av British Energy, den största kärnkraftsoperatören i Storbritannien.

En av säkerhetscheferna har tidigare arbetat som polisbefäl. Med franska underrättelsetjänstens initierade bombning av Greenpeaces flaggskepp Rainbow Warrior för 24 år sedan i minne utreds nu huruvida världens största kärnreaktoroperatör anlitat en privatdetektivbyrå, som drivs av en tidigare medlem av den franska säkerhetstjänsten, för att olagligt spionera på miljöaktivister och infiltrera anti-nukleära led. Kargus privatdetektivbyrå uppges ha anlitats av ÉDF för att "tillhandahålla ospecificerade tjänster".

ÉDF förnekar anklagelserna och hävdar istället att det är de som fallit offer för illegal verksamhet genom Kargus självvådiga beslut att spionera på Greenpeace. Dock ska "datorexperten" redan ha erkänt.

Källor: IntelNews.org, 2009-04-04; Greenpeace.org, 2009-04-02 och Guardian.co.uk, 2009-04-01

Gigantiskt botnät styrs från Ukraina

FBI och brittisk polis uppges jaga ett gäng på sex IT-brottslingar från Ukraina som misstänks ha skapat ett rekordstort zombienätverk bestående av cirka 1,9 miljoner datorer världen över. I nätverket ingår bland annat 77 amerikanska regeringsdomäner, stora universitet och några av världens största privata företag. Det är oklart hur många svenska datorer som ingår i nätverket.

Med hjälp av en ukrainsk server kan angriparna fjärrstyra de kapade datorerna, ladda ned ytterligare skadlig kod och avlyssna datorerna genom att registrera tangentbordstryckningar vilket öppnar möjligheten att använda nätet till riktat företagsspionage. Säkerhetsexperter från företaget Finjan har kunnat undersöka servern, då den förvånansvärt nog inte skyddats till 100 procent.

Botnät skapas i regel med hjälp av trojaner eller annan typ av skadlig kod som sprids via falska e-postutskick, svagheter i webbläsare alternativt genom andra webbsidors länkar och nedladdningsbar programvara.

Källa: Computer Sweden, 2009-04-22

Misstänkt företagsspionage mot Americas Cup-vinnaren Alinghi

Åtminstone en person ska ha arresterats i Villeneuve i Frankrike, misstänkt för företagsspionage mot det schweiziska Americas Cup-syndikatet Alinghi. Fransk polis har varit mycket förtegen om denna utredning, som är kopplad till seglingens motsvarighet till formel ett, och hänvisar förfrågningar till franska rättssystemets centrala informationskontor.

På YouTube har man sedan en kort tid tillbaka kunnat se en 3D-modell av en Alinghi-båt som uppges emanera från spionbilder. Det är okänt om händelserna har något samband.

Källa: Spybusters.blogspot.com, 2009-05-14

Topp hemlig telefon stulen

Australiensiska teleoperatören Telstras före detta VD uppges ha blivit utsatt för en fiktjuv som bestulit honom på en mobiltelefon. Men det var inte vilken telefon som helst utan en prototyp med den senaste utvecklingsversionen av Microsofts operativsystem Windows Mobile 6.5.

Stölden inträffade i Barcelona där han befann sig på 3GSM: *Mobile World Congress*, världens största mobiltelekommunikationskonferens, dit telefonen lånats ut av Microsoft för att visas upp.

Oklarheter råder kring vilken telefonmodell det gäller, men det talas om att det antingen var en HTC Touch Pro 2 eller en Touch Diamond 2.

Förutsatt att fiktjuven vet vad han eller hon kommit över kan stölden orsaka stora problem för Microsoft, som varit mycket återhållsamma gällande vem som får testköra produkten. Windows Mobile 6.5 släpps först i slutet av 2009. Trots risken för företagsspionage uppges Microsoft ta det inträffade med ro.

Den före detta VD:n har varit mycket kontroversiell under sin tid på Telstra. Han uppges ha återvänt till USA och avgått från sin chefspost på Telstra i maj 2009 – en dryg månad före utsatt tid.

Källor: Computer World, 2009-05-21; The Sydney Morning Herald, 2009-05-19 och Computer Sweden, 2009-02-19

Pentagons Joint Strike Fighter jet-projekt utsatt för cyberspioner

Amerikanska försvarsdepartementets mest påkostade vapenprogram någonsin, det 300 miljarder US-dollar dyra Joint Strike Fighter jet-projektet, har utsatts för intrång av cyberspioner.

Inkräkterna har kopierat och laddat ned flera terabyte data med anknytning till design och elektroniska system. Informationen kan ge kunskap som underlättar framtagandet av försvarsmetoder mot flygplanet. Dock fick de inte tillgång till det allra mest känsliga materialet då det lagras på datorer som inte är internetanslutna.

Man har inte kunnat fastställa identiteten på dem som ligger bakom intrånget, och inte heller skadornas omfattning på det amerikanska försvarets program varken ur ett säkerhets- eller finansiellt perspektiv.

Före detta amerikanska tjänstemän har spekulerat i huruvida attackerna kan ha sitt ursprung i Kina. Liknande attacker tycks ha eskalerat de senaste sex månaderna och det är såväl militära som civila myndigheter och privata företag som berörts.

Källa: The Wall Street Journal, 2009-04-21

USA:s elnät angripet av spioner

Cyberspioner ska ha gjort intrång i USA:s elnät och placerat ut mjukvaruprogram med syfte att störa systemet. Någon störning har inte noterats, men man har varnat för att så kan komma att ske vid händelse av krig eller någon annan form av krissituation. Enligt såväl före detta som nuvarande säkerhetstjänstemän kommer spionerna främst från Kina och Ryssland, men även från andra länder.

Ett flertal liknande intrång har upptäckts och tycks öka i antal. De flesta har upptäckts av underrättelsetjänsten och inte av dem som drabbats. Underrättelsepersonal ser med oro på illasinnade försök att via internet kartlägga USA:s infrastruktur såsom elnät, kärnkraftsverk och finansiella nätverk. Även vatten, avlopp och annan basstruktur kan vara i fara.

Att skydda USA:s infrastruktur är en av Obama-administrationens prioriterade frågor. Bush-administrationens kongress godkände 17 miljarder US-dollar i hemliga fonder för att skydda regeringens datornätverk. Bara det senaste halvåret har Pentagon lagt ut 100 miljoner US-dollar på reparation av cyberskador. Det övervägs att framöver även inkludera privata datornätverk i skyddsprogrammet.

Det ökade beroendet av internetbaserade kommunikationsverktyg har ökat kontrollsystemens sårbarhet gentemot hackers och spioner. I huvudsak antas Kina och Ryssland ligga bakom attackerna, men även terroristgrupper kan komma att utveckla förmågan att penetrera amerikansk infrastruktur, menar underrättelsepersonal och cybersäkerhetsspecialister.

Ryssland och Kina har förnekat all sådan verksamhet och tillbakavisar anklagelserna som rena spekulationer.

Källa: The Wall Street Journal, 2009-04-08

Razzia mot misstänkta i Patriahärvan

Den finska försvarskoncernen Patria har drabbats av en mutskandal. Finska och slovenska polisen har genomfört en razzia mot de misstänkta bostäder och arbetsplatser på olika håll i Slovenien. En av de huvudmisstänkta uppges vara österrikare så numera ingår även österrikiska polisen i den gemensamma utredningsgruppen.

Koncernen misstänks för att via mellanhänder ha betalat över 21 miljoner euro i mutor till flera höga slovenska tjänstemän och politiker inför att man år 2006 kom överens om att sälja 136 pansarfordon av typen AMV till slovenska staten – ett kontrakt värt närmare 300 miljoner euro. Polisen misstänkte i höstas att det förekommit liknande oegentligheter i samband med en annan affär där Patria sålde kanoner till Egypten. Det fanns då även misstankar om att Patrias affärer i Kroatien inte heller tål dagsljus.

En tidigare VD vid Patria misstänks inte bara för grovt givande av muta och bestickning i näringsverksamhet, utan häktades i höstas misstänkt även för försök till företagsspionage. I augusti förra året tvingades han avgå som VD och hävdade under hösten att han var oskyldig till brott. Istället skyllde han på att den politiska oppositionen i Slovenien ska ha misstänkliggjort Patria på inrikespolitiska grunder.

Centralkriminalpolisen hade som mål att bli klara med förundersökningen under våren 2009.

Källa: Svenska.yle.fi, 2009-04-15; Svenska.yle.fi, 2009-03-26; Hbl.fi (Hufvudstadsbladet), 2008-11-14 och Svenska.yle.fi, 2008-09-05

Angie's List stämmer konkurrenten Trustys.com för företagsspionage

Angie's List erbjuder en söktjänst på internet där man presenteras bedömningar för varje enskild leverantör eller företag inom olika branscher. Grundaren av nykomlingen Trustys.com har enligt Angie's List stulit tusentals filer från dem i syfte att starta en konkurrerande verksamhet.

Till en början ska Trustys.com:s grundare varit en vanlig medlem på Angie's List, för att sedan ha använt sig av ett så kallat botmjukvaruprogram för att tillskansa sig tjänsteleverantörsrapporter, leverantörsbedömningar och annan information som använts till Trustys.com.

Den stämades advokat bestrider anklagelserna.

Källa: InfoSec News, 2009-01-14

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 Åsa Hedin

Säkerhetspolisen, Box 12312, 102 28 Stockholm
Tfn: 010-568 70 00 • Fax: 010-568 70 10
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