



## SAS i Norge får böta för spionage

Flygbolaget SAS i Norge döms till fyra miljoner norska kronor i böter för industrispionage mot konkurrenten Norweigan. Domstolen anser att SAS har inhämtat och använt företagshemligheter från Norwegian under perioden december 2001 till november 2005. Uppgifterna ska SAS ha kommit över via ett bokningssystem.

SAS Norge har tidigare frikänts i en lägre instans. SAS reagerar därför med förvåning:

– Vi menar att det inte lagts fram några bevis som stödjer saken den här gången heller, säger en hög representant från SAS.

Domen anses göra det möjligt för Norweigan att driva en civilrättslig process mot SAS. Företaget har tidigare hävdats att SAS beteende kan ha kostat lågprisbolaget upp emot en halv miljard kronor, ett belopp som kan utkrävas i en civilrättslig process.

Källa: [www.dinapengar.se](http://www.dinapengar.se), 2007-10-02

## Företagsledning är måltavlor för industrispionage

Flera exempel på att företagsledningar och personer på hög nivå inom företag är attraktiva måltavlor för datorbaserade angrepp har uppdragats. Kriminella personer har utgivit sig för att tillhöra ett rekryteringsföretag och kontaktat ledande befattningshavare via e-post och på så sätt fört in illasinnad kod.

Den typ av handlingar som skickats har uppfattats som logiska försändelser och för mottagaren rimliga att acceptera och öppna.

Källa: [ZDNet Australia](http://ZDNet Australia), 2007-09-25

**SAS I NORGE FÅR BÖTA FÖR SPIONAGE**  
se sidan 1

**FÖRETAGSLEDNINGAR ÄR MÅLTAVLOR FÖR INDUSTRI-SPIONAGE**  
se sidan 1

**JAPANSKA FÖRETAG RUSTAR SIG FÖR ATT MÖTA HOTET FRÅN INDUSTRI-SPIONER**  
se sidan 2

**TVÅ PERSONER ANKLAGADE FÖR SPIONERI SÖKTE FINANSIERING I KINA**  
se sidan 2

**EXPERTER FÖRSIKTIGA I UTTALANDEN OM PÅSTÄDDA KINESISKA DATOR-INTRÅNG**  
se sidan 2

**AMERIKANSKA FBI MENAR ATT FÖRETAG BEHÖVER LÄRA SIG OM KONTRASPIONAGE**  
se sidan 3

**NYTILLTRÄDD KINESISK SPIONCHEF EXPERT PÅ AFFÄRSHEMLIGHETER**  
se sidan 3

**HACKERS STAL KONFIDENTIELLA UPPGIFTER OM 60 000 NORSKA PERSONER**  
se sidan 4

**SÄKERHETSPROFIL GRIPEN MISS-TÄNKT FÖR SPIONERI**  
se sidan 4

Nyhetsbrevet baseras på information från ett urval av artiklar som handlar om företags- eller industrispionage. Artiklarna är publicerade i svenska och internationella källor från augusti 2007 till och med november 2007.

## Japanska företag rustar sig för att möta hotet från industri-spioner

Japanska företag ökar sitt skydd mot stöld av ny teknik och information genom att i högre utsträckning övervaka sin personal och personer som besöker företagets lokaler.

En förklaring till denna trend anses vara den förändring som metoder för industrispionage har genomgått. Inträffade incidenter påvisar att framväxten av informationsteknologi har skapat större handlingsutrymme för illasinnade personer att stjäla affärshemligheter, ofta med stöd från personal ur det drabbade företaget.

Det finns exempel på företag som vidtar säkerhetshöjande åtgärder till den grad att det påverkar deras konkurrenskraft negativt. Under hösten 2006 lät ett stort amerikanskt IT-företag undersöka sina styrelsemedlemmar i ett försök att finna källan till informationsläckage. Denna undersökning resulterade i en polisutredning med anledning av de olagliga metoder som vidtagits för att övervaka och kartlägga delar av den egna personalen.

Motmedel mot företagsspionage utvecklas i allt snabbare takt och moderna företag står inför utmaningen att finna en balans mellan skyddet av affärshemligheter och personalens integritet.

*Källa: Nikkei Telecom 21, 2007-09-25*

## Två personer anklagade för spioneri sökte finansiering i Kina

En federal jury dömde två personer i Kalifornien, USA, för att ha konspirerat i syfte att stjäla hemlig information om känslig högteknologi. De två personerna, båda anställda vid det drabbade företaget, beskylls för att ha stulit informationen för att själva vidareutveckla produkterna. Finansiering för vidareutvecklingen ska de ha försökt att erhålla från ett statsfinansierat forskningsprojekt i Kina.

*Källa: IDG News Service, 2007-09-27*

## Experter försiktiga i uttalanden om påstådda kinesiska datorintrång

Sedan en tid har kinesiska myndigheter pekats ut som bakomliggande aktörer till flertalet datorbaserade intrång mot olika länders regeringar. Enligt regeringarnas rapportering förefaller intrången härstamma från Kina.

Nu vill flera säkerhetsexperter höja ett varningens finger mot att dra slutsatser alltför snabbt. Bara för att angreppen förefaller härstamma från Kina behöver det inte innebära att de ursprungligen initierats från ett helt annat land.

Datorer i utvecklingsländer kan mycket väl utgöra sista anhalt då en IT-angripare planerar angreppets väg till målet. Mycket på grund av bristande säkerhetssystem och rutiner i utvecklingsländerna – ett svagt system är lättare att utgå från än ett säkerhetsmässigt avancerat IT-system.

Att dessutom försöka identifiera om intrånget är statsfinansierat är en komplex utmaning som ofta kräver omfattande kompetenser och resurser.

En hög representant från ett internationellt känt IT-säkerhetsföretag har uttryckt oro över att företag i alltför hög utsträckning fokuserar på intrångsprevention och lätt förbiser åtgärder som begränsar att information exporteras ut från de egna IT-systemen.

*Källa: Computer World, 2007-09-24*

## Amerikanska FBI menar att företag behöver lära sig om kontraspionage

Amerikanska Federal Bureau of Investigation (FBI) uppmanar allt fler företag att ansluta sig till satsningen Counterintelligence Domain Program. Genom samarbete med näringslivet förväntar sig FBI att bättre kunna motarbeta hackers och datastöld.

Det tilltagande hotet från spionage utfört med hjälp av högteknologi, såsom datorintrång, har medfört att FBI nu uppmanar akademiska organisationer och privata företag att bättre rusta sig mot dessa hot.

Bland annat menar FBI att företag i högre utsträckning än vad som gjorts tidigare behöver övervaka sin verksamhet för att lättare kunna utreda ett händelseförlopp när ett informationsläckage misstänks eller upptäcks.

Ett bättre samarbete mellan FBI och akademiska och privata organisationer, i kombination med FBI-arrangerade utbildningsseminarium syftar ytterst till att identifiera forskning, information och teknologi som kan vara föremål för främmande underrättelseintresse. Genom att etablera relationer och ett aktivt informationsutbyte mellan de i Domain-programmet ingående organisationerna hoppas FBI tidigare kunna upptäcka illasinnade inhämtningsförsök.

Chefen för Domain-programmet Tom Mahlik kommenterar satsningen:

– Det handlar inte längre om traditionella spioner; ingenjören, studenten, affärskontakten är exempel på karaktärer som numera representerar hotet. Det är just dessa karaktärer som i ökad utsträckning bereds access till företags-hemligheter, kritisk information och forskningsmaterial vid universiteten.

Stora företag har öppet börjat beskriva problemen de har med IT-stödda informationsstölder. Vid Usenix Security Symposium som hölls i Boston i augusti 2007 beskrev Jerry Brady, IT-säkerhetschef för den världsomspännande finansjätten Morgan Stanley, hotet organisationen

upplevde från dylika attacker som en rådande affärsrealitet. Särskilt bekymmersamt uppgavs läget vara i fjärran östern.

*Källa: Infoworld, 2007-09-06*

## Nyttillträdd kinesisk spionchef expert på affärshemligheter

Utnämningen av Geng Huichang till minister med ansvar för statssäkerhet indikerar en kinesisk satsning på att i ännu större utsträckning inhämta, men också skydda affärshemligheter. *Ministeriet för statssäkerhet* har länge beskrivits som Kinas version av före detta Sovjetunionens beryktade KGB.

För att möjliggöra satsningen på affärshemligheter och kommersiellt orienterad information har några av ministeriets uppgifter förts över till den kinesiska militären eller till polisiära myndigheter, enligt Hong Kong-baserade Information Center for Human Rights and Democracy.

Geng uppges ha spenderat största delen av sin karriär inom området internationella relationer. Geng var chef för den regeringsstödda China Institute of Contemporary International Relations till och med 1995, då han stationerades utomlands.

Sedan 1998 har Geng arbetat som ställföreträdande minister vid *Ministeriet för statssäkerhet* och har bland annat föreläst om tekniker för att skydda och inhämta affärshemligheter.

*Källa: Associated Press, 2007-08-31*

## Hackers stal konfidentiella uppgifter om 60 000 norska personer

Hackers påstås ha utnyttjat en brist hos en av teleoperatören Tele2:s webbplatser och därigenom kommit över abonnemangsinnehavares personnummer och adresser. Det totala antalet berörda personer uppgick till 1,3 procent av Norges befolkning.

Tele2, som uppmanats flera gånger att öka säkerheten på webbplatsen, har lovat att vidta åtgärder. Norska polisen utreder stölden.

*Källa: AFP (Brisbane Times), 2007-08-12*

## Säkerhetsprofil gripen misstänkt för spioneri

En ansedd italiensk säkerhetsexpert har gripits för påstådd delaktighet i eftermälet till spionskandalen som kretsar kring företaget Telecom Italia.

Experten är gripen misstänkt för datorintrång och olovlig avlyssning enligt lokala italienska källor. Som del av ett IT-säkerhetsteam ska italienaren ha utfört penetrationstester av Telecom Italias IT-säkerhetssystem. Inom ramen för dessa tester ska en trojansk häst ha förts in i systemen. Teamet påstås även ha initierat olovlig avlyssning.

Den italienska polisen utreder ärendet.

*Källa: The Register, 2007-11-08*

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)**