
DSI
DJURLING
SÄKERHETSINFORMATION

DSI AB

- Är ett säkerhetsföretag inriktat på skydd av immateriella tillgångar såsom information, kunskap och strukturkapital.

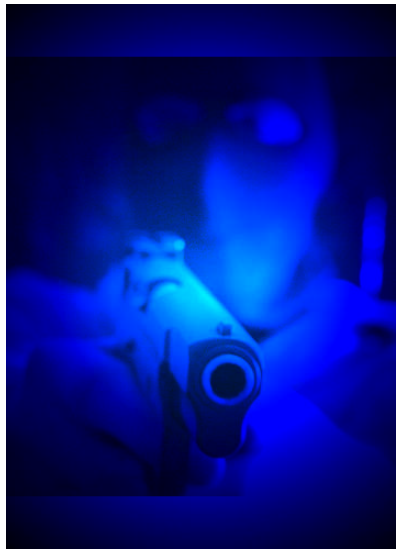
- Skyddet ges genom ett kvalificerat stöd i säkerhetsarbetet av de immateriella tillgångarna utifrån ett helhetsperspektiv, dvs IT-system, organisation, människor/personal.

Tomas Djurling

- Har arbetat inom den svenska underrättelsetjänsten i mer än 17 år.
- Fram till 1995 som systemprogrammerare på stordatorer och som projektledare.
- Under tiden 1996 – 2006 har jag byggt upp och drivit en enhet inom FRA som har till uppgift att skydda svensk samhällsviktig och samhällskritisk information och infrastruktur mot gränsöverskridande organiserad brottslighet, aktivism, industrispionage, cyberterror, andra länders informationsoperationer (IO) och psykologiska operationer (PSYOPS)

Praeparatus supervivet

Hoten mot våra IT-system



DJURLING
SÄKERHETSINFORMATION

HOTBILD IT-BROTTSLIGHETEN

- IT-brottsligheten och IT-relaterade brott
- Hackares ändrade inriktning (företagsledare etc. nytt mål)
- Kartläggning ett vanligt medel inför IT-brott
- Organisationsanpassade och riktade attacker mycket vanligare
- Autonom miljö (vänsterextrema grupper, Valet 2006 Nordiska förlaget

DJURLING
SÄKERHETSINFORMATION

HOTBILD IT-BROTTSLIGHETEN

Botnet (Robotnet)

- Är ett riktat medvetet sätt att ta över bristfälligt skyddade klient- och hemdatorer
- Tar över datorer i en omfattning som hittills saknar motstycke
- Datorerna används sedan i brottsliga syften
- Mindre botnets och priserna sjunker

DJURLING
SÄKERHETSINFORMATION

POLITISKT MOTIVERADE CYBERATTACKER

Mohammedkarikatyrerna

- Den största politiskt motiverade cyberattacken någonsin
- Internet Islamic Brigades m.fl. 100-talet kända islamistiska grupper.
- Bilder och text med hot om bombattacker, Jihad etc.
- Sverige och andra länder blev utsatta

Andra politiskt motiverade cyberattacker

- Amerikanskt spionplan 2001
- Amerikansk och brittisk invasion av Irak 2003
- Estlands flytt av krigsmonument 2007
- Lars Vilks rondellhund Sverige 2007


Terrorhot driver på stadsnät

Men Sverige är långt efter på trådlösa nät

DJURLING SÄKERHETSINFORMATION

POLITISKT MOTIVERADE CYBERATTACKER

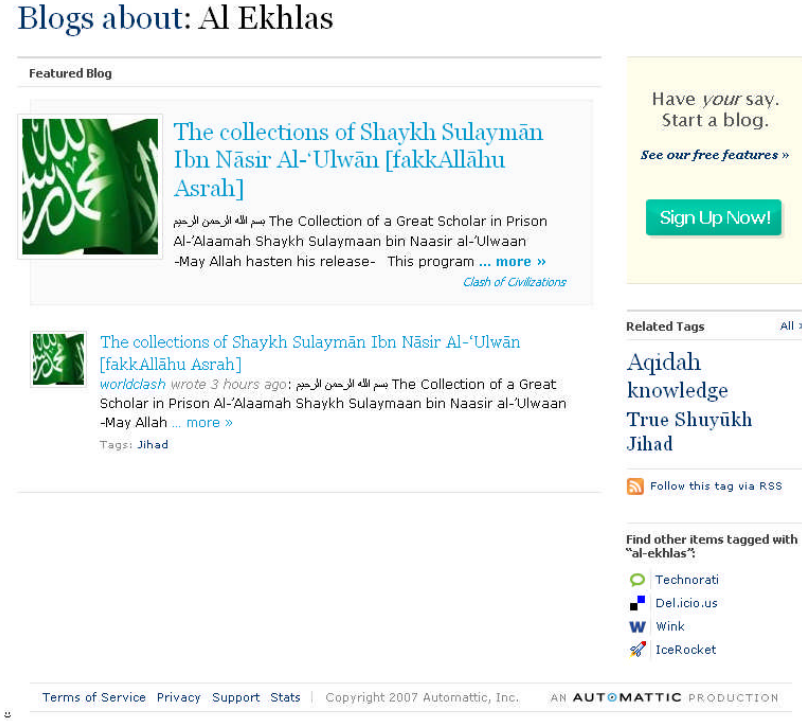
Når fantasien overgår virkeligheden

Sandheden om 11/9

DJURLING
SÄKERHETSINFORMATION

POLITISKT MOTIVERADE CYBERATTACKER

Sverige oktober 2007



Blogs about: Al Ekhlas

Featured Blog

The collections of Shaykh Sulaymān Ibn Nāsir Al-'Ulwān [fakkAllāhu Asrah]

بسم الله الرحمن الرحيم The Collection of a Great Scholar in Prison Al-'Alaamah Shaykh Sulaymaan bin Naasir al-'Ulwaan -May Allah hasten his release- This program ... more »

Clash of Civilizations

The collections of Shaykh Sulaymān Ibn Nāsir Al-'Ulwān [fakkAllāhu Asrah]

worldclash wrote 3 hours ago: بسم الله الرحمن الرحيم The Collection of a Great Scholar in Prison Al-'Alaamah Shaykh Sulaymaan bin Naasir al-'Ulwaan -May Allah ... more »

Tags: Jihad

Have *your* say. Start a blog.

See our free features »

Sign Up Now!

Related Tags All »

Aqidah knowledge True Shuyūkh Jihad

Follow this tag via RSS

Find other items tagged with "al-ekhlas":

Technorati
Del.icio.us
Wink
IceRocket

Terms of Service Privacy Support Stats | Copyright 2007 Automattic, Inc. AN AUTOMATTIC PRODUCTION

10 NYHETER

Svenskt hackerkrig mot Turkiet

Ett hackerkrig har brutit ut mellan Sverige och Turkiet. Förra veckan angrep turkiska hackare tusentals svenska sajter på internet och i helgen hämnades de svenska hackarna genom att bland annat

10 NYHETER

SvD lördag 6 oktober 2007

Sverige angrips på islamistisk hemsida

Påstådda al-Qaida-anhängare angriper Sverige i en ny video som har publicerats på en islamistisk webbsida. I filmen finns bilder på maskerade och beväpnade män, konstnären Lars Vilks och kung Carl XVI Gustaf. Men även Lars Vilks omdiskuterade Muhammedteckning visas i videon.

Lars Vilks teckning av profeten Muhammed som rondellhund har fått någon eller några som kallar sig "anhängarna av al-Qaida i Sverige" att producera en drygt fem minuter lång anti-svensk video.

Filmen publicerades i tisdags på det läsenordskyddade, islamistiska webbforumet al-Ekhlas. Det uppger den privatfinansierade, USA-baserade organisationen Site, som övervakar islamistiska webbplatser.

Inga direkta hot mot Sverige uttalas i den nya videon. En manröst läser en dikt som hyllar profeten Muhammed och samma budskap förs fram i en text på arabiska som rullar över skärmen.

"Hunden skäller, men dess skall skadar inte vår karaktär. Och ondskan kommer att träffa dig exakt", lyder en del av texten.

I videon visas bilder på konstnären Lars Vilks och på kung Carl XVI Gustaf. Filmen består övrigt av en serie stillbilder på moskéer, protestdemonstrationer, beväpnade mujaheddin-krigare och tecknade svenska flaggor.

"Din ära är min ära, min profet – tiden är inne för att beslutsamt försvara din ära", skriver filmskaparna.

Terroristexperten Magnus Ranstorp vid Försvarshögskolan har tittat på filmen för SvDs räkning. Han anser att det svårt att bedöma hur allvarligt man ska se på innehållet i filmen och vem som kan stå bakom den.

– Det skulle kunna vara en amatörs hemmaproduktion lika väl som det skulle kunna vara en allvarlig terrorist.

Magnus Ranstorp betonar att det inte finns något nytt, unikt material i filmen. Han förklarar att det är "förväntat att sådana här videor nu kommer fram".

Ranstorp pekar också på att det finns flera märkliga inslag i videon. Bilden på kungen är sannolikt från ett statsbesök i Kanada, vilket leder spåren till Nordamerika.

I videon visas även Lars Vilks Muhammedteckning flera gånger.

– Det stärker misstankarna om att det rör sig om en hemmaproduktion, säger Magnus Ranstorp.

Den svenska säkerhetspolisen, Säpo, känner till videon.

– Vi har sett den. Men jag vill inte kommentera enskilda videor som just har dykt upp på nätet. Vi tar allting på allvar och gör våra bedömningar hela tiden, säger Säpos informationsdirektör Anders Thornberg.

Lars Vilks, som har polisbeskydd efter uppståndelsen kring hans teckning, tar den nya videon med ro. Han säger att den "kan vara spännande att ha med i konstprojektet". Samtidigt tar han hoten på allvar.

– Det som är faran är om man får med sig folk som finns här i landet. Det är där det verkliga hotet ligger, säger Lars Vilks.

Det svenska hovet vill inte kommentera att kungen förekommer i videon.

BJÖRN MALMSTRÖM

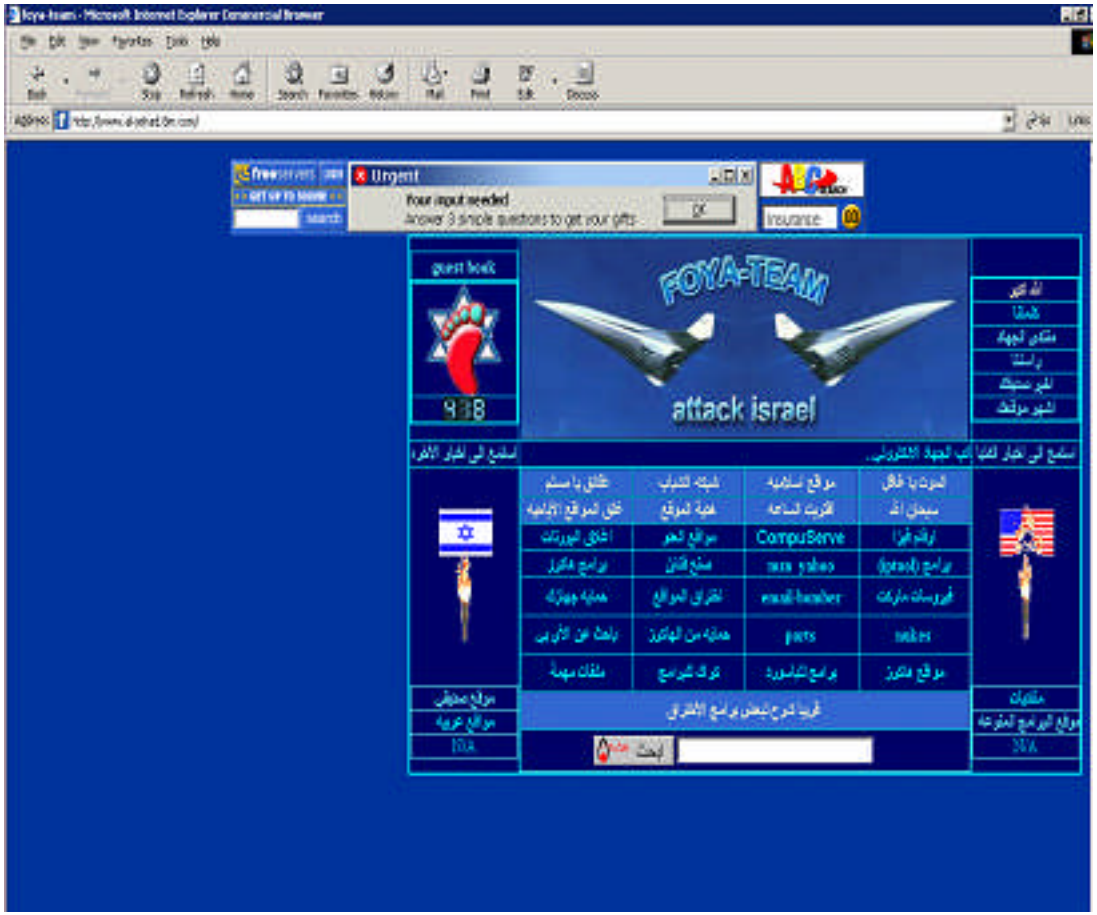
08-13 54 12, bjorn.malmstrom@svd.se

DJURLING SÄKERHETSINFORMATION

HOTBILD TERRORISTER

- Utnyttjar allmänt tillgänglig infrastruktur för planering, informationsinsamling, propaganda och desinformation
- Finansierar delar av sin verksamhet genom cyberattacker
- Rekryterar hackare och andra brottslingar
- SCADA-systemen är ett självklart mål för terrorister. Det är bara en tidsfråga innan det händer.

HAMAS WEB WARFARE



FOYA-Team

Instructions in building bomb email attacks, hacking etc.

DJURLING
SÄKERHETSINFORMATION

POLITISKT MOTIVERADE CYBERATTACKER

Al-Jihad Al-Elektroni (Electronic Jihad)

Unknown sponsorship

DJURLING
SÄKERHETSINFORMATION

HOTBILD INDUSTRISPIONAGE

- Mellan konkurrenter i samma bransch och från andra nationer
- Industrispionage från rysk och östeuropeisk sida ökade efter Sovjetunionens fall
- Utländska underrättelsetjänster ofta drivande i industri-spionaget
- Det vistas under en normalperiod agenter från ca 20 nationer i Sverige

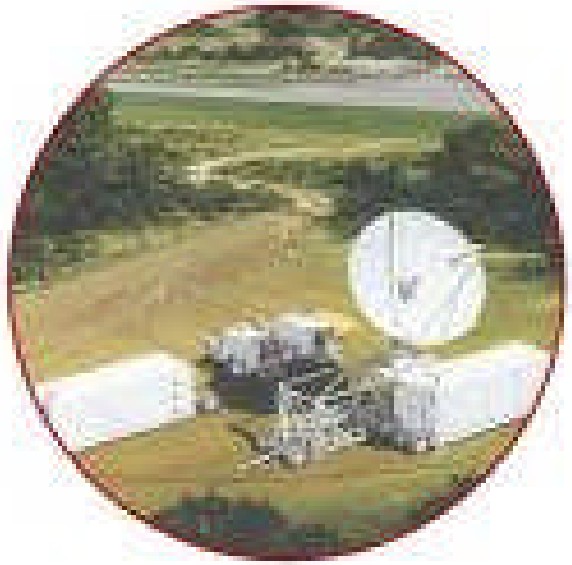
HOTBILD ANDRA NATIONER

- Industrispionage
- Informationsoperationer (IO)
- Psykologiska operationer (PSYOPS)

INFORMATIONSOPERATIONER(IO)

- VAD ÄR IO? -

- Informationsoperationer
- Informationskrigföring
- Information Warfare



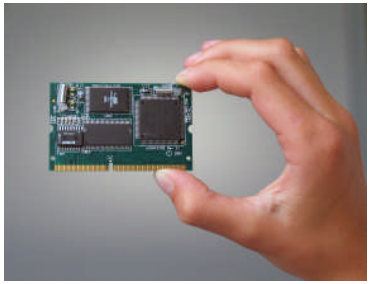
”In order to win victory we try our best to seal the eyes and ears of the enemy, making him blind and deaf, and to create confusion in the minds of the enemy commanders, driving them insane.”

Mao Tse Tung. On the protracted war (1938)

INFORMATIONSOPERATIONER(IO)

- VAD ÄR MÅLET MED IO? -

- Informationsöverläge
- Nationell styrka (ekonomisk styrka)
- Underrättelseinhämtning
- Opinionspåverkan
- Få insyn i, manipulera, förändra och förstöra motståndarens information och informationssystem



INFORMATIONSOPERATIONER(IO)

- DE TRE KLASSERNA? -

- Klass I – individnivå
- Klass II – företag, organisationer eller nationell nivå
- Klass III – militära eller globala hot

Industrispionage hamnar under klass II

DJURLING
SÄKERHETSINFORMATION

INFORMATIONSOPERATIONER(IO)

- DESS SJU BESTÅNDSDELAR -

- Command and Controll (C2) Warfare
- Intelligenced Based Warefare (IBW)
- Electronic Based Warfare (EBW)
- Psycological Warfare (Psy W)
- Hacker Warfare
- Economic Information Warfare
- Cyber Warfare

INFORMATIONSOPERATIONER(IO)

- CYBERSPIONAGE ÄR BILLIGT -

- Fler än 150 länder bedriver underrättelse- inhämtning på Internet
- Kraftig årlig ökning mot företag och myndigheter i västvärlden

DJURLING
SÄKERHETSINFORMATION

INFORMATIONSOPERATIONER

- Informationsoperationer omspänner i stort sett all verksamhet och alla system i samhället och därmed stora delar av rikets militära och civila ledning såväl i fred, kris, konflikt ock krig.

- Av synnerlig vikt är både civila och militära förberedelser i fredstid.

IO-DOKTRINER

Land	Grundsyn	Antal organisationer
USA	**Befälhavare kan använda IO när de ser ett behov därav**	14
Kina	**Kina avser att använda detta för att stärka sin ekonomiska position i världssamfundet**	Minst 2
Frankrike	**Har alltid hävdat att de använder alla medel för att stärka sin konkurrenskraft gentemot andra länder**	Minst 2

- Rysslands syn på informationsoperationer
- Indien (västerländska företagsetableringar i Indien)
- Nord Korea

INFORMATIONSOPERATIONER

- EXEMPEL TÄNKTA MÅL -

- Ledarskapet (politiskt, diplomatisk, civilt, militärt, socialt och kulturellt)
- Civil infrastruktur (telekommunikation, transporter, energi, finans, industri, forskning, media, skydd etc.)
- Militär infrastruktur (tele- och datakommunikation och underrättelseorganisationer etc.)
- Vapensystem (flygplan, fartyg, artilleri, luftförsvar)
- Grupper (ideologiska, etniska, kriminella och religiösa)
- Allmänheten (som kollektiv, opinionspåverkan samt på individnivå)

DJURLING
SÄKERHETSINFORMATION

INFORMATIONSOPERATIONER

- UTFÖRS DETTA I FREDSTID? -

Joint Doctrine for Information Operations 9 October 1998

Peace:
- Psychological operations
- Operations security and deception
- Other capabilities and related activities
- Information assurance

Crisis:
- Electronic warfare
- Physical attack and destruction

Conflict:
- All of the above but in greater scale

INFORMATIONSOPERATIONER
- UTFÖRS DETTA I FREDSTID? -

Statsstödd storskaligt industrispionage

- Storbritannien utsatt april 2005
- Kanada och Frankrike tidigare
- Tyskland, Israel och USA de senaste

- Allt som kan omsättas till pengar
- Allt som ger konkurrensfördelar
- Allt inom forskning och utveckling (miljöteknik)
- Allt som påverkar börserna
- Allt som påverkar växlingskurserna

Är du redo om dessa attacker riktas mot dig och din organisation?

INFORMATIONSOPERATIONER
- UTFÖRS DETTA I FREDSTID? -

Hotbilden mot dig

- Det är ur angriparens perspektiv intresset för informationen eller systemen räknas
- Ekonomiskt spionage, Konkurrensfördelar och F&U
- Allmänt destabiliserande åtgärder inom organisationen
- Förändra och manipulera informationen
- Allt som kan rubba förtroendet för samhället

INFORMATIONSOPERATIONER
- UTFÖRS DETTA I FREDSTID? -

Hotbilden mot din organisation

Kvalificerade aktörer som agerar mot Sverige och västvärlden nu:

- Kina
- Indien (vid företagsetableringar i Indien)
- Nordkorea
- Ryssland

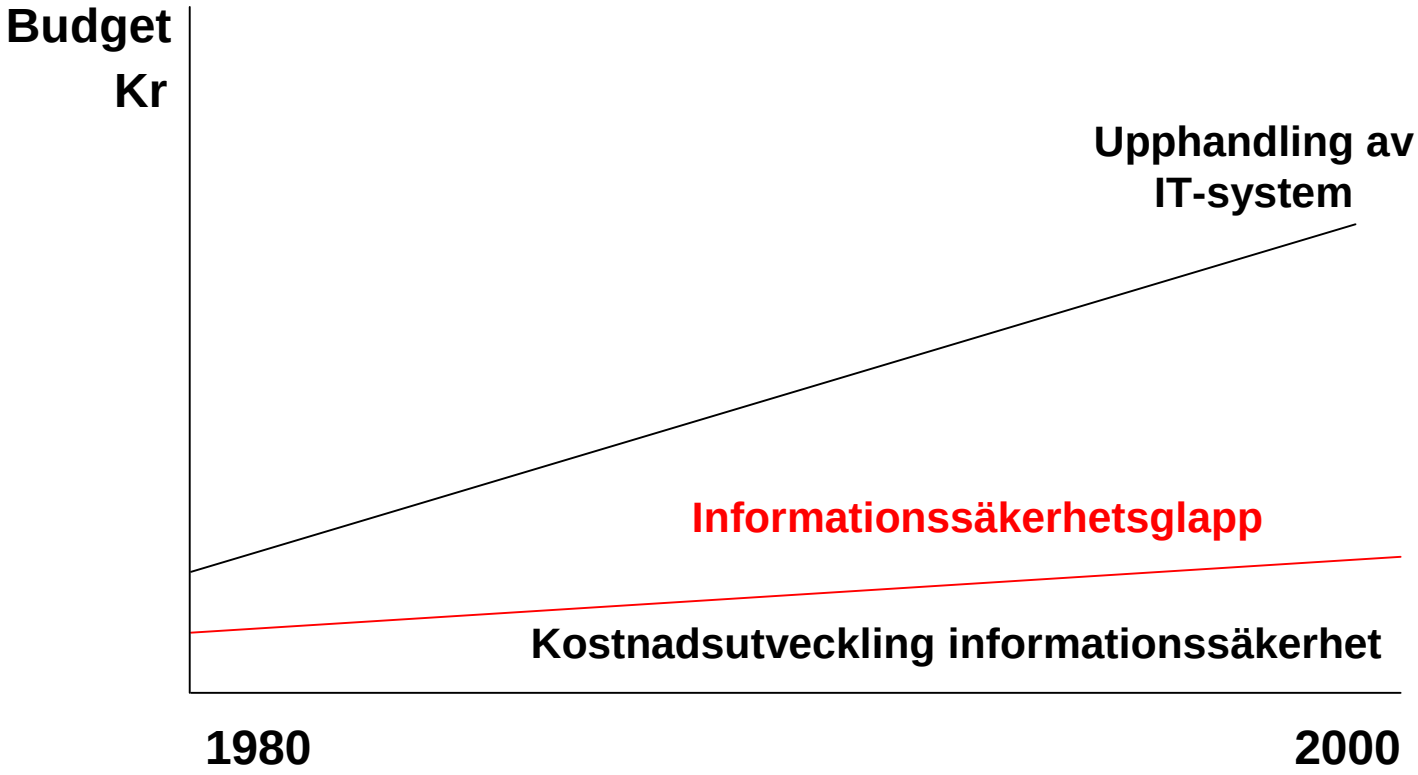
Den stulna kunskapen sprids i länderna till deras företag och organisationer.

Konkurrensen sätts ur spel
Acrobat reader, attackerna mot Sverige

BUDGETUTVECKLINGEN FM

- IT-SYSTEM OCH INFORMATIONSSÄKERHET? -

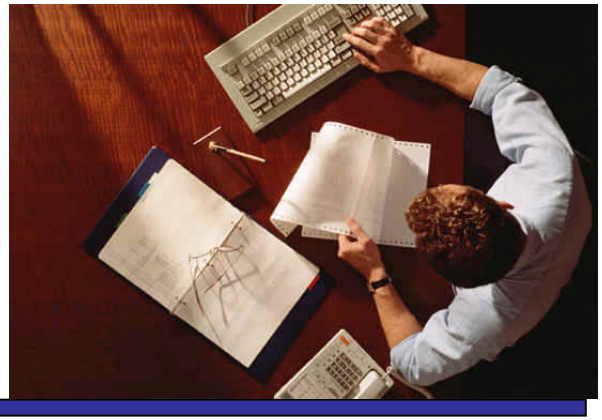
Är samhället sårbart?



DJURLING
SÄKERHETSINFORMATION

FINANSIELLA RISKER

- Likviditet
- Räntor
- Valutor
- Kreditvärdighet och förtroende
- Marknaden



DJURLING
SÄKERHETSINFORMATION

FINANSIELLA RISKER

☐ Likviditet

- Organiserad brottslighet
- Insiderproblem
- Lagar och föreskrifter
- Informationsoperationer
- Industrispionage
- Haktivism/Cyber-terrorism

☐ Räntor

- Informationsoperationer
  - Nationell (nivå 2)
  - Global nivå (nivå 3)

☐ Valutor

- Informationsoperationer
- Cyberterrorism

☐ Kreditvärdighet och förtroende

- Information operations
  - Desinformation
  - Economic operations

☐ Marknaden

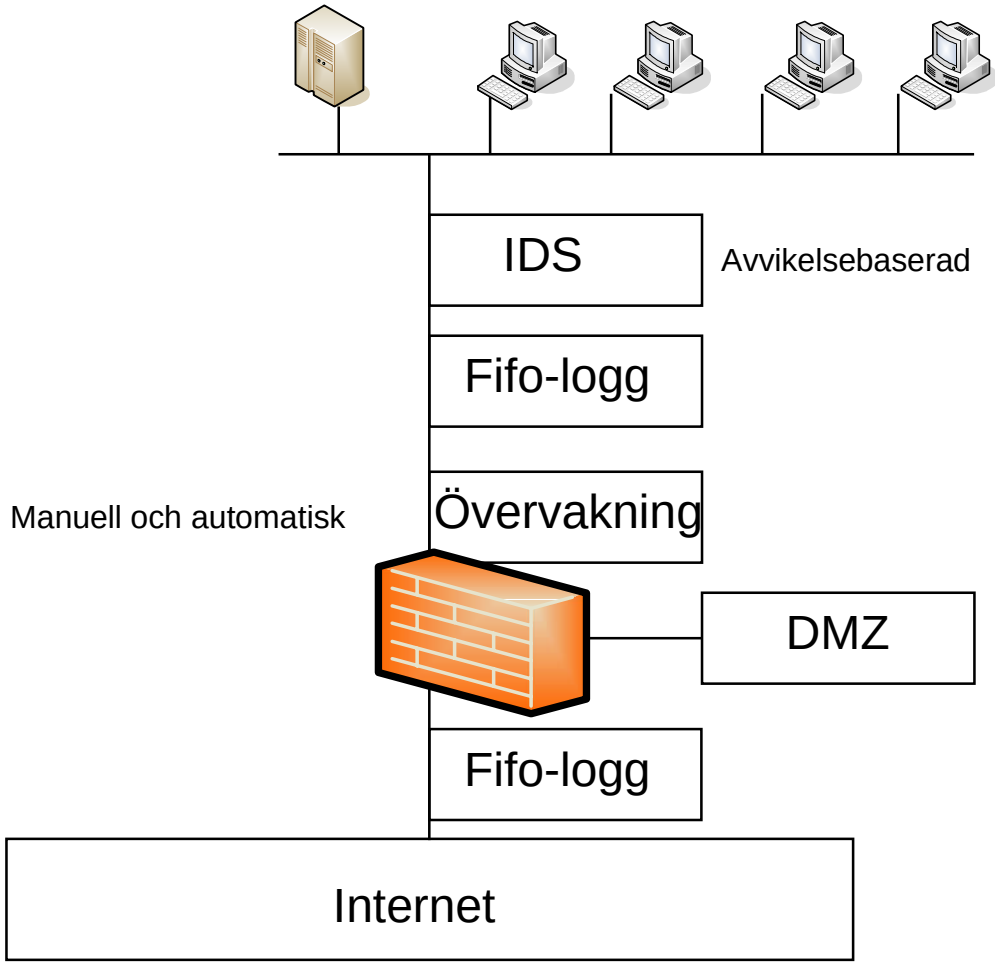
- Konkurenskraft
- Organiserad brottslighet
- Lagar och föreskrifter
- Informations operationer
- Hacktivism/Cyber-terrorism

FINANSIELLA HOT

- 85-95 % av alla affärsprocesser förlitar sig enbart på IT-system och integriteten i systemen och dess information. Att affärskritisk information inte blivit avsiktligt eller oavsiktligt förvanskad (Gartner Group survey).

- Vad skulle hända om du inte kan lita på din information, om du inte kan skilja på originaldata och förvanskad data?

HANTERA SITUATIONEN



IT-incidentfunktion

-upptäcka intrång

-begränsa skadan

-stoppa attacken

-undersöka

-analysera

-forensiska analyser

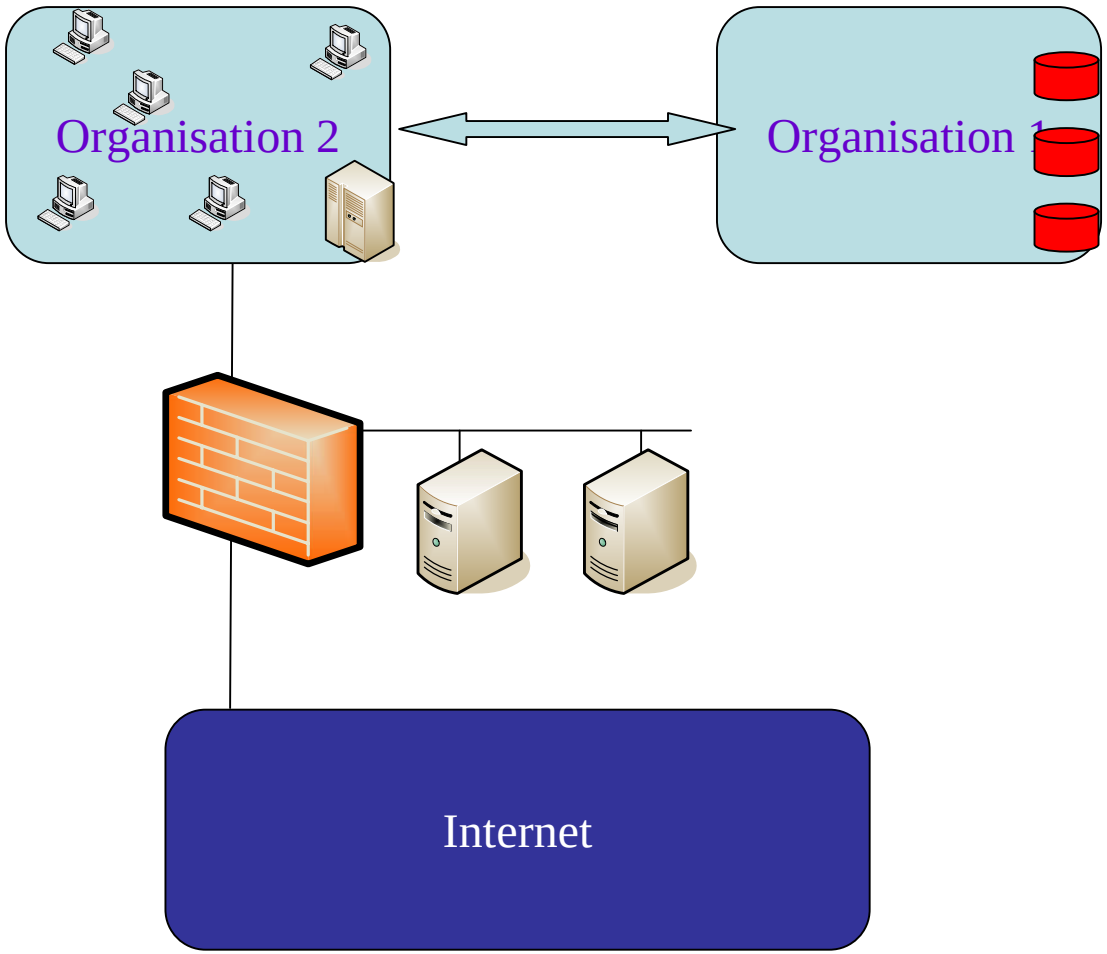
-återställa system

-återuppta verksamhet

-etc.

DJURLING
SÄKERHETSINFORMATION

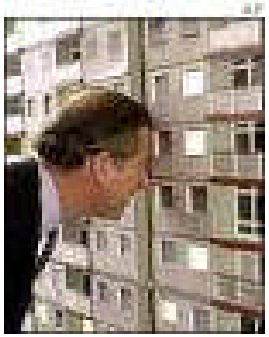
EXEMPEL FRÅN VERKLIGHETEN



DJURLING
SÄKERHETSINFORMATION

FRAMTIDA PROBLEMOMRÅDEN

- W-lan, bluetooth och R-fid etc.
- Social engineering (flera nya böcker i ämnet)
- Trådlösa tangentbord
- Klienter och Hem-Pc (browsers och surfning, Explorer, Firefox eller annan browser)
- Trojaner, maskar, virus målinriktade
- Vishing (nästa generations Phishing)
- IP-telefoni (PBX och IT-problematiken sammanslagen)
- Smarta hem, smarta bilar
- Den unga fildelargenerationen
- Nordic battlegroup, EUs snabbinsatsstyrka
- Google Apps, saas etc



DJURLING
SÄKERHETSINFORMATION

Klienter och Hem-pc

DJURLING
SÄKERHETSINFORMATION

KLIENTER OCH HEM-PC

- Varför ska jag skydda min Hem-Pc?
- Du är personligt ansvarig för vad som lagras i din dator
- Brottslingar lagrar olagligt material i andras datorer
- Dina bankaffärer över Internet (pin-koder, lösenord, dokument etc.)
- Din Hem-Pc kan vara vägen in på din arbetsplats
- Din dator kan användas i attacker mot andra

KLIENTER OCH HEM-PC

Start up your own phishing business for only US$30

Date: October 16, 2006

The marketplace for phishing toolkits, which can allow technophobe criminals to quickly and easily set up spoofed versions of banking Web sites, is booming, with kits changing hands for as little as US$30.

Although phishing kits are nothing new, over the past year their quantity and quality have increased dramatically, according to Dan Hubbard, who is vice president of security research for Websense and a representative of the Anti-Phishing Working Group.

"[Phishing kits] have been around for years but the volume is one of the big changes … the kits available are better designed," Hubbard told ZDNet Australia in a telephone interview last week.

KLIENTER OCH HEM-PC

- Ta hoten på allvar
- Bara brandväggar som skydd räcker inte
- Du måste upptäcka när dina skydd fallerar
- Du måste logga och övervaka manuellt och automatiskt
- Du måste ha en kompetent och samövad IT-incidentorganisation
- Du måste förbereda dig på att hoten blir verklighet
- När det händer går det mycket fort

HANTERA SITUATIONEN

- Organisation
- Säkerhetsarbetet (en del av affärsprocessen)
- IT-säkerhet och informationssäkerhet
- Skalskydd och tillträdesbegränsning
- Personal, chefer, konsulter och underleverantörer
- Glöm inte människan i säkerhetssammanhanget
- Säkerhet och skydd mot insiders börjar innan rekryteringen startar

HANTERA SITUATIONEN

Ledningens synliga och tydliga engagemang är en förutsättning

En god beställarkompetens är ett krav

Följ upp och kontrollera (ett beslut utan uppföljning är endast en from förhoppning om att beslutet ska följas)

IT-OSÄKERHET

Lite kul, eller?

- Flygsimulator i Microsoft Excel 97
- Flipperspel i Word 97
- Bilrallyspel i Access 2000
- AVG Antivirus
- Visual Basic, Visual C++, Visual J++
- Corel Draw, Photoshop, Photopaint, PowerPoint
- 12 st i Windows XP, 2 st i Vista och ca 30 i Mac OS 2 senaste

November 2007 11 068 eastereggs registrerade - se själv
www.eeggs.com

Tack för visat intresse!

Aktuella föredrag

- Hoten mot våra IT-system
- Social engineering Del 1
- Social engineering Del 2
- Angriparens väg till ditt lösenord
- Insiderproblematiken grund
- Rekrytering med fokus på säkerhet och kompetens
- Olika säkerhetslösningar (för och nackdelar)
- Varför säkerhet
- Vem har kunskapen att bli en IT-brottsling
- Säkerhetssamtal avslutad anställning
- Att införa kryptering i verksamheten
- Säkerhet i mobila enheter
- Beredningsperspektivet (ledning och beredning)
- Ledningsperspektivet (ledning och beredning)
- Vägen till en säkerhetsmedveten personal

Tjänster

- Säkerhetschef uthyres

- Strategisk rådgivning
- Sårbarhetsanalys
- Hotbildsanalys
- Tillträdesbegränsning
- Infiltrationsskydd
- Penetrationstester
- IT-teknisk rådgivning

Utbildning

Beställarkompetens
Rekrytering med fokus på säkerhet
Informationssäkerhet

Frågor?

DJURLING
SÄKERHETSINFORMATION

Tel: 08/760 08 80 Mobil: 070/715 73 32

www.djurling.se E:post: info@djurling.se