

You may live your life *dangerously*
Your IT systems **may not!**



Outpost24

Jimmy Kruuse



You may live your life *dangerously*
Your IT systems **may not!**



Du kanske lever ditt liv farligt,
Dina IT-system **borde inte!**

Hur mår Ni egentligen?



You may live your life *dangerously*
Your IT systems **may not!**



Proaktivitet istället för reaktivitet



You may live your life *dangerously*
Your IT systems **may not!**



Kontroll istället för brandsläckning



You may live your life *dangerously*
Your IT systems **may not!**



Vems ansvar i kommunen
vid en "lyckad" hackingattack?



You may live your life *dangerously*
Your IT systems **may not!**



Vem ansvarar för kostnaden för en
"lyckad" hackingattack?



You may live your life *dangerously*
Your IT systems **may not!**



Attacker och hackingförsök sker konstant, världen över... - Är Sverige förskonat?



**"Hackers attack computers every 39 seconds
for searching weak usernames and
passwords"**

According to a study done by University of
Maryland, hackers try to gain access to computers
every 39 seconds."

Källa: Outpost24.com, 2007-02-09



You may live your life *dangerously*
Your IT systems **may not!**



"Men vår kommun är inte så
intressant för hackers."

"Vi är inte gårdar som många andra kommuner. Vi har inte några stora aktörer förumärta.""



You may live your life *dangerously*
Your IT systems **may not!**



Vem är hackern?



- Studenten som automatiserat hackingen
- Industrispioner
- "Scriptkiddies"
- Politiska och/eller religiösa attentat
- "Web defacing"
- Hämndaktioner
- Ekonomisk brottslighet (t.ex. utpressning)
- Personliga fiender till anställda/politiker



You may live your life *dangerously*
Your IT systems **may not!**



Brandskydd



- Brandskyddsutrustning
- Brandlarm
- Automatiska larm
- Brandförsäkring

- Antalet bränder i verksamheten?
- Antalet falsklarm?

- Totala kostnaden?



You may live your life *dangerously*
Your IT systems **may not!**



Inbrottsskydd



- Inbrottsskydd (galler, säkerhetsdörrar m.m.)
- Inbrottslarm
- Automatiska larm
- Inbrottsförsäkring

- Antalet inbrott mot verksamheten?
- Antalet falsklarm?

- Totala kostnaden?



You may live your life *dangerously*
Your IT systems **may not!**



Informationsskydd

- Informationsskydd (brandväggar, koder, m.m.)
- Kontrollfunktioner?
- Automatiska larm?
- Informationsförsäkring?

- Antalet attacker mot verksamheten?
- Antalet falsklarm?

- Totala kostnaden?



You may live your life *dangerously*
Your IT systems **may not!**



UTGÅVA 3



You may live your life *dangerously*
Your IT systems **may not!**



Utdrag
från BITS

13. HANTERING AV INFORMATIONSSÄKERHETSINCIDENTER

13.1 Rapportering av säkerhetshändelser och svagheter

Mål: "Att säkerställa att informationssäkerhetsincidenter och svagheter hos informationssystem rapporteras på ett sådant sätt att korrigerande åtgärder kan vidtas i rätt tid."

BASNIVÅ

- Det ska finnas fastlagda rutiner för hur användare ska agera vid funktionsfel, misstanke om intrång eller vid andra störningar (Säkerhetsinstruktion, användare).



You may live your life
Your IT systems **may not!**



Utdrag
från BITS

benämning (socialförsäkringsregisterlag, patientjournallag etc.)

- Bokföringsförordningen

Tryckfrihetsförordningens krav på att allmän handling ska vara tillgänglig ska tillgodoses.

Tips!

Viss vägledning för tillämpning av offentlighets- och arkivlagstiftning ges i Statskontorets publikation "Offentlighet och IT 2002:1".

15.2 Efterlevnad av säkerhetspolicies, -standarder och teknisk efterlevnad

Mål: "Att säkerställa att system följer organisationens säkerhetspolicies och -standarder."

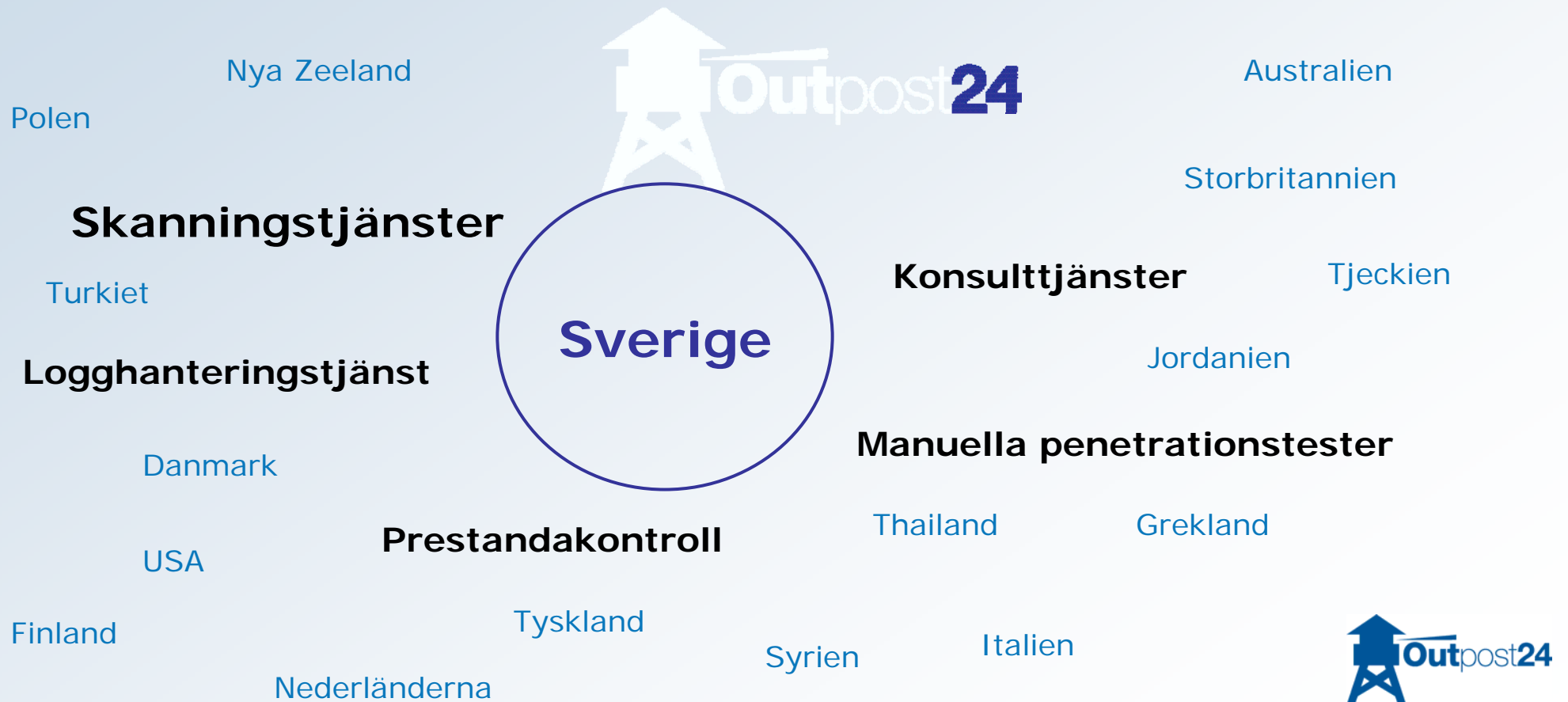
BASNIVÅ

- Interna och externa penetrationstester ska göras återkommande.
- Ledningspersoner ska regelbundet granska att säkerhetsrutiner, -policy och -normer efterlevs.
- Penetrationstester på externa kommunikationssystem (FW etc.) respektive på interna informationssystem ska göras återkommande.

■ 67



You may live your life *dangerously*
Your IT systems **may not!**



You may live your life *dangerously*
Your IT systems **may not!**



Outscan / HIAB

- **Skanningsverktyg** för alla era externa/interna IP-adresser
- **Vulnerability Management Solution** undersökande samtliga noder
- Unik **webbapplikationsskanner**
- **Compliance Monitoring** (ISO, BS, DS, BITS etc.)
- **Change Management System** med inbyggt alarmsystem (supporterar ITIL)
- **Statistik** uppbyggt av generell rapportgenerator
- Uppfyller **IT audit** krav (som dokumentation)
- **Lätt att implementera**



You may live your life *dangerously*
Your IT systems **may not!**



LogMon

- Loggövervakningsverktyg för alla era loggkällor
- Högpresterande skalbar Log Management Solution
- Grafisk presentation av pågående incidenter
- Larmfunktion
- Stark sökmotor med historisk spårbarhetssökning
- Förenkling av loggbackup
- Lätt att implementera



You may live your life *dangerously*
Your IT systems may not !



OUTSCAN Security Test Report

Sections

- >> Report info
- >> Executive summary - Security Risk Overview
- >> Executive summary - Security Threat Categories
- >> Executive summary - Security Threat Families
- >> Host list summary
- >> Threat list
- >> Executive summary - Security Top Port List
- >> Open port list
- >> Modification list
- >> Active disabled script list
- >> High risk threat details
- >> Medium risk threat details
- >> Low risk threat details
- >> Other risk threat details



You may live your life *dangerously*
Your IT systems **may not!**



OUTSCAN Security Test Report

Sections

- >> Report info
- >> Executive summary
- >> Executive summary
- >> Executive summary
- >> Host list summary
- >> Threat list
- >> Executive summary
- >> Open port list
- >> Modification list
- >> Active disabled
- >> High risk threats
- >> Medium risk threats
- >> Low risk threats
- >> Other risk threats

Report info

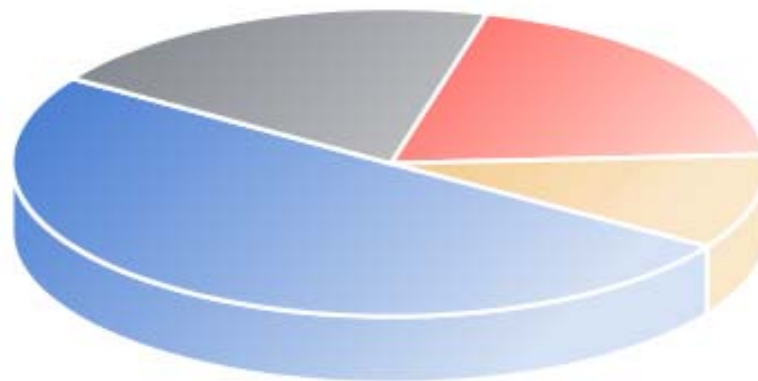
Report id:	A9CCECFE3DDB9545BE9AB21F2E0C7EF8
group:	None
Host:	192.168.200.15
Date:	Latest: 2005-06-14 10:55 - 2005-06-14 10:55
Number of tests:	1
Number of threats found:	10



You may live your life *dangerously*
Your IT systems **may not!**



Executive summary - Security Risk Overview



● High = 2 ● Medium = 1 ● Low = 5 ● Other = 2

[High Risk]

These types of threats should be addressed first and are typically easy to exploit. These security threats can compromise the integrity of your data, be used to take your system(s) off-line, or can be used for denial of service (DoS).

[Medium Risk]

Security threats, which can open your system(s) to unauthorized access or expose your data, are considered medium risk. Although usually (but not always) more complex to exploit, these types of threats are also very important to address.

[Low Risk]

This level of security threats is used for problems that typically cannot be used independently to gain unauthorized access to your data or compromise your system(s). However, these types of threats are commonly combined with other information to exploit your network.

[Other Risk]

This classification is used to provide informational data about your system(s). These types of security threats are typically not direct vulnerabilities, but they do expose additional information and data about your network.

OUTSCA

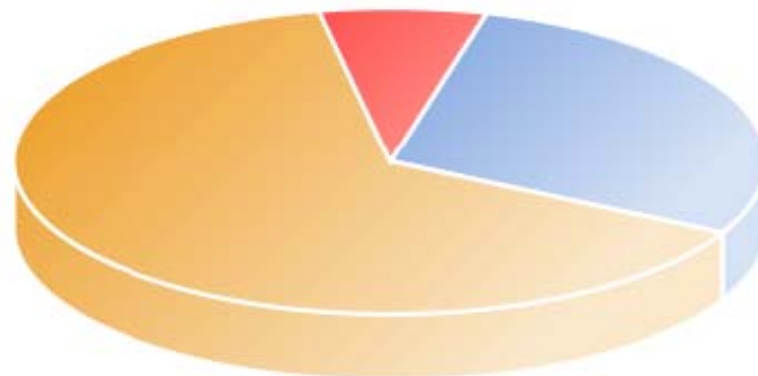
Sections

- >> Report info
- >> Executive sum
- >> Executive sum
- >> Executive sum
- >> Host list summ
- >> Threat list
- >> Executive sum
- >> Open port list
- >> Modification li
- >> Active disable
- >> High risk threa
- >> Medium risk th
- >> Low risk threa
- >> Other risk threa

You may live your life *dangerously*
Your IT systems **may not!**



Executive summary - Security Threat Categories



● Port = 4 ● Info = 9 ● Hole = 1

[Hole]

This part of the report is very important. It shows how many security holes Outscan has discovered. They are divided into 4 levels (low to high).

[Info]

This shows how many enumerations Outscan has found. Information leakage from your server, Usernames, Passwords, Software versions. This method uses four levels (low to high) listed below whilst scanning.

[Port]

This part of the report contains information on how many services have open ports on your computer that Outscan was able to find using different scanning methods like SYN / FIN / CONNECT() / UDP.

OUTSCAN

Sections

- >> Report info
- >> Executive sum
- >> Executive sum
- >> Executive sum
- >> Host list summ
- >> Threat list
- >> Executive sum
- >> Open port list
- >> Modification li
- >> Active disable
- >> High risk threa
- >> Medium risk th
- >> Low risk threa
- >> Other risk threa



You may live your life *dangerously*
Your IT systems **may not!**



OUTSCAN Security Test Report

Sections

- >> Report info
- >> Executive summary - Security Risk Overview
- >> Executive summary
- >> Executive summary
- >> Host list summary
- >> Threat list
- >> Executive summary
- >> Open port list
- >> Modification list
- >> Active disabled
- >> High risk threats
- >> Medium risk threats
- >> Low risk threats
- >> Other risk threats

Open port list

192.168.200.15	21 - ftp (21/tcp)
2005-06-14 10:55	80 - http (80/tcp)
	111 - sunrpc (111/tcp)
	826 - unknown (826/tcp)



You may live
Your IT s

OUTSCA

Sections

- >> Report info
- >> Executive sum
- >> Executive sum
- >> Executive sum
- >> Host list summ
- >> Threat list
- >> Executive sum
- >> Open port list
- >> Modification li
- >> Active disable
- >> High risk threa
- >> Medium risk th
- >> Low risk threa
- >> Other risk threa

High risk threat details

Script id: 10235

Name: statd service

Port: 823

Level: Info

Risk factor: High Risk: ■

Family: RPC

Description: The statd RPC service is running. This service has a long history of security holes, so you should really know what you are doing if you decide to let it run.

* NO SECURITY HOLE REGARDING THIS PROGRAM HAVE BEEN TESTED, SO THIS MIGHT BE A FALSE POSITIVE *

We suggest you to disable this service.

Risk factor : High

CVE: CVE-1999-0018 CVE-1999-0019 CVE-1999-0493

Bugtraq: 127 450 6831 11785

Task: 192.168.200.15 - 2005-06-14 10:55: Not assigned



You may live your life *dangerously*
Your IT systems **may not!**



Slutligen... Är allt detta så viktigt?

- Tja, det beror väl på...

- Bryr Ni er utifall varumärket skadas?
- Har Ni enbart data som Ni gärna vill dela med alla?
- Litar Ni mer än till 100% på alla anställda?
- Är Er verksamhet inte beroende av IT?
- Är Era system redan säkra nog?



You may live your life *dangerously*
Your IT systems **may not!**



Det är **ditt** val!
Kanske är det **ditt** ansvar?

