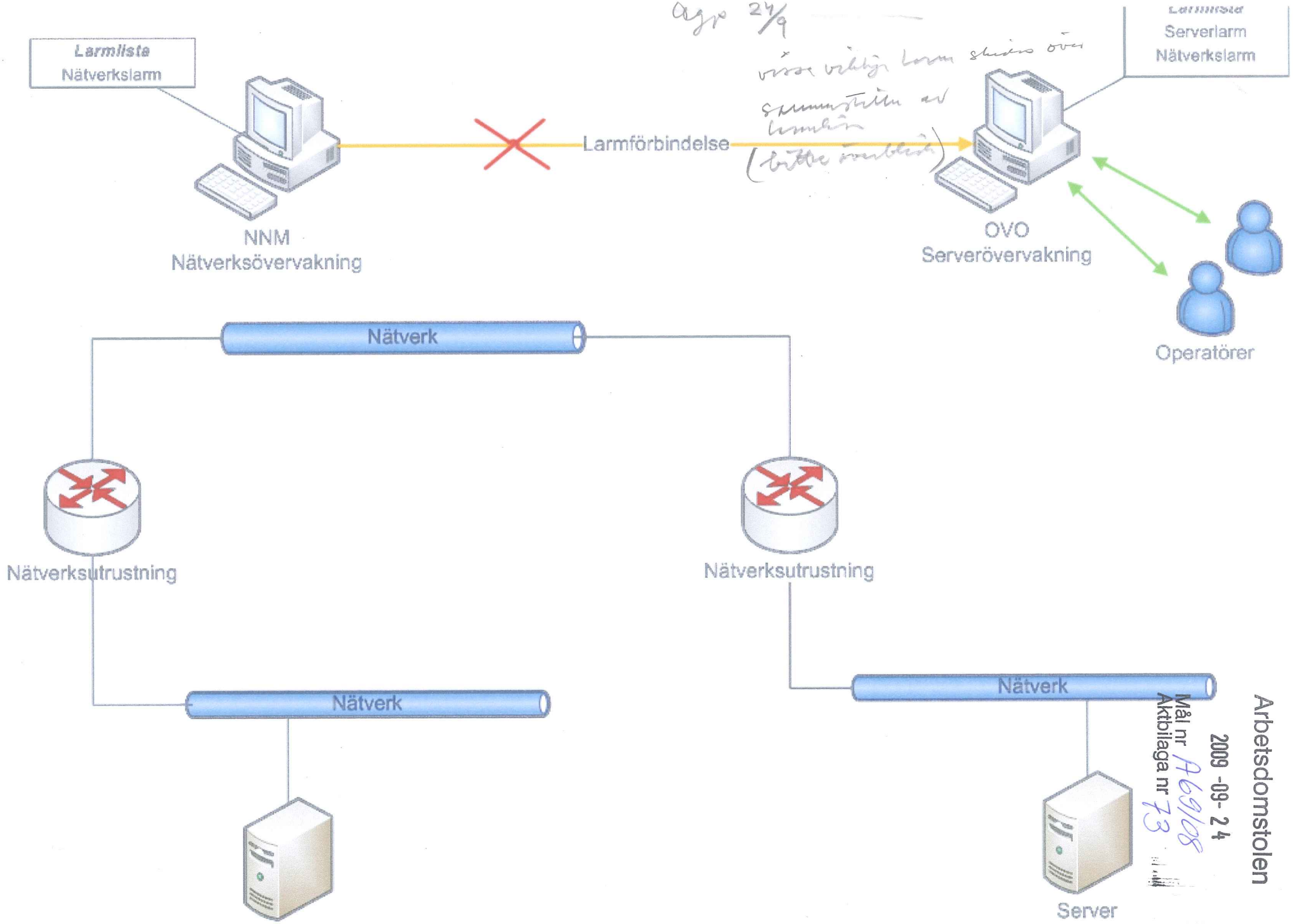
Agp 24/9

vissa vårdjr larm skickas över
sammanställn av larmen
(bättre överblick)



Arbetsdomstolen
2009 -09- 24
Mål nr A 69/08
Aktbilaga nr 73

Vittnesförhör

André Rickardsson

André Rickardsson

bitsec

- Operativ chef
  Bitsec AB
- Avdelningsdirektör
  Säkerhetspolisen SÄPO
- Departementssekreterare
  Regeringskansliet
- Departementssekreterare
  Utrikesdepartementet

2

$ %&' (') *'*'+, -*-'. , &'/ 0* 123 4, '*&, '56/ , ') , -57 89: ' '5, &*%; ; ; <=5: . "
>0, '29, ', ?', 5, %*%': 4) '5*/ / @%%29') : 5'ABC5'. 2%5-, ''8&'2D'E55, 1=5: . '*%50*'29'?8'BF"
7G'*H'+E99*'@?', %'56/ , ''IJK 2IG'?8'>0, '29, 5'*. +*55*&'2M: 5/ 0*'5*. -'?8'>NOP'&6' "
) *%9, % . 7G'&, '56/ , ') , -5/ : %': 1, ''?8'. E%&29) , -, ''. , &'5*.) 61502' Q9*'5E5-, . RO8"
>NOP'9, % . 7G'&, ') *%'&, 55@: . 'S, '-*1, -'IJ'+': H5@', &%2%9*''': 4) '&, 1-*92-'2'
. , -: &@0, 4/ 12%9'7G'@', &%2%9*''*0'IJK+': H'25*. *'+, -, '. , &'T2' 5/ '2 5'IJK+': H5': -, 1R'
B-+2&*''2*0*%4, '*&'IJK56/ , ') , -'?8'7G'50*'5) G95/ : 1*%R'

! " #$%&($&*$)+,-#&/ 0. $1+23 0. 1. ") &' 23 4&

'KU ', %52'5/ '*%* 1E5V+, 02556/ '2%9"
'KJ, / %25/ *'2%: '. *Q. %556/ , ') , -5*%* 1E5, '"
'KI%42&, %) *%, '2%9"
'KF*-*/ : . . @%2 *Q. %'
'K>6/ , ') , -51G5%2%9*'"'

Var det Bastian Baghfalekys arbetsstation som användes?

IDENTIFIERING AV ANVÄNDARE

Analys av Bastian Baghfalekys arbetsstation

I HP:s rapport anges ett antal tidpunkter där användaren Bastian Baghfalekys loggar in i servern eller startar det grafiska gränssnittet för nätverksövervakningen. Benämns NNM GUI i tabellen och i HP:s rapport.

Nr	Tidpunkt	Händelse
1	2007-05-15 09:18	Person x startar sudosh på servern U30230
2	2007-05-21 09:26	Person x startar sudosh på servern U30230
3	2007-05-22 09:06	Person x startar sudosh på servern U30230
4	2007-05-22 16:05	Person X startar NNM GUI
5	2007-05-22 16:12	Person X startar NNM GUI
6	2007-05-23 16:23	X hoppar ur VI och båda NNM GUI sessionerna stängs

Tabell 1

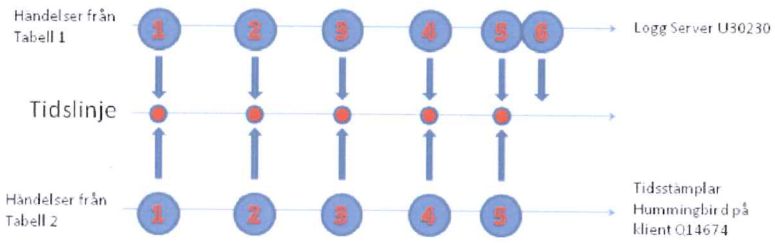
Analys av Bastian Baghfalekys arbetsstation

Kommunikationen mellan servern och arbetsstationen sker via programmet Hummingbird, som startas i arbetsstationen. Trots att det saknas loggning i programvaran Hummingbird och i arbetsstationen, så går det att genom en analys av tidsstämplar för filer som ingår eller används av programvaran Hummingbird, att se spår av vissa av de i loggen noterade händelserna.

Sekvens	Namn	Senast ändrad	Filtyp HP-version, PROFILE
1			Filtyp HP-version, PROFILE
			Filtyp startar nu det på servern
			U50030
2			Filtyp startar nu det på servern
			U50030
3			Filtyp startar nu det på servern
			U50030
*			Startar HBMC.EXE
2			Startar HBMC.EXE

Tabell 2

Analys av Bastian Baghfalekys arbetsstation



Genom att jämföra ändringar i tidsstämplar för filer på arbetsstationen Q14674 (Bastian Baghfalekys arbetsstation) och loggen i servern U30230 går det med stor visshet konstatera ett starkt samband.

Sambandet är så starkt att det inte går att hitta en annan förklaring än att det är Bastian Baghfalekys arbetsstation som använts för händelserna noterade i loggfilen enligt tabell 1.

Identifiering av användaren

- Det finns ett antal saker som talar för att det är Bastian Baghfaleky som genomfört de åtgärder som loggats i systemen
  - Bastians konto används för åtgärderna
  - Bastians arbetsstation används för åtgärderna
  - Filer flyttas till Bastians hemmakatalog
  - Arbetsstationen står på ett bevakat kontor
  - Stark kontroll av användarens identitet sker via Skatteverkets behörighets- och kontrollsystem
  - Det krävs ett personligt kort för att använda arbetsstationen
  - Inga spår av intrång i arbetsstationen funna

Misstag eller medveten handling?

FUNKTIONSBORTFALL

Notering 2 i HP-rapporten

- Tid 16:10 Datum 2007-05-22

16:10 X flyttar ett antal namngivna filer under /opt/OV/bin till /home/basbag/work1

```
u30230# rv Create_NodeDownFile.Switch.ovpl Check_NodeDownFile.ovpl.org.org
Create_Server_JnixFile.ovpl ovrequestd.org ovrequestd /home/basbag/work1

mv: ovrequestd: cannot unlink: Text file busy
```

"vektyrsäu" åtgärden

- Den viktiga delen är att följande fil flyttas

```
Check_NodeDownFile.ovpl.org.org
```

- Resultatet blir ett funktionsbortfall för nätverkslarm till operatörerna
  - Motsvarar att någon klipper av en larmkabel till en larmcentral

x enligt experterna Hlindberg o. Libäck

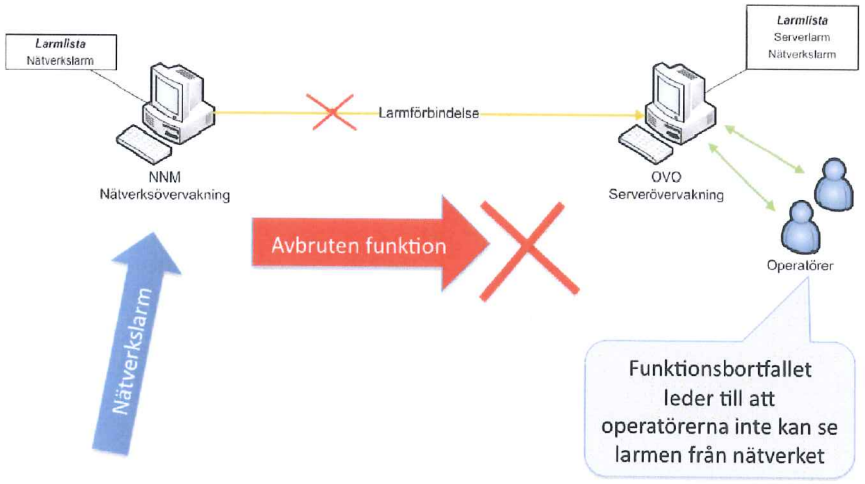
\ 6' '3 1, %]) , 4/ ^\ : &, F: _ %L2, R 0? IR '9R '9'SEH*5'. , &'/ : . . *%& -". 0'"". : 0, a'7 8%'
/ *-*1: 9, %'V. ?-VP b V+2%'QI1'Vj : . , V+*5+*9V_ : '/ ! "@ ?) G' "I*'. , %7G' "&, %%*'7@% Q. %'
*H'56%&*5'7 8%\ \ M'"%-G0, '0*/ %2%9a'QI1'P b P '">, '0, 'G0, '0*/ %2%9, %aRc : %5, / 0, %5, %'
0'"&, H'6' '*H': ?, '*-G', '%*'2%e, '/ : . . , ' '*H'5, '%6' 'G0, '0*/ *&'%-0, '/ 5@' @5-%2%9"
51@*' '7@%9, '*R'

Vj : . , V+*5+*9V6' 'D*5Q*%D*9) 7*1, / E5') , . . */ *-*1: 9"

AR = medvetna handling namngivna "chtrl", inget misstag

;"

Funktionsbortfall



Notering 4 i HP-rapporten

```
# Created using xnmevents by root on ti mar 06 16:45:49

EVENT OV_Router_Down .1.3.6.1.4.1.11.2.17.1.0.58916865 "Router alarms" Warning
FORMAT Node Down  $2 Capabilities: $8  Root Cause: $9 $10
EXEC /opt/OV/bin/Create_NodeDownFile.ovpl $3 $2
DISPLAY Router        $2      ner ||||
NODES r*
SDESC

EVENT OV_Router_Up .1.3.6.1.4.1.11.2.17.1.0.58916864 "Router alarms" Normal
FORMAT Node Up  Capabilities: $8  Root Cause: $9 $10
EXEC /opt/OV/bin/Check_NodeDownFile.ovpl crg.org $3 $2
NODES r*
SDESC
```

1

Tradp.conf efter 2007-05-22 $OV_CONF/C/trapd.conf

```
# Created using xnmtrap by root on Tue May 22 16:14:54

EVENT OV_Router_Down .1.3.6.1.4.1.11.2.17.1.0.58916865 "Router alarms" Warning
FORMAT Node Down  $2 Capabilities: $8  Root Cause: $9 $10
DISPLAY Router        $2      ner ||||
NODES r*
SDESC

EVENT OV_Router_Up .1.3.6.1.4.1.11.2.17.1.0.58916864 "Router alarms" Normal
FORMAT Node Up  Capabilities: $8  Root Cause: $9 $10
NODES r*
SDESC
```

2

3

Tidpunkt för förändringen 16:14:54

! R F, -'98' "-E&D9-'*H'5, '*H'Ae A] '" *&, '%*'3%%5'. , &'2'&, %Q&D*', '0, '52 %, %'7 8%'
#ddZKd<KdY'! YCX<CX; "

#R F, -'98' "-E&D9-'*H'5, '*H'Ae A] '" *&, '%*'2%e, '3%%5'. , &'20, '52 %, %5: . '5? *' *&, 5"
#ddZKd<K#'! YC XC<X"

WR J 2&? @% -'7G '%6' "&, %%*'/ : %3 9 @*Q. %5, %*5-'5? *' *&, 5"

Funktionsbortfall

- Skadan
  - Först flyttas filen enligt Notering 2
  - Tidpunkt för flytten av filen är 16:10
  - Redan nu har funktionsbortfallet inträffat
- "Upprensning"
  - Sedan ändras konfiguration i filen trapd.conf enligt Notering 4
  - Tidpunkt för ändringen är 16:14:54
  - Genom ändring av trapd.conf kommer nu heller inga larm i NMM som klagar på att filen enligt Notering 2 saknas

Loggfilen för 2007-05-22

```
-------
u302290# ls -la
total 38
drwxr-xr-x  5 orj.in    lok2000     1024 May 22 09:45 .
drwxr-xr-x 104 root      root        2048 May  2 16:02 ..
-rw-------  1 orj.in    lok2000       50 Jan 18 09:15 .Xauthority
-rw-r--r--  1 orj.in    lok2000      708 May 22 09:42 .bash_aliases
-rw-------  1 orj.in    lok2000     1607 May 22 09:43 .bash_history
-rw-r--r--  1 orj.in    lok2000     2766 Mar  2 12:54 .bashrc
drwx------  3 orj.in    lok2000       96 May 21 15:18 .mozilla
-rw-r-----  1 orj.in    lok2000       21 Jan  3 08:45 .news_time
-rw-rw-rw-  1 orj.in    lok2000        0 May 21 15:18 .owweb.conf
-rw-r--r--  1 orj.in    lok2000      713 May 22 09:46 .profile
-rw-------  1 orj.in    lok2000      326 May 22 09:42 .sh_history
drwx------  2 orj.in    lok2000       56 May 22 09:45 .ssh
drwxr-xr-x  5 root      sys           96 May 22 09:37 .sw
-rw-r--r--  1 orj.in    lok2000     6030 May 22 09:45 swlist_070522
u302290# mail .bash_history                bastian.baghfaleky@skatteverket.se <.bash_history
u302290#
```

16:24

Slut på loggfilen

Vid 16:24 den 22 maj 2007 tar loggfilen slut. Det betyder att det inte registreras flera kommandon på systemet för användaren Bastian Baghfaleky under resten av dagen.

Återspelning av loggfilen med sudosh-replay

Loggfilen för 2007-05-23

Återspelning av loggfilen med sudosh-replay

- Bastian Baghfaleky har inte
  - Flyttat
  - Kopierat
  - någon fil under denna dag som påverkat funktionen för larm i systemet
- Bastian aktiviteter under 2007-05-23
  - kontrollerar vilka kommandon orjlin utfört
  - Epostar .bash_history från orjlin till sig själv
  - Lär sig kommandot tail
  - Skapar filen /tmp/kalle

Misstag eller medveten handling?

- Borttagningen av filen 2
- Upprensning av filen trapd.conf 4
- Ovan talar för att:
  - åtgärden var avsiktlig
  - konsekvensen av åtgärden var klar
- Det finns mycket som talar för att handlingen var medveten
- Bastian såsom erfaren administratör borde vara fullständig medveten om konsekvensen av åtgärden
- Bastian har varken efter 16:10 den 22 maj eller under den 23 maj försökt att åtgärda funktionsbortfallet 2

Var åtgärderna efter Incidenten nödvändiga?

INCIDENTEN

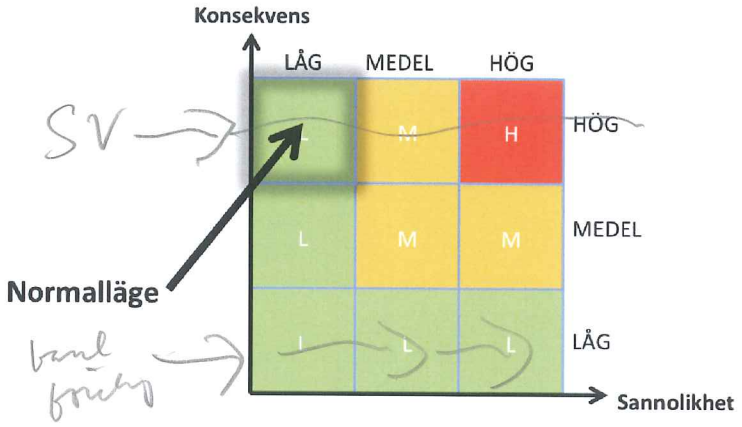
Normalläge

Driftsläge

Tidsaxel

Riskanalys

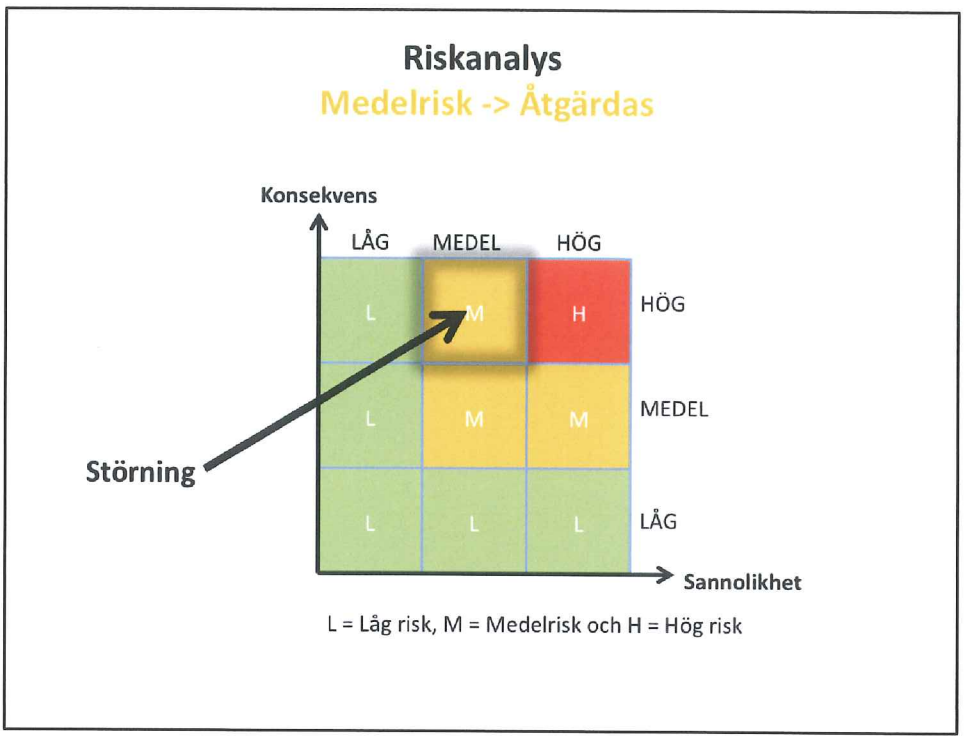
Låg risk -> Ingen åtgärd



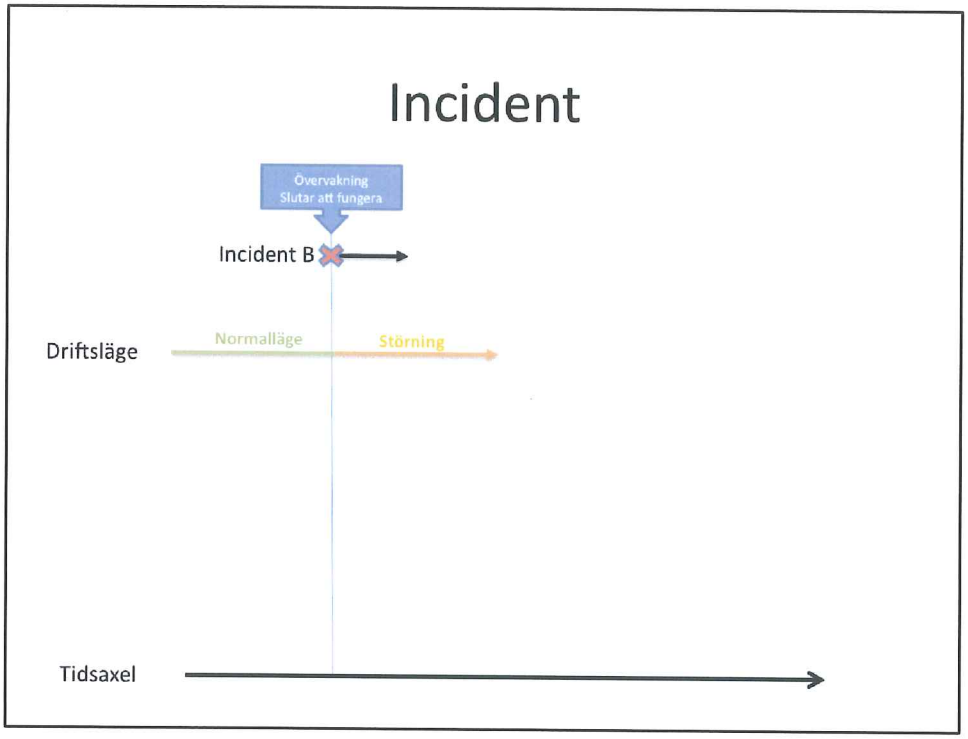
L = Låg risk, M = Medelrisk och H = Hög risk

Incidenten (start)

- 23 maj 2007 upptäcks att delar av Skatteverkets nätverksövervakning plötsligt har försvunnit
- Riskbedömningen är medelrisk och måste åtgärdas
- Felsökning och analys inleds



c: %5, / 0, %5'*0", %5-G %2%9'2C0, '0*/ %2%957@% Q: %, %6' '* 1Q&'*H'+, &G *'5: . ') G9R F, H*'? R9R*R*H'C0, '0*/ %2%9, %6' ", %'. E4/ , -'02/ Q9-'&, 1'256/ , ') , -, %7G '>/ *H, 0, '/ , -5" 5*.) 6 1150 2/ Q9*'5E5-, . R

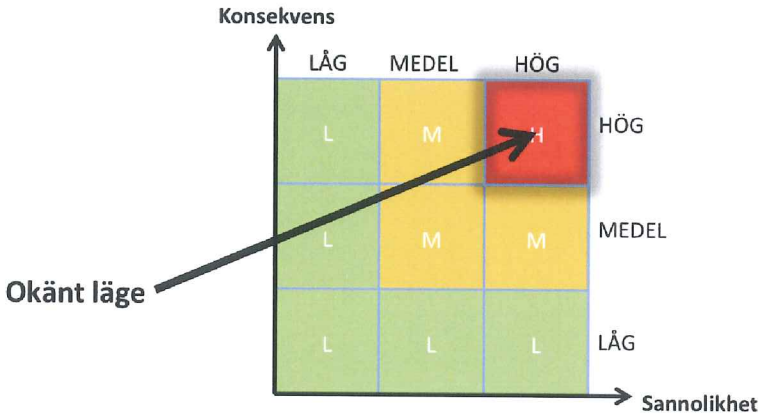

Incident
Övervakning
Slutar att fungera
Incident B
Driftsläge
Normalläge
Störning
Tidsaxel

Incidenten (eskalerar)

- 4 juni 2007, Bastian Baghfaleky medverkar inte till att lösa störningen
- Dokumentation av systemet är bristfällig eller saknas helt
- Riskbedömningen mht Bastian Baghfalekys inställning och tidigare agerande är "hög risk" och måste åtgärdas omedelbart
- Beslut att ominstallera övervakningen för att komma tillbaks till ett känt läge

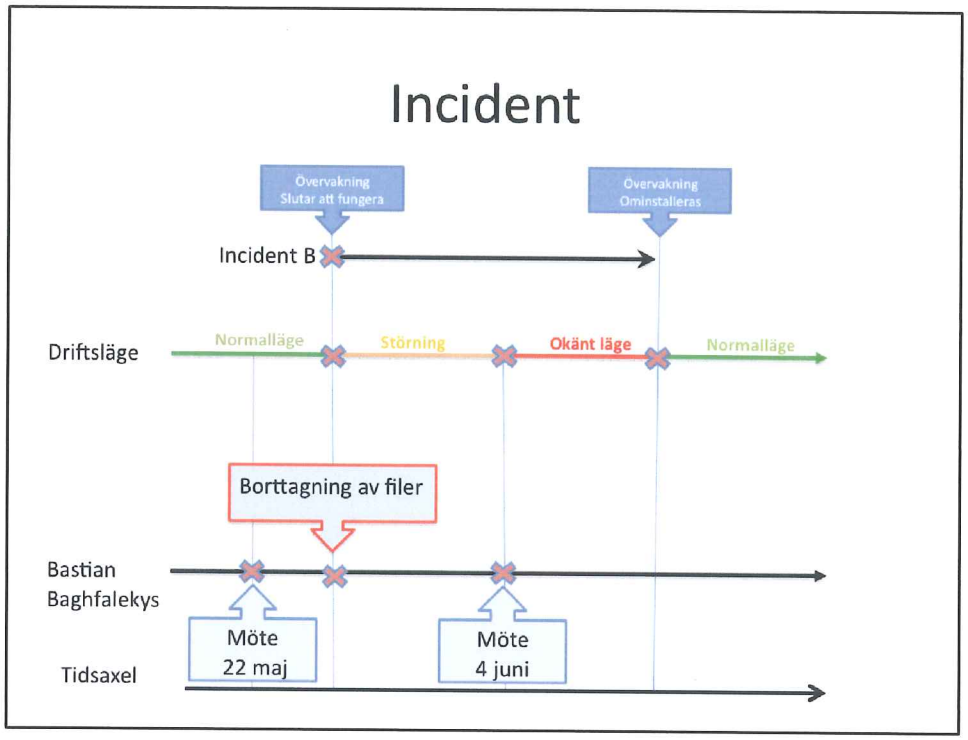
Riskanalys

Hög risk -> Åtgärdas omgående



L = Låg risk, M = Medelrisk och H = Hög risk

#W


Incident
Övervakning Slutar att fungera
Övervakning Ominstalleras
Incident B
Driftsläge
Normalläge
Störning
Okänt läge
Normalläge
Borttagning av filer
Bastian Baghfalekys
Möte 22 maj
Möte 4 juni
Tidsaxel

#X'

Incident

- De åtgärder som Skatteverket genomfört
  - Utreda
  - Analysera
  - Ominstallera övervakningen
- Samtliga åtgärder som genomförts är helt enligt de principer och policys som är normala för drift av samhällsviktiga system
- Min bedömning är att de åtgärder som Skatteverket genomfört var helt nödvändiga och ett minimum för att komma tillbaks till ett känt läge och normal drift

man kunde ha gjort än mer
(man visste sig ett fullständigt)

→ Övervakn. i samhällsvikt. system