Polismyndigheten
i Stockholms län

Bilaga B

Övriga externa rapporter

0201-K81864-12

Bilagan innehåller:

Åklagarmyndigheten
Internationella Åklagarkammaren Stockholm
Åklagare Henrik Olin
Hantverkargatan 25 A, plan 5
107 22 Stockholm

Stockholm den 22 februari 2013

Incidentbeskrivning

1. Organisation och verksamhet Applicate

Inledning
Bolaget Infodata Applicate AB som nyligen namnändrats till Bisnode Information AB (nedan "**Applicate**") ingår i Bisnodekoncernen, i vilken koncern även InfoTorg AB ingår. Bisnodekoncernen är en marknadsledande utgivare av digital affärsinformation med tjänster inom kredit-, marknads- och affärsinformation.

Nedan följer en beskrivning kring bolagens historia, organisation och den verksamhet som bedrevs vid tidpunkten för incidenten.

Bakgrund
Applicate har sitt ursprung i den statliga myndigheten DAFA som bildades 1970. 1986 blev DAFA ett statligt affärsdrivande bolag, och 1990 bildades Infodata AB som en del inom DAFA Data AB.

Under åren från 1993 och framåt förändrades ägarbilden flera gånger via bland andra Sema Group och amerikanska Schlumberger. År 2005 förvärvade Ratos aktiemajoriteten i Infodata AB och Bonniers Affärsinformation AB. Ratos slog ihop de båda bolagen till en ny koncern som fick namnet Bisnode. Som en följd av ambitionen att renodla verksamheterna inom Bisnode påbörjades 2006 arbetet med att dela upp Infodata AB i fem bolag, Infodata Applicate AB och InfoTorg AB är två av dessa. InfoTorg AB var tidigare således bara ett varumärke inom Infodata, men blev 2006 alltså ett eget produkt- och säljbolag.

Organisationsförändring
Efter incidenten i september 2012 påbörjades ett nytt förändringsarbete av organisationen inom Bisnodekoncernen. Syftet med omorganisationen är att samla kompetens och skapa ett mer enat Bisnode så att kunderna ska kunna ta del av den expertis som finns i hela koncernen. Den tidigare organisationen baserades på många självständiga enheter med egna varumärken och den nya organisationen innebär att man skapar en plattform där alla anställda ska ingå i en organisation och vara anställda i Bisnode. De tidigare enskilda bolagen samlas i tre tydliga affärsområden som bedrivs i Bisnode Information AB (tidigare Applicate), Bisnode Kredit AB och Bisnode Marknad AB samt i en gemensam affärsstödjande enhet i moderbolaget Bisnode Sverige AB. Applicate har som ett led i den organisatoriska förändringen den 17 december 2012 namnändrats till Bisnode Information AB. I samband med namnändringen delades Applicates verksamhet upp i två delar, varav IT-förvaltningsdelarna flyttades till den för koncernen gemensamma affärsstödjande enheten Bisnode IT, en avdelning inom moderbolaget Bisnode Sverige AB. Den huvudsakliga verksamheten dvs.

utvecklingen av applikationer, finns kvar i bolaget Applicate (som namnändrats till Bisnode Information AB).

I samband med uppdelningen av verksamheten och namnändringen av Applicate till Bisnode Information AB har även en fusion inletts av koncernbolagen InfoTorg AB och Infodata AB som innebär att dessa bolag fusioneras upp i Bisnode Information AB. Fusionen förväntas vara verkställd under våren 2013. En skiss som utvisar den relevanta koncernstrukturen vid tidpunkten för incidenten och hur den förändrats därefter bifogas.

Verksamheter och tjänster vid tidpunkten för incidenten

Applicate

Applicates verksamhet består av att utveckla s.k. applikationer. En applikation är datorprogram som är avsett för en viss tillämpning i praktiskt arbete av en användare t.ex. ett ordbehandlingsprogram eller ett program som gör det möjligt att koppla upp sig på webben och använda funktioner på en hemsida, till skillnad från systemprogram såsom t.ex. operativsystem som är avsedda för datorns inre arbete och som utgör den plattform som krävs för att applikationerna ska kunna användas t.ex. på en dator eller smartphone. Applicate är bl.a. specialiserat på att utveckla applikationer med hjälp av vilka användare kan söka och få fram information från olika offentliga register och databaser, t.ex. bolagsregistret och fastighetsregistret. Applikationerna som utvecklats kan närmast beskrivas som verktyg genom vilka användare av applikationerna får tillgång till informationen i registren och databaserna i sökbar och strukturerad form. Applicate utvecklar kontinuerligt applikationerna så att användarna kan ta fram och ladda ned relevant information från olika register och databaser så att de uppfyller användarens behov. Applicate utvecklar bl.a. applikationerna som används för InfoTorgs tjänster.

InfoTorg AB

InfoTorg AB (nedan "**InfoTorg**") är ett tjänsteföretag som tillhandahåller besluts- och affärsinformation till sina kunder som utgörs av företag, organisationer och myndigheter. Den information som InfoTorgs kunder får tillgång till via InfoTorg utgör med några få undantag (se t.ex. nedan beträffande SPAR) offentlig och publik information från officiella register och databaser.

För att över huvud taget kunna använda InfoTorgs informationstjänster krävs att man ingått ett kundavtal med InfoTorg. Varje kund tilldelas ett eller flera användarkonton som ger kunden tillgång till de av InfoTorgs informationstjänster som kunden har träffat avtal om ska ingå i tjänsterna. Ett användarkonto ger således användaren endast tillgång till de tjänster som omfattas av kundavtalet och inte till alla InfoTorgs tjänster generellt. Ett användarkonto består av ett registrerat användarnamn och ett lösenord för användarnamnet.

Kunderna kan med användarkontot få tillgång till InfoTorgs informationstjänster online via webben eller integrerat i kundernas egna system. InfoTorg tillhandahåller också registervårdstjänster som uppdaterar kundernas kundregister med aktuell information och bevakar de förändringar som berör kundernas register. Det vanligaste sättet att nå InfoTorgs tjänster är via webben. Via InfoTorgs hemsida på webben kan kunden logga in med sina tilldelade användarkonton. När användarnamnet och lösenordet verifierats kan användaren söka och ladda ned information från de register och databaser som kunden har valt.

De informationssökningar som kundens användare har utfört loggas och InfoTorg fakturerar sina kunder i enlighet med dessa loggar som ligger till grund för kundfakturorna som kan specificeras på

användarnivå. Dessa loggar kan även användas för att t.ex. efterforska vilka sökningar som en kunds användare utfört.

SPAR

InfoTorg är bl a auktoriserad återförsäljare av SPAR-information från koncernbolaget Infodata AB. Infodata AB har sedan många år ett avtal med staten såsom servicebyrå och personuppgiftsbiträde att ombesörja drift, produktion, underhåll och marknadsföring m m av SPAR. Infodata AB anlitar för detta uppdrag Applicate som underbiträde, som i sin tur har outsourcat drift och förvaltning till Logica. Huvudmannaskapet för SPAR har Skatteverket såsom personuppgiftsansvarig.

I SPAR-lagen regleras i detalj vilka uppgifter som får finnas i SPAR och vilka uppgifter som får lämnas ut till olika företag och organisationer. I SPAR finns det fyra olika behörighetskategorier som beskriver vilken typ av information som en viss typ av kund/användare äger rätt att erhålla ur registret. Vilken av dessa behörigheter ett företag eller myndighet har framgår av myndighetsbeslut som Skatteverket SPAR fattat. Härutöver finns det en särskild behörighet som avser utlämning av personuppgifter för personer med sekretessmarkering och denna behörighet kan endast ges till en myndighet efter det att särskilt tillstånd meddelats enligt med 22 kap. 1 § offentlighets- och sekretesslagen (2009:400).
När en kund till InfoTorg önskar få tillgång till SPAR ombesörjer InfoTorg såsom kundombud en ansökan för kundens räkning till Skatteverket SPAR. I ansökan fylls uppgift i om kunden önskar utökad behörighet enligt någon av ovanstående angivna behörighetskategorier. Skatteverket gör sedan en prövning om kunden ska erhålla åtkomst till SPAR. Av beslutet framgår om kunden får tillstånd och vilken behörighetskategori som kunden omfattas av. Skatteverket delger kunden och kundombudet InfoTorg sitt beslut. Därefter ger InfoTorg kunden åtkomst till SPAR enligt de uppgifter som framgår av Skatteverkets beslut.

Outsourcing IT-drift Logica

Applicate har outsourcat IT-driften för de applikationer som Applicate utvecklat till Logica. Även för de applikationer som InfoTorg och andra delar utav Bisnode utvecklat handhar Logica IT-driften för. I Logicas diftsåtagande ingår t.ex. även lagring av användarkonton och system för verifiering av användarkonton vid inloggning.

2. Kronologisk beskrivning incidenten

Onsdagen den 7 mars 2012

En anställd hos Applicate som bland annat har som arbetsuppgift att ta fram faktureringsunderlag till InfoTorg baserat på datafiler som utvisar InfoTorgs kunders nyttjande av InfoTorgs informationstjänster fick strax efter klockan 7 på morgonen upp ett varningsmeddelande på sin datorskärm som varnar för det sker ovanliga aktiviteter i stordatormiljön bestående i att ett av InfoTorgs användarkonton (användarkonto beskrivs under punkten 1) försöker få tillgång till ett mycket stort antal av de datafiler som den anställde administrerar och som användarkontot inte är behörigt att få del av.

Vid halvåttatiden på morgonen kontaktar den anställde enligt Applicates incidentrutin Applicates säkerhetschef och berättar att användarkontot obehörigen försöker komma åt ca 10 000 av de datafiler som den anställde administrerar.

Säkerhetschefen fattar misstanke om att det med stor sannolikhet föreligger en säkerhetsincident och att någon försöker använda användarkontot på ett oegentligt sätt.

Säkerhetschefen kontaktar därför omgående Applicates driftschef och rapporterar vad man upptäckt. Driftchefen kontaktar nu i enlighet med Applicates incidentrutin Applicates VD för att avrapportera vad man upptäckt. Applicate bildar ett incidentteam som bl.a. består av Applicates VD, driftschef och säkerhetschef. Teamet börjar arbeta dygnet runt med att hantera incidenten.

Det visar sig att användarkontot tillhör en av InfoTorgs säljare och användarkontot spärras. Man kontaktar säljaren som bedyrar att inloggningsuppgifterna för användarkontot har hanterats på ett korrekt sätt och inte lämnats ut till någon annan samt att hon själv inte använt kontot på det sätt som framgår av loggarna i datasystemet.

Driftchefen kontaktar Logica och man bokar ett möte under förmiddagen nästa dag.

Torsdagen den 8 mars 2012

Vid halv tiotiden på morgonen har Applicates incidentteam det bokade mötet med Logicas kundansvarige för Applicate och Logicas säkerhetschef. Vid mötet avrapporterar Applicate mer i detalj vad man upptäckt och man anmäler in en säkerhetsincident till Logica.

Fredagen den 9 mars 2012

Under dagen framkommer det att flera användarkonton används på ett märkligt och oegentligt sätt. Genom att spåra IP-adresser kan man börja spåra varifrån man loggat in på användarkontona. (En IP-adress är ett protokoll som reglerar datatrafiken på internet. Varje internetanslutning tilldelas ett IP-nummer som motsvarar telefonnumret i telenätet. Man spårar således upp från vilken internetanslutning användare av användarkonton loggat in på användarkontot.) Det framkommer då att inloggningar skett från en mängd olika internetanslutningar på en mängd olika platser och länder i världen, bl.a. från Kambodja, varifrån InfoTorgs kunder normalt inte kopplar upp sig. Rent fysiskt kan en användare av ett användarkonto omöjligen logga in från så många olika internetanslutningar i olika länder på så kort tid, vilket ytterligare befäster Applicates uppfattning att någon eller några olovligen bereder sig tillgång till InfoTorgs kunders användarkonton.

Applicates VD kontaktar Logicas VD för att tydliggöra att det enligt Applicates uppfattning föreligger en pågående säkerhetsincident hos Logica.

Logica tilldelar Applicate en person som hjälper Applicate att spärra misstänkta IP-adresser från vilka någon eller några försöker logga in på användarkonton som används oegentligt.

Lördagen och söndagen den 10 och 11 mars 2012

Applicates incidentteam undersöker kontinuerligt loggar och misstänkta IP-adresser och man spärrar misstänkta IP-adresser och användarkonton som man misstänker används på ett oegentligt sätt.

Måndagen den 12 mars till tisdagen den 20 mars 2012

Dagliga avstämningsmöten avhålls mellan Applicate och Logica. Applicates incidentteam fortsätter att kontinuerligt undersöka loggar och misstänkta IP-adresser samt att spärra misstänkta IP-adresser och oegentligt brukade användarkonton. Man upptäcker att antalet användarkonton som används på ett oegentligt sätt hela tiden ökar. På måndagen den 19 mars 2012 bestämmer sig därför Applicates incidentteam att informera polisen om incidenten och Applicates incidentteam kontaktar polisen.

Onsdagen den 21 mars 2012

Vid 8.20 tiden på morgonen informerar Logica Applicate om att det förelegat olovliga/misstänkta inloggningar inte bara i den del av Logicas stordatorsystem som exklusivt används av Logica för

tillhandahållande av tjänster till Applicate och InfoTorg, kallat SYS19, utan även i en annan del av Logicas stordatorsystem som Applicate/InfoTorg delar med andra benämnt SYS3. Vidare informerar Logica om att man upptäckt att någon obehörig fått tag på en superanvändaridentitet, en s.k. NUS, som ger användaren i det närmaste obegränsat tillträde till hela SYS3 och SYS19. Vid halvtretiden på eftermiddagen kan Applicates incidentteam sluta sig till att filer med känslig information tillhörande skatteverket har hämtats ut. Logica informerar nu Applicate om att intrånget ökat i omfattning samt att man informerat skatteverkets och kronofogdens säkerhetschefer. Klockan 16:38 på eftermiddagen gör den obehörige NUS-användaren ett misslyckat påloggningsförsök och vid åtta tiden på kvällen identifieras intrångsförsök från nya IP-adresser.

Fredagen den 23 mars 2012

Fr.o.m. detta datum drivs arbetet med incidenthanteringen från Rikspolisen och Verksamhetsskydd. Logica, IBM, Applicate/InfoTorg och KPMG arbetar från denna stund tillsammans med inblandade myndigheter och förser dem med loggar. Man arbetar utifrån en åtgärdslista och Logica. Applicate/InfoTorg påbörjar att vidta åtgärder i infrastrukturen för att förhindra liknade incidenter och intrång i framtiden. I april 2012 avtar intrångsförsöken.

3. Skada och kostnader

Krävande arbetsinsatser

Utredningen av orsaken, åtgärderna och efterarbetet har varit krävande och kostsamma för bolagen inom Bisnodekoncernen. Flera anställda inom Bisnodekoncernen har lagt ned mycket tid och arbete på övertid för att arbeta med frågor som rör incidenthanteringen. I denna kostnadsbeskrivning har hänsyn inte tagits till de indirekta kostnaderna i form av resurser som annars skulle ha använts på sedvanligt sätt i den löpande verksamheten.

InfoTorg har fått informera och skriva incidentrapporter till alla de kunder som har drabbats av intrånget i form av "kapade" användaridentiteter.

Lösenordsförändringen har också inneburit en omfattande kommunikationsinsats mot samtliga kunder.

Personalresurser och externa konsulter

Hos Applicate har externa konsulter anlitats för ett sammantaget belopp om ca 2 000 000 kr för arbete med incidenten.

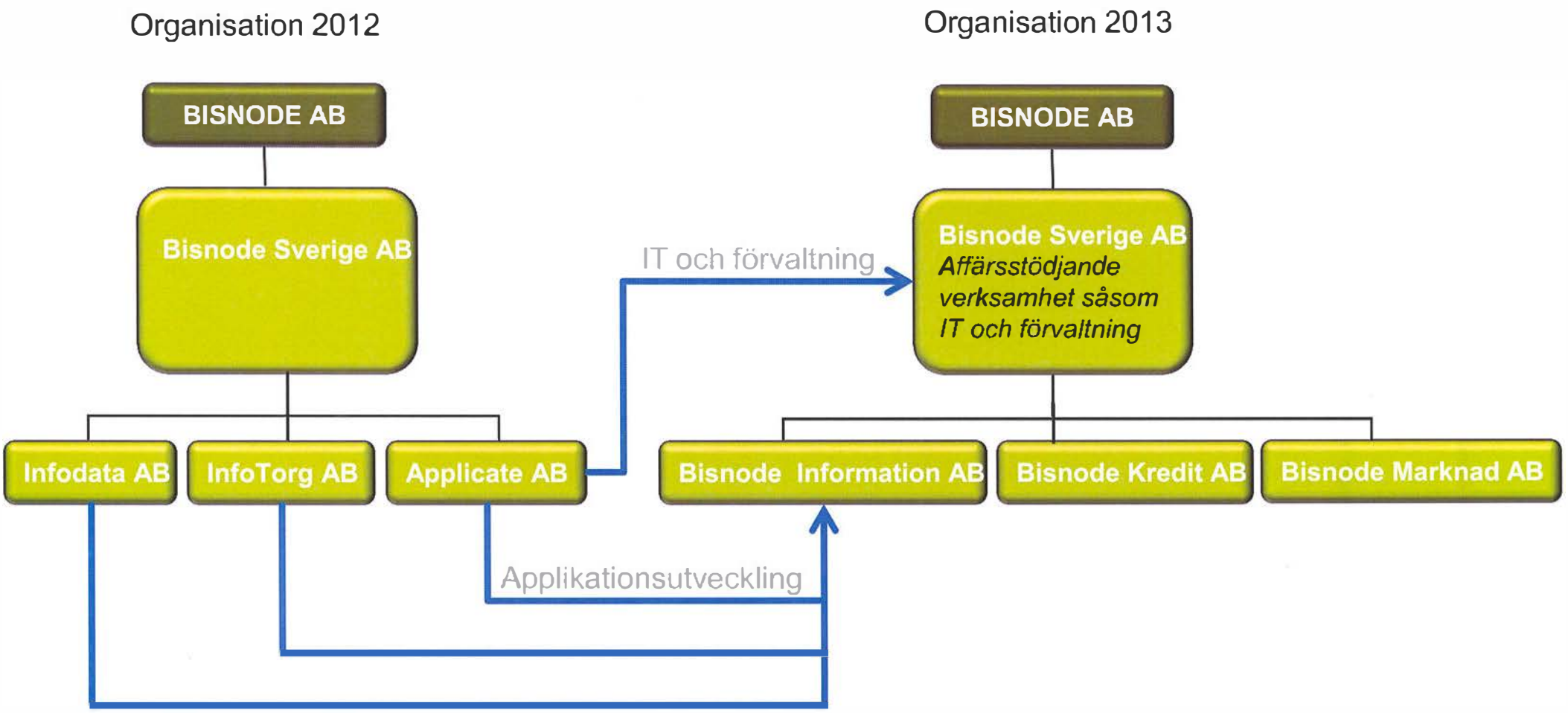
InfoTorg har som en följd av incidenten efter inrådan från KPMG och skatteverket som ett led i det åtgärdsprogram som togs fram i anledning av incidenten ändrat rutinerna för lösenordshanteringen för InfoTorgs tjänster på så sätt att det krävs mer komplexa lösenord för användarkontona. För genomförandet av lösenordsförändringen inom en mycket snäv tidsram har förstärkning av personalresurser krävts i form av att hyra in extra externa konsulter, men även i forma av övertidsarbete för befintlig personal. Sammantaget har InfoTorg haft en kostnad för detta som uppgår till ca 2 200 000 kr.

Utöver dessa nämnda kostnader har personer på ledande befattningar inom koncernen lagt ner tid motsvarande ca 440 000 kr. Nyckelpersoner inom Bisnode har också varit tvungna att lägga ned arbetstid på att kontrollera loggning, följa upp kreditupplysningsutredningar och göra felsökningar m m. Kostnaderna för detta uppskattas till ca 275 000 kr.

Sammanfattningsvis uppgår Bisnodekoncernens skada och kostnader i anledning av incidenten till ca 4 915 000 kr.

Denna incidentrapport har tagits fram av Applicates incidentteam under ledning av Applicates driftschef.

Översikt Bisnodes svenska organisation



DELNING

Anders Kylesten
010-574 85 42

Datum
2012-10-18

Dnr

Skatteverkets beskrivning av konsekvenser

Skatteverket överlämnar bilagda konsekvensbedömning till Åklagarmyndigheten för underhandssynpunkter.

Anders Kylesten
Säkerhetschef

Marie Berg
010-574 87 57

PROMEMORIA

Datum
2012-10-18

Skatteverkets beskrivning av konsekvenserna med anledning av dataintrånget

1 BAKGRUND

Skatteverket har av åklagaren fått i uppdrag att lämna en beskrivning av Navet (Skatteverkets system för distribution av folkbokföringsuppgifter till samhället) i allmänna ordalag samt att lämna en beskrivning av vilka konsekvenser som uppkom för verket.

2 ALLMÄN BESKRIVNING AV NAVET

Navets funktioner regleras av lagen (2001:182) och förordningen (2001:589) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet. Navet uppdateras kontinuerligt under dagen allteftersom ärenden registreras i folkbokföringen.

Navet innehåller uppgifter om samtliga personer som är folkbokförda eller av annan anledning tilldelats ett personnummer eller samordningsnummer.

Följande tjänster finns i Navet:
- Ändringsavisering
- Urval
- Slumpmässigt urval
- Ändringsavisering/urval mot infil
- Web Services – ePersondata

Med ändringsavisering avses löpande avisering av uppgifter som ändrats på personer i folkbokföringen. Mottagaren erhåller de uppgifter på de personer som mottagaren själv har rätt att behandliga enligt personuppgiftslagen. Det går att välja antingen daglig eller veckovis ändringsavisering.

Med Web Services - ePersondata avses överföring av personposter till myndigheterna för direktuppdatering. För åtkomst till uppgifterna krävs certifikat.

För övriga tjänster hänvisas till bifogad bilaga Allmän beskrivning av Navet

Uppgifterna lämnas i form av kodade datafiler. Navet tillhandahåller inte program eller system för behandling av datafilerna.

"Skyddade personuppgifter" är en samlingsrubrik som Skatteverket använder för de olika skyddsåtgärderna sekretessmarkering, kvarskrivning och fingerade personuppgifter.

Marie Berg
010-574 87 57

PROMEMORIA

Datum
2012-10-18

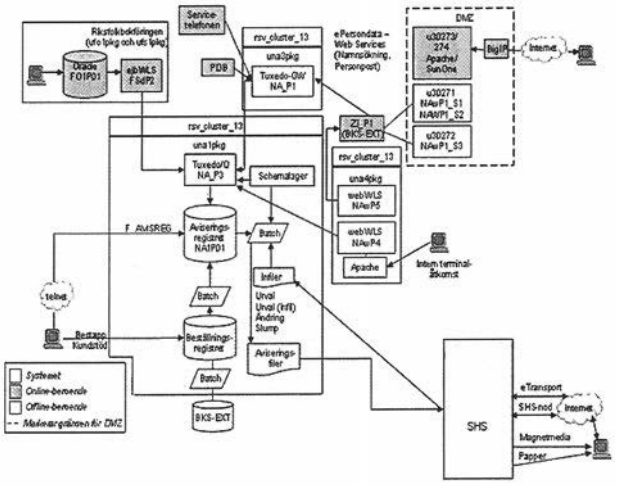
Varje myndighet är ansvarig för sina egna personregister. Det innebär att det är myndigheten själv som bestämmer vad som ska presenteras för användarna. Det finns således ingen övergripande policy för hur myndigheterna ska behandla skyddade personuppgifter. Frågan om skyddade personuppgifter kan lämnas ut prövas av respektive myndighet med stöd av lagen om offentlighet och sekretess.

I Navet finns möjlighet att beställa färre uppgifter för sekretessmarkerade personer eller att helt avstå från dessa uppgifter.

Se mer information om Navet i bifogad bilaga.

Nedan beskrivs översiktlig hur Navet fungerar.

Översiktsbild Navet



Skatteverket

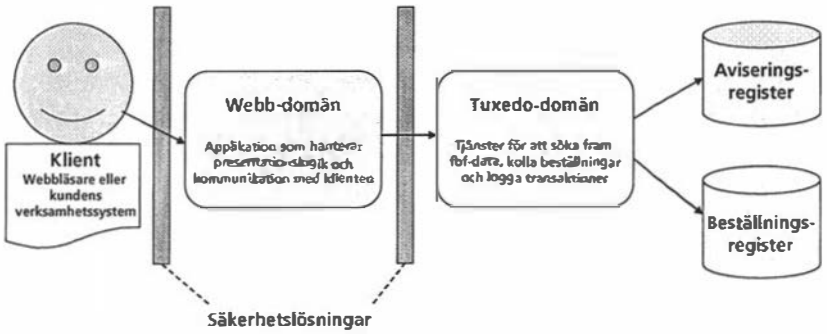
Marie Berg
010-574 87 57

PROMEMORIA

Datum
2012-10-18

3 KORT BESKRIVNING AV GRUNDARKITETKTUREN FÖR NAVETS ONLINETJÄNSTER

Grundarkitektur för Navets Onlinetjänster



Skatteverket

Vid kommunikation via Internet får den nyckel/certifikat som behövs för att koppla upp sig mot Navet inte placeras på en enskild tjänstemans dator utan på en server till vilken en begränsad mängd personer har tillgång.

4 KONSEKVENSER HOS SKATTEVERKET MED ANLEDNING AV DATAINTRÅNGET

Skatteverket har lagt ner mest tid och kraft med att ta hand om konsekvenserna perioden 27 mars – 13 april 2012.

Den redovisade tidsåtgången för denna period uppgår till 13 522 timmar. Till denna tidsåtgång har tid lagts ner för incidenthantering inom driften.

Skatteverket har idag inte kunnat uppskatta om denna incident har påverkat vårat förtroende i någon större omfattning. Vi har valt att inte särskilt undersöka detta.

Den 20 mars 2012 fick Skatteverket SKV) information om dataintrånget hos Logica. Med hänsyn till omfattningen av Kronofogdens dataförlust, i samband

Marie Berg
010-574 87 57

PROMEMORIA

Datum
2012-10-18

med dataintrånget, och uppgiften om att 10 000 personnummer avseende personer med skyddade personuppgifter låg ute på nätet, gjorde vi bedömningen att det fanns en teoretisk risk att namn och kontaktuppgifter kunde kopplas till dessa personnummer.

Vi kom fram till att av de 10 000 personer vars personnummer låg ute på nätet så var det inledningsvis 3 800 som var berörda.

Den 26 mars började SKV skissa på olika scenarier för att ta ställning till vad som behövde göras för att ta om hand oroliga medborgare med skyddade personuppgifter och de som teoretiskt möjligt kunde vara berörda av intrånget. För att kunna hantera inkomna samtal på ett enhetligt sätt och för att leda den operativa verksamheten på kontoren tog SKV fram ett förslag på ett KontaktCenter, bemannat med skyddshandläggare från regionerna.

Den 27 – 29 mars jobbbar SKV vidare med att skapa ett KontaktCenter. Två telefonnummer beställdes, ett för generella fråga från oroliga medborgare och ett som skulle användas i brevet som skulle skickas ut till berörda.

Vi jobbade även vidare med att ta reda på hur många som kunde tänkas vara berörda. Den summa vi nu utgick ifrån vad 2 200 personer (gäldenärer med aktuella skyddade personuppgifter)

Den 29 mars var KontaktCentret bemannat med 7 skyddshandläggare från regionerna samt personal från SKVs huvudkontor.

142 personer hade då hört av sig till SKV med anledning av dataintrånget.

I slutet av mars skickar vi ut brev till sammanlagt 2 200 personer (gäldenärer hos KFM) där vi bedömt att en teoretisk möjlighet finns att identifiera namn och kontaktuppgifter.

I början av april får vi information om att det finns en teoretisk risk att uppgifter om skyddade personuppgifter kan har kommit ut via aviseringsfiler från Navet till KFM. Med anledning av detta beslutar vi oss för att kontakta ytterligare 665 personer.

Vår ambition var att samtliga där en teoretisk risk fanns för röjda personuppgifter skulle ha kontakts innan påskhelgen.

PROMEMORIA

Marie Berg
010-574 87 57

Datum
2012-10-18

Den 3- 11 april fortsätter arbete i Kontaktcentret och vi beslutar att montera ner Kontaktcenter fr o m den 12 april. Det i brevet angivna numret hanterades av skyddshandläggare på region.

Teoretiskt berörda personer med skyddade personuppgifter är uppskattade till 2 865 st (2 200 gäldenärer med skyddade uppgifter och 665 st i tre aviseringsfiler till KFM)

SKV har sedan 12 april 2012 återgått till normalläge vad gäller hanteringen av skyddade personuppgifter.

Frågor kring incidenten har hanterats i linjen på regionerna eller av huvudkontoret.

Verksamhetsansvarig chef har löpande fått information från förundersökningen som kan vara aktuell för bedömning om någon ytterligare person kan vara berörd av det polisanmälda intrånget. Inom ramen för ordinarie linjearbete har kontakt tagits med ev. ytterligare berörda personer. Vidare har prövning skett om kontakt ska tas i de fall ytterligare personer har dykt upp i utredningen. Denna prövning har skett av personal på huvudkontoret.

Fram till den 28 maj 2012 har 2 168 berörda personer varit i kontakt med Skatteverket på det särskilda telefonnumret som upprättades i samband med att Kontaktcentret öppnades.

Händelsen innebär att vi följer alla uttag av personuppgifter från Navet extra noga. Alla uttag av uppgifter som avviker från normala rutiner kontrolleras en extra gång för att säkerställa att det är behöriga uttag av information och särskilt om det rör en större mängd uppgifter rörande personer med skyddade personuppgifter.

Bilaga
Allmän information om Navet

Skatteverket

Navet

AVISERING AV FOLKBOKFÖRINGSUPPGIFTER

ALLMÄN BESKRIVNING

Ändrat i denna version:

Kapitel 8 Beskrivning av innehållet i Navet; lagt till 'Folkbokföringstyp ' i - *historik*

Bilaga 2 Hantering av infil; ändrat felaktig referens

NAVET

Innehållsförteckning

Skatteverket
Postadress 171 94 SOLNA
Telefon 010-574 80 60
Telefax 08-29 37 44
www.skatteverket.se
E-postadress navet.solna@skatteverket.se

Bilagor

1 Koder för typer av ärenden
2 Hantering av infil
3 Hantering av filer då färre uppgifter beställts för sekretessmarkerade personer
4 Filsammansättning avseende olika ändringsdagar
5 Arbetsgång vid användning av Internet
6 Exempel på personavi
7 Exempel på aviseringslista
8 Exempel på personlista
9 Exempel på adressetiketter
10 Allmänna villkor

Skatteverket
Postadress 171 94 SOLNA
Telefon 010-574 80 50
Telefax 08-28 37 44
www.skatteverket.se
E-postadress navet.solna@skatteverket.se

NAVET

1 Inledning

Alla myndigheter i samhället har rätt att, mot avgift, erhålla uppgifter från folkbokföringen genom Navet (Skatteverkets system för distribution av folkbokföringsuppgifter till samhället). Navets funktioner regleras av lagen (2001:182) och förordningen (2001:589)om behandling av person-uppgifter i Skatteverkets folkbokföringsverksamhet.

All dokumentation om Navet finns på Skatteverkets hemsida, www.skatteverket.se – Företag & organisationer - För myndigheter & kommuner - Navet.

Kontakta Navet för kundstöd på navet.solna@skatteverket.se

2 Folkbokföring och spridning av uppgifterna

Folkbokföringen är den grundläggande registreringen av befolkningen i Sverige. I folkbokföringen registreras uppgifter om identitet, bosättning och familjeförhållanden.

Skatteverket ansvarar för folkbokföringen. Verksamheten bedrivs vid skattekontor spridda över landet där registrering sker i folkbokförings-databasen.

Personbevis och andra registerutdrag lämnas av skattekontoren.

Maskinell spridning av uppgifterna sker med hjälp av Navet. Navet uppdateras kontinuerligt under dagen allteftersom ärenden registreras i folkbokföringen.

Uppgifterna lämnas i form av kodade datafiler. Filformat och andra specifikationer finns i "Avisering av folkbokföringsuppgifter - Teknisk beskrivning". Navet tillhandahåller inte program eller system för behandling av datafilerna.

3 Tjänster

Följande tjänster finns i Navet.

- Ändringsavisering
- Urval
- Slumpmässigt urval
- Ändringsavisering/urval mot infil
- Web Services - ePersondata

3.1 Ändringsavisering

Med ändringsavisering avses löpande avisering av uppgifter som ändrats på personer i folkbokföringen.

Mottagaren erhåller de uppgifter på de personer som mottagaren själv har rätt att behandla enligt personuppgiftslagen. Personerna avgränsas exempelvis geografiskt (län, kommun, församling) eller åldersmässigt, se närmare under avsnitt 4, Sökbegrepp.

Tjänsten inleds i regel med att ett grunduttag görs och att ändringsaviseringen påbörjas veckan därefter.

Det sker en ändringsavisering när ändring gjorts av någon av de uppgifter som kunden har beställt, exempelvis namn eller civilstånd. Det går alltså inte att välja att aviseras endast om vissa händelser, exempelvis inflyttningar.

Det går att välja antingen daglig eller veckovis ändringsavisering. Vid veckovis ändringsavisering kommer varje veckodag för sig i ett eget skikt.

Leveranser till mottagarna sker tisdag – lördag, alltså dagen efter normal kontorsarbetsdag. De ärenden som eventuellt registrerats under lördag och söndag aviseras på tisdag tillsammans med de ärenden

som registrerats på måndag. Då helgdag infaller mitt i veckan sker ingen avisering dagen efteråt. Om avvikelse planeras från dessa rutiner informeras kunderna om detta genom särskilt meddelande.

Mottagaren kan välja att aviseras hela personposten (totalpost) oavsett vilka uppgifter för en person som förändrats eller att få endast de uppgifter som förändrats (ändringspost). Vid totalpost går det inte att avläsa i aviseringsfilen vilka uppgifter på personen som har förändrats. Man kan dock välja, såväl vid totalpost som vid ändringspost, att posten innehåller en kod för de typer av ärenden som föranlett förändringen t ex flyttning, vigsel eller förvärv av svenskt medborgarskap (se bilaga 1).

Det är även möjligt att beställa löpnumrering av aviseringsfilerna. Löpnummer underlättar att hålla ordning på att inte någon fil "tappas bort" och att filerna behandlas i rätt ordning. Löpnumret återfinns i Info.nav-filen (etikettfilen), vilket innebär att den måste låsas först för att få informationen. Löpnumret ska även sättas på etiketten utanpå eventuellt magnetmedium. För mottagare med e-transport/SHS skickas information om löpnumret i Navets fil navet_<löpnummer>.inf.

Förutom löpnumrering kan även "brytposter" beställas. Då framgår, vid veckovis ändringsavisering, var i filen den ena dagen slutar och den andra börjar (startpost). För att ytterligare underlätta, kompletteras startposten med det datum posten blivit upplagd i Navet.

Format och utseende för löpnummer och brytposter framgår av den tekniska beskrivningen.

3.2 Urval

Urval kan vara engångsuttag eller med viss periodicitet t.ex. en gång per år.

Möjliga sökbegrepp anges under avsitt 4, Sökbegrepp.

Vid urval erhålls samtliga de personer som motsvarar angivna sökbegrepp. Undantag från detta är slumpmässigt urval, se nästa punkt.

Det är alltid den aktuella status på uppgifterna vid uttagstillfället som redovisas. Det går alltså inte att söka ut personer som bott i ett område viss tid. Inte heller personer som flyttat ut från eller in till ett område under viss tid.

Resultatet av urvalet framgår först när uttaget har gjorts ur Navet. Det går därmed inte att på förhand upplysa om hur många personer som uttaget kommer att resultera i. Det innebär också att man på förhand inte kan ge besked om hur många personer som är folkbokförda inom ett visst område. Sådan information lämnas dock av Statistiska centralbyrån (SCB).

Vid uttag av urval på mediaformatet Adressetiketter kan man göra valet att få texten 'Till målsmanför' för personer under 18 år. Denna text skrivs på raden ovanför namnet.

3.3 Slumpmässigt urval

En slumpmässig beställning kan vara ett enkelt urval där ett visst antal personer ska slumpas fram för ett visst kretsområde och vissa sökbegrepp. En beställning kan också vara mer komplex där ett visst antal individer ska tas fram slumpmässigt för varje undergrupp av t.ex. kön, åldersgrupp, kretsområde. För varje beställning från en kund genererar de olika undergrupperna (delbeställningarna) automatiskt en datafil med personnummer som underlag för att ta fram de begärda uppgifterna.

Exempel på beställningar:

Exempel 1 - Enkel beställning
1000 slumpmässigt utvalda kvinnor boende i Luleå kommun.
(1 undergrupp -> 1 delbeställning + 1 datafilsbeställning)

Exempel 2- Komplex beställning
Kretsområde: Luleå kommun.
50 män resp 50 kvinnor önskas slumpmässigt ur varje åldersgrupp: 20-29, 30-39, 40-49, 50-59, 60-69, 70-79
(12 undergrupper -> 12 delbeställningar + 1 datafilsbeställning)

Slumpmässigt urval har en egen prissättning. En fast avgift tas ut för varje delbeställning (200 kr). Även det slutliga urvalet med hjälp av datafilen har ett eget fast pris (5000 kr) + det normala rörliga priset vid urval.

Beställningsblanketten är ännu inte anpassad för slumpmässigt urval. Vid beställning bör kontakt tas med Skatteverket.

3.4 Ändringsavisering/urval mot infil

I stället för att ange en personkrets med hjälp av olika sökbegrepp kan mottagaren själv ange personkretsen med hjälp av en frågefil (infil), såväl vid regelbunden ändringsavisering som vid urval. Personnumren anges i indatafilen enligt visst format och skickas in på ADB-medium eller via linjeöverföring till Navet. En närmare beskrivning av förfarandet finns i bilaga 2.

3.5 Web Services - ePersondata

Tjänsten är en kombination av de två funktionerna

- Överföring av personposter till myndigheterna för direktuppdatering.

- Namnsökning

Vid överföring av personposter levereras de i samma format som vid vanlig avisering. Ett personnummer (alternativt samordningsnummer eller tilldelat personnummer av annan anledning än folkbokföring) anges varvid mottagaren har personposten i sin egen applikation inom några sekunder. De uppgifter som på

detta sätt får hämtas in är de uppgifter som mottagaren själv har rätt att behandla i sitt register.

Alla myndigheter har dock rätt att, även om de inte får behandla uppgifterna i sitt register, ta del av uppgift om personnummer (även samordningsnummer och tilldelat personnummer av annan anledning än folkbokföring visas), namn, adress, folkbokföring och avregistrering.

Vid Namnsökning kan personnumret sökas fram med hjälp av olika parametrar. Förnamn, mellannamn, efternamn, födelsetid, kön, postnummerområde eller några av dem i kombination används som sökbegrepp. Resulterar sökningen i fler än 100 möjliga personer måste sökvillkoren begränsas för att svar ska erhållas. Avgift debiteras endast i de fall sökningen resulterar i ett svar.

Öppethållandetider framgår av Allmänna villkor, bilaga 10 till den Allmänna beskrivningen.

Ytterligare upplysningar lämnas i bilaga 6 till den tekniska beskrivningen "Teknisk handledning Web Service".

För åtkomst krävs certifikat, som f.n. utfärdas av Steria.

4 Sökbegrepp

Vid ändringsavisering och urval finns dessa sökbegrepp för att bestämma de personer som ska ingå i uttaget:

- födelsetid, även intervall
- viss ålder innevarande år, även intervall
- kön
- geografiskt område: län, kommun, församling eller postnummerområde
- svenskt, norskt, finskt, danskt, isländskt, inom eller utom EU-medborgarskap
- datum för svenskt medborgarskap, även intervall
- avlidna eller utvandrade, inkl datum, även intervall

Det går inte använda andra villkor än de angivna sökbegreppen. Det går t.ex. inte att ta fram alla personer med 2 barn eller alla ogifta män.

Däremot går det med hjälp av datumuppgiften att ta fram nyblivna svenska medborgare i visst område och även de som avlidit i eller utvandrat från visst område.

Som sökbegrepp kan användas kategorin avlidna eller utvandrade. Med detta avses att man kan få avisering på personer som tidigare år avregistrerade från folkbokföringen om t.ex. ändrad utlandsadress för en utvandrad person eller rättelse av dödS- resp utvandringsdatum.

Vid val av endast kategorin folkbokförda får man förstås avisering även vid dödsfall, utvandring och invandring.

5 Sortering

Urvalsuttagen kan sorteras efter olika variabler, numeriskt eller alfabetiskt, i första hand, i andra hand, i tredje hand osv.. Förutom samma variabler som sökbegreppen kan sortering ske även i efternamns- och postortsordning.

6 Media för utdata

Avisering och urval kan levereras på dessa olika sätt:

- filöverföring med direktåtkomst via Internet (Web Services).
- filöverföring satsvis via Internet, antingen med hjälp av SHS-nod eller e-Transport.
- magnetmedia i form av cd
- pappersutskrifter i form av personlista (ca 10 per sida), aviseringslista (ca 4 per sida), personavi

(1 per sida) och adressetiketter, se bilagorna 6 - 9.

7 Beställning av tjänster

Beställning görs på den blankett som Skatteverket fastställt. Blanketten med anvisningar finns på Skatteverkets hemsida. På blanketten finns hänvisning till Navets gällande dokumentation, inklusive Allmänna villkor och prislista. Blanketten fungerar därmed som en offert om inte annat anges. Avtal anses ingånget när en beställning har inkommit till Skatteverket. Efter att beställningen registrerats skickar Navet en orderbekräftelse.

Beställningsblanketten tillsammans med orderbekräftelsen utgör dokumentationen över överenskommelsen med Skatteverket. Navet använder samma villkor vad avser terminnehåll, format, tillgänglighet etc. mot alla kunder. De villkor som gäller är de som framgår av dokumenten på Navets hemsida. Ändras någonting i systemet så ändras den gällande dokumentationen. Endast i undantagsfall behöver någon särskild dokumentation över överenskommelsen upprättas.

I de allmänna villkoren anges att mottagande myndighet garanterar att erhållna uppgifter inte behandlas i strid med personuppgiftslagen. Det är alltså mottagaren som är ansvarig för den behandling eller det eventuella utlämnande som sker av uppgifter efter det att de lämnats från Navet. Detta gäller oavsett om mottagaren konstruerat ett eget datasystem eller om en servicebyrå anlitas, dit uppgifterna enligt mottagarens önskemål ska levereras.

Kringaktiviteter såsom kuvertering mm tillhandahålls inte av Skatteverket. Denna typ av tjänster erbjuds av ett antal aktörer på marknaden som mottagarna själva får anlita.

8 Beskrivning av innehållet i Navet

Registret innehåller samtliga personer som är folkbokförda eller av annan anledning tilldelats personnummer eller samordningsnummer.

Följande uppgifter för personerna finns i registret, presenterade i den ordning de redovisas i den tekniska beskrivningen. Vissa uppgifter, huvudsakligen av teknisk eller administrativ karaktär, men även s.k. sårlösningsuppgifter som endast vissa myndigheter får enligt särskild förordning, presenteras inte här:

- *personnummer*
För varje person som registreras i folkbokföringen fastställs ett personnummer som identitetsbeteckning.

Sedan 2009-07-01 kan personnummer tilldelas även för utländsk ambassadpersonal och andra med diplomatisk immunitet. Det innebär att personer som omfattas av lagen (1976:661) om immunitet och privilegier och som inte ska folkbokföras i Sveriges, i vissa fall får tilldelas ett personnummer på begäran av Regeringskansliet. Personnumret aviseras i samma fält som ett samordningsnummer.

- *tilldelat personnummer*
Personer som tilldelats personnummer utan att vara folkbokförda. Om en person tilldelats personnummer av annan anledning än folkbokföring och sedan blir folkbokförd behåller han det tidigare tilldelade personnumret. Detta är alltså inte något tillfälligt nummer som senare ersätts av annat nummer.

De uppgifter som redovisas för dessa personer är endast personnummer och namn.

Tilldelat personnummer levereras endast till vissa centrala myndigheter.

Efter 1999-12-31 tilldelas personnummer endast för personer som är folkbokförda.

- *samordningsnummer*
Sedan 2000-01-01 tilldelas samordningsnummer för personer som inte är folkbokförda. Blir personen senare folkbokförd erhåller den ett personnummer. Samordningsnumret är uppbyggt som ett personnummer fast med talet 60 adderat till födelsedagen.

För personer med samordningsnummer redovisas även namn, medborgarskap och födelseort samt om dessa uppgifter är styrkta.

Samordningsnummer levereras vid ändringsavisering endast till vissa centrala myndigheter.

I fältet för samordningsnummer aviseras sedan 2009-07-01 även personnummer för utländsk ambassadpersonal och andra med diplomatisk immunitet som inte ska folkbokföras i Sveriges.

- *sekretessmarkering*
Markering för att särskild sekretessprövning ska ske innan uppgifter om personen utlämnas (även kallat skydd av personuppgifter).

- *ärendetyp, kod*
Vid ändringsavisering innehåller varje personpost koder för de ärenden som gjorts på personen sedan senaste avisering, se bilaga 1. Se även Teknisk beskrivning, avsnitt 6.5.1, Kommentar till termkod.

- *hänvisningspersonnummer*
För de personer som bytt personnummer anges tidigare personnummer/samordningsnummer.

Det gamla personnumret/samordningsnumret utgör även den en egen personpost. I det fallet är det det nya personnumret som anges som hänvisningspersonnummer.

- *avregistreringsorsak*
Uppgift om avregistreringsorsak anges enligt följande

AV = avliden
UV = utvandrad

GN = gammalt personnummer (anges för det nummer som upphör vid personnummerbyte eller dubbla personnummer)
GS = gammalt samordningsnummer

Fr.o.m. 2006-09-20
OB = avregistrerad från folkbokföringen som obefintlig
TA= teknisk avregistrering av personnummer, exempelvis vid annullering av invandring
AS= annullering av samordningsnummer

Innan 2006-09-20
AN = avregistrerad från folkbokföringen av annan anledning än avliden eller utvandrad, exempelvis vid obefintlighet eller annullering av invandring.

Datum (år, mån, dag) anges för senaste ändring.

- *namn*
En persons namn består av förnamn och efternamn samt i vissa fall även mellannamn. Ett aviseringsnamn på 36 tecken skapas för personer vars hela namn överstiger detta antal tecken.

Om uppgift om tilltalsnamn finns för förnamn markeras detta med en numerisk tvåställig kod enligt följande exempel:

För förnamn markeras tilltalsnamnet med en numerisk tvåställig kod enligt följande exempel:

Eva Mia: Mia är tilltalsnamnet, markeras med 20.

Kjell Olof: Kjell Olof är tilltalsnamn, markeras med 12.

Hedvig Britt-Marie: Britt-Marie är tilltalsnamn, markeras med 23 (förnamn med bindestreck betraktas som två namn).

- *folkbokföring*
Den fastighet som en person är folkbokförd på. I begreppet ingår följande

lån

kommun
församling
fastighetsbeteckning
fiktivt nummer för fastighet

Ett fiktivt nummer finns på de fastigheter som tillhör mer än ett valdistrikt. För de flesta fastigheter är det fiktiva numret noll.

Datum (år, mån, dag) anger när personen folkbokfördes på fastigheten.

Även om en person inte är bosatt på en viss fastighet ska han folkbokföras i en viss församling. Han folkbokförs då under rubriken "På församlingen skriven".

Den vars adress och vistelseort är okänd folkbokförs under rubriken "Utan känt hemvist".

- *folkbokföringsadress*
Adressen till en persons folkbokföringsfastighet (bostadsadress). Adressen är uppbyggd enligt den nya adresstandarden SS 61 34 01 och innehåller följande termer:

c/o
utdelningsadress 1
utdelningsadress 2
postnummer
postort

- *riksnycklar*
Riksnycklar för lägenhet, adressplats och fastighet på personnivå

- *särskild postadress*
En särskild postadress är den adress till vilken en persons post ska delas ut. Adressen är uppbyggd enligt den nya adresstandarden SS 61 34 01 och innehåller följande termer:

c/o
utdelningsadress 1
utdelningsadress 2
postnummer

postort

En person kan ha både en folkbokföringsadress och en särskild postadress. Som särskild postadress aviseras också postadress för personer med samordningsnummer.

- *prioriterad adress*
De huvudsakliga adresstyperna är folkbokföringsadress och särskild postadress. De flesta personer har bara folkbokföringsadress. Man kan alltid välja en eller flera adresser, i den mån de finns, för en person, men med detta val kan man se till att få endast en adress, som prioriteras före de andra. Här bortses från ev. utlandsadress. Prioriterad adress innebär att den särskilda postadressen redovisas om det finns en sådan, i annat fall redovisas folkbokföringsadressen.

- *utlandsadress*
En person som är utvandrad kan anmäla en adress där han kan nås i utlandet eller i Sverige. Adressen är uppbyggd enligt den nya adresstandarden SS 61 34 01 och innehåller följande termer

utdelningsadress 1
utdelningsadress 2
utdelningsadress 3
land

En folkbokförd person kan ha både en folkbokföringsadress och en utlandsadress.

- *datum för utlandsadress*
Det datum som utlandsadressen registrerades i folkbokföringen.

- *datum för rösträtt*
Det datum som utlandsadressen registrerades i folkbokföringen. För den som på nytt anmäler att han eller hon vill finnas kvar i röstlängden eller anmäler adressändring börjar en ny tioårsperiod att löpa.

- *civilstånd*

Uppgift om aktuellt civilstånd anges med följande koder

OG = ogift
G = gift
Ä = änka/änkling
S = skild
RP = registrerad partner
SP = skild partner
EP = efterlevande partner

Datum (år, mån, dag) för civilståndsändring anges.

- *födelsehemort*
För en person som är född i Sverige anges län och födelsehemort (församling) i klartext.

- *födelseort*
För en person som är född utomlands anges födelseort och födelseland i klartext. En person kan ha både födelsehemort och födelseort (om modern var folkbokförd i Sverige vid födelsen).

- *invandringsdatum*
Datum (år, mån, dag) för när en person folkbokfördes vid senaste inflyttningen från utlandet.

- *make/maka/partner*
Anges med personnummer för make/maka/partner.

Observera att det för make/maka/partner, förälder, barn eller annan relation endast anges personnummer. Det går alltså inte att i ett och samma uttag för en viss krets barn, utöver personnumren, t.ex. få föräldrarnas namn och adress. Undantaget är då en relationsperson aldrig varit folkbokförd och inte heller har personnummer av annan anledning. Då redovisas födelsetid och namn för denne.

- *vårdnadshavare*
För ett barn under 18 år anges vårdnadshavarna med personnummer. Vårdnadshavarna kan vara en eller två, i undantagsfall flera än två.

- *vårdnadshavare för*

För en person över 18 år anges vilka barn en person är vårdnadshavare för med barnens personnummer.

- *föräldrar*
För samtliga personer anges vilka som är personens moder och fader med personnummer. Det framgår inte om relationen är biologisk eller grundad på adoptivt förhållande. Även avliden förälder och dödsdatum redovisas. Observera att ett barn p.g.a. partneradoption kan ha två mödrar eller två fäder.

Fr.o.m. 1 juni 2006 redovisas även relationstypen Förälder: en kvinna som är registrerad partner eller sambo med en annan kvinna (modern), och som enligt 1 kap. 9 § föräldrabalken skall anses som förälder till barnet.

- *barn*
För en person anges de barn en person har med personnummer. Det framgår inte om relationen är biologisk eller grundad på adoptivt förhållande. Med barn menas här samtliga barn oavsett ålder. Även avlidet barn och dödsdatum redovisas.

- *medborgarskap*
Alla personer har minst ett registrerat medborgarskap. Även uppgiften okänt, under utredning och statslös registreras. För person med både svenskt och utländskt medborgarskap registreras endast det svenska. En person som inte är svensk medborgare kan ha upp till tre registrerade medborgarskap. Uppgift om datum (år, mån, dag) för förvärv av svenskt eller registrering av utländskt medborgarskap anges.

Medborgarskapet registreras med en tvåställig bokstavskod enligt standarden ISO 3166. Förteckning över landskoder finns på Navets hemsida, www.skatteverket.se - Företag & organisationer - För myndigheter & kommuner - Navet.

Datum (år, mån, dag) anges för när personen förvärvade medborgarskapet. För personer som förvärvat svenskt medborgarskap före 1991-07-01 anges endast nollor.

- *historik*
Samtliga uppgifter om en persons folkbokföring under innevarande år och de två näst föregående åren samt den senast ändrade uppgiften dessförinnan. Även den aktuella uppgiften redovisas. Varje uppgift innehåller följande termer:

länkommunförsamlingfastighetsbeteckningdatum (år, mån, dag) anges för när personen folkbokfördes på fastighetenfolkbokföringstyp (FB = Folkbokförd, UV = Utvandrad och OB = Obefintlig)

- *föregående folkbokföringsadress*
Uppgift som vid ändring av folkbokföringsadressen visar den gamla adressen. Det behöver inte vara en faktisk flyttning, det gäller även vid en administrativ ändring som t.ex. postnummerändring. Den kan endast erhållas vid den löpande ändringsaviseringen, den lagras inte i Navet.

9 Skydd av personuppgifter

"Skyddade personuppgifter" är en samlingsrubrik som Skatteverket använder för de olika skyddsåtgärderna sekretessmarkering, kvarskrivning och fingerade personuppgifter.

Enligt 22 kap. 1 § offentlighets- och sekretesslagen är uppgifter inom folkbokföringsverksamheten i regel offentliga. Sekretess gäller om det av särskild anledning kan antas att en person, eller någon närstående, kan lida skada eller men om uppgifter om personen lämnas ut.

9.1 Sekretessmarkering

I de fall skattekontoret på förhand kan bedöma att utlämnande av uppgifter om en person kan förorsaka

personförföljelse eller annan skada kan en s.k. markering för särskild sekretessprövning ("sekretessmarkering") sättas för personen i folkbokföringsdatabasen. En sådan bedömning på förhand kan exempelvis grundas på att personen själv redogör för omständigheterna.

Exempel på en situation då personuppgifter kan skyddas är når en kvinna begär att hennes adress inte skall lämnas ut till en tidigare make eftersom det finns ett konkret hot om att han skall utsätta henne för skada. Detsamma gäller en politisk flykting som vill skydda sig mot repressalier från meningsmotståndare.

Det finns inte några formella krav för att få en sekretessmarkering. Någon form av intyg, exempelvis från polis eller socialtjänst, eller annan utredning som styrker åberopade förhållanden bör finnas som underlag för bedömningen. En allmänt uttalad motvilja mot att ha kontakt med en annan person är inte tillräckligt skäl för en sekretessmarkering. Inte heller är det tillräckligt att endast ange ett yrke som normalt kan vara utsatt för vissa risker, exempelvis polis eller åklagare, som skäl för sekretessmarkering. Det bör röra sig om ett konkret hot i det enskilda fallet.

Sekretessmarkeringen motsvarar i princip den hemligstämpling som, enligt 5 kap. 5 § offentlighets- och sekretesslagen, kan åsättas en allmän handling. Det framgår inte av själva markeringen vilken uppgift om personen i folkbokföringen som kan vara känslig. Det behöver inte bara vara adressen som är den skyddsvärda uppgiften, det kan även vara nytt namn eller uppgifter om närstående.

Markeringen skall fungera som en varningssignal så att en noggrann prövning görs innan några uppgifter om personen lämnas ut. En sekretessmarkering innebär inte någon absolut sekretess. Vid en begäran om utlämnande av personuppgifter ska myndigheten göra en självständig sekretessbedömning. Vid bedömningen kan myndigheten komma fram till att uppgifterna ska lämnas ut.

Det är vanligt att sekretessmarkeringen i olika sammanhang benämns "adresskydd", "skyddad adress", "skyddad identitet" eller t.o.m. "identitetsbyte".

Alla personer som berörs av en hotsituation, exempelvis samboende personer, bör ha motsvarande skydd så att den hotade inte kan spåras upp via kända familjerelationer.

Omprövning av sekretessmarkeringen sker i regel varje år. Den skyddade personen ska därvid redogöra för de aktuella förhållandena varvid det prövas om skyddet ska vara kvar.

Skatteverket aviserar sekretessmarkeringen till andra myndigheter tillsammans med övriga uppgifter om personen. Markeringen innebär alltså inte att sekretessbelagda uppgifter utesluts i aviseringen. När sekretessmarkeringen tas bort aviseras detta.

Sekretessmarkeringen förhindrar inte t.ex. rättsvårdande instanser att komma i kontakt med personen. Myndigheter som av legala skäl behöver uppgifterna får det.

I övrigt ger Skatteverket service till de som vill nå en skyddad person genom att vidarebefordra postförsändelser till denne. Avsändaren behöver inte veta var i landet personen är folkbokförd utan kan lämna försändelsen till närmaste förmedlingskontor. Se mer om detta i Skatteverkets vägledning för hantering av sekretess.

I september 2010 var 12 420 personer sekretessmarkerade i Sverige

9.2 Kvarskrivning

Ett annat sätt att skydda personuppgifter i folkbokföringen är att genom beslut om kvarskrivning enligt 16 § folkbokföringslagen medge en person vid flyttning att vara folkbokförd på den gamla folkbokföringsorten i högst tre år.

Kravet för en person att få bli kvarskriven är att han av särskilda skäl kan antas bli utsatt för brott, förföljelser eller allvarliga trakasserier på annat sätt. Omständigheterna ska i princip motsvara

de som gäller för meddelande av besöksförbud enligt lagen (1988:688) om besöksförbud.

Fördelen med kvarskrivning är att den verkliga bostadsorten inte framgår av folkbokföringsregistret och därmed inte heller sprids till aviseringsmottagarna. Den gamla adressen tas bort och personen registreras som "på församlingen skriven". Skattekontorets adress anges som en särskild postadress.

Det som aviseras till andra myndigheter är en flyttning där personen blivit "på församlingen skriven" och med den särskilda postadressen. Någon annan särskild markering aviseras inte. All post går då till skattekontoret som har den faktiska adressen manuellt förvarad och kan vidarebefordra posten.

Kvarskrivningen fungerar som ett adresskydd. Men i regel får en kvarskriven person också en sekretessmarkering. Då aviseras naturligtvis även sekretessmarkeringen.

Antalet kvarskrivningar inom landet är blygsamt i förhållande till antalet sekretessmarkeringar. I september 2010 var 1 728 personer kvarskrivna i Sverige.

Anledningen till detta kan vara att det kan vara besvärligt att ta del av samhällsservicen om man är folkbokförd någon annanstans än där man bor. Folkbokföringen har betydelse för exempelvis tillgång till förskoleplats, skolgång eller bostadsbidrag. Dessutom är beskattning och rösträtt knutet till folkbokföringsorten.

Det kan påpekas att när en person i vanliga fall folkbokförs "utan känt hemvist" så är detta inte detsamma som skyddad adress. Det innebär endast att skattekontoret inte kunnat bedöma var personen normalt tillbringar sin dygnsvila.

9.3 Fingerade personuppgifter

Vid särskilt allvarliga hot kan en person medges att under högst fem år använda annan identitet. Beslut

om detta meddelas av Stockholms tingsrätt efter ansökan hos Rikspolisstyrelsen (RPS).

I folkbokföringen avregistreras den gamla identiteten som obefintlig. Den nya identiteten inregistreras på ett sådant sätt att det inte framgår att det rör sig om fingerade personuppgifter. Kopplingen mellan identiteterna finns endast hos RPS.

Det som aviseras vid identitetsbytet är endast avregistrering av en person som obefintlig. Den nya identiteten aviseras som en vanlig nyinsättning, exempelvis invandring, utan att det anges att det är en ny identitet.

Det finns för närvarande ca 20 personer som har fingerade personuppgifter i folkbokföringsregistret.

9.4 Hantering av skyddade personuppgifter inom Skatteverket

Åtkomsten inom Skatteverket till personuppgifter vid sekretessmarkering är begränsad till en särskild behörighet. Ärendehandläggning avseende skyddade personer har inom folkbokföring, beskattning och fastighetstaxering sedan 2004-01-01 koncentrerats till ett fåtal personer inom Skatteverkets respektive tio regioner.

I folkbokföringssystemet visas motsvarande information för en sekretessmarkerad person, men även för make, föräldrar eller barn som är folkbokförda på samma adress.

Handläggningen av ett skatte- eller folkbokföringsärende för sekretessmarkerad person kan endast ske med den särskilda behörigheten till terminalsystemet.

På blanketter inom skatteområdet som ska användas av annan än den sekretessmarkerade personen, t.ex. jämkningsbeslut eller kontrolluppgift, anges inte adressen för att förhindra en onödig spridning av uppgiften.

Kopia av blankett där adress skrivs ut, t.ex. deklaration, kan endast tas fram med särskild behörighet. Detsamma gäller för personbevis inom folkbokföringen.

Vid kvarskrivning utblankas inga uppgifter eftersom den mest känsliga uppgiften, dvs. den faktiska bostadsadressen, inte finns i registret.

Det är endast ett fåtal personer inom varje region som känner till grunden för sekretessmarkeringen respektive kvarskrivningen och som beslutar om dessa åtgärder. Det är också bara de som avgör om en skyddad uppgift kan lämnas ut och till vem.

I de fall adress för skyddad person inte lämnas ut till andra myndigheter fungerar Skatteverket som brevlåda för de skyddade personerna. Kronofogdemyndigheten erhåller t.ex. inte uppgift om bostadsadress förrän det blir fråga om bostadsförrättning och skriftlig framställning skett om att få ut adressen samt förordnande skett om sekretess. I kronofogdemyndighetens terminalsystem är samtliga personuppgifter utom personnummer bortblankade för sekretessmarkerade personer.

Ansökningshandlingar för sekretessmarkering respektive kvarskrivning och övriga uppgifter som t.ex. polisutredningar m.m. förvaras inlåsta på ett betryggande sätt.

9.5 Möjliga alternativ vid beställning av uppgifter för sekretessmarkerade personer

9.5.1 Allmänt

Varje myndighet är ansvarig för sina egna personregister. Det innebär att det är myndigheten själv som, utifrån sina egna verksamhetsbehov, bestämmer vad som ska presenteras för användarna. Det finns således ingen övergripande policy för hur myndigheterna ska behandla uppgifter om t.ex. sekretessmarkerade personer.

Fråga om spärrmarkerade uppgifter kan lämnas ut eller inte prövas av respektive myndighet med stöd av sekretesslagens bestämmelser. Det är även respektive myndighet själv som avgör, med hänsyn till verksamhetens behov, om den vill ha uppgifter

om sekretessmarkerade personer och hur den väljer att hantera dessa uppgifter i sina register.

I Navet finns möjlighet att beställa färre uppgifter för sekretessmarkerade personer eller att helt avstå från dem.

I syfte att förbättra och underlätta hanteringen för aviseringsmottagarna samt stärka säkerheten för sekretesskyddade personer har tre stycken förändringar gjorts vid den löpande ändringsavisering.

De nya funktionerna är valbara (eftersom de inte fanns från början i Navet) men vår starka förhoppning är att mottagarna avstår från dem endast om det finns särskilda skäl.

9.5.2 Flyttsignal

När en sekretessmarkerad person flyttar ut från en registerhållares område aviseras förutom personnummer och sekretessmarkeringen alltid och endast koden 99 i fältet för län (termkod 01022).

Bakgrunden till ändringen är att om en registerhållare valt att normalt endast få uppgift om t.ex. personnummer och namn för en sekretessmarkerad person så ska han ändå få en signal om när personen flyttar från området (har folkbokföringsuppgiften valts bort så kan man ju inte se att den ändrats).

Ett annat skäl är att det knappast finns någon anledning att avslöja för utflyttningsområdet var en sekretessmarkerad person flyttar. Den förföljande personen kan ju t.o.m. ha sitt arbete i kommunen eller landstinget som den sekretessmarkerade personen flyttar från.

9.5.3 Totalpost när sekretessmarkering hävs

När sekretessmarkering hävs för en person aviseras alltid en totalpost, alltså även till de mottagare som normalt endast har ändringspost (endast ändrade termer).

Skälet till denna ändring är att många mottagare väljer att radera bort alla uppgifter (förutom kanske personnummer och namn) på en sekretessmarkerad person som flyttar in i området. När markeringen hävts har de mottagare med ändringspost i aviseringen hittills endast fått uppgift om att markeringen hävts, resten av uppgifterna för personen har de då saknat.

Med denna funktion bör flera mottagare komma att använda metoden att radera uppgifter som inte behövs.

9.5.4 Alltid sekretessmarkering vid ändringspost

När ändringsavisering sker för en sekretessmarkerad person skickas alltid sekretessmarkeringen med, oavsett vilken uppgift som ändrats.

Ett skäl till denna ändring är att det för mottagare med ändringspost inte av själva aviseringsposten framgått att personen är sekretessmarkerad om ändringen avsett t.ex. namn eller adress. Aviseringsposten, som ligger t.ex. på cd såväl före uppdateringen som efter (som backup) har därmed varit oskyddad och det har varit risk för att uppgifterna röjts.

Ett annat skäl hör samman med hanteringen av de dubbla filer som blir resultatet när en mottagare valt färre uppgifter för sekretesskyddade personer, se bilaga 3. Det har hittills varit lite besvärligt för mottagare med ändringspost att avgöra i vilken ordning filerna ska läsas in. När sekretessmarkeringen alltid är med bör det vara enklare.

Av olika anledningar kanske någon av dessa tre nya funktioner inte passar alla mottagande system. De har därför gjorts valbara. Men vi vill återigen understryka vikten av att aviseringsmottagarna för in dessa funktioner i sina system för att stärka säkerheten kring sekretessen.

10 Gallring av uppgifter i Navet

När en person avregistrerats som utvandrad, avliden eller av annan anledning innan 2005-11-28 gallrades samtliga uppgifter direkt utom personnummer, namn, adress för utvandrad, senaste folkbokföring, medborgarskap samt avregistreringsorsak och datum. Efter 2005-11-28 gallras inga uppgifter längre. För de avregistrerade personer som tidigare har gallrats uppdateras Navet med de gallrade uppgifterna när ett ärende (exempelvis rättelse eller ändrad utlandsadress) görs för personen.

Personer som avregistrerats före 1991 år helt utgallrade ur registret, med undantag för utvandrade svenska medborgare.

Personer födda före 1920 och som har avregistrerats som utvandrade eller obefintliga före 1990 har inte laddats in i registret.

Om en person anmält en utlandsadress senare än datumet för avregistreringen gallras adressen 10 år efter anmälningsdatum.

För folkbokförda personer gallras uppgift om datum för invandring 4 år efter utgången av registreringsåret.

KODER FÖR TYPER AV ÄRENDEN

Kod	Ärende
1	Personnummerbyte
2	Dubbla personnummer
3	Sekretessmarkering
5	Samordningsnummer
6	Födelse
9	Faderskap, registrering och avslut
12	Vårdnad, registrering och avslut
21	Efternamn
25	Mellannamn
29	Förnamn med ev. tilltalsnamns markering
32	Aviseringsnamn
36	Medborgarskap
37	Föräldraskap, registrering och avslut
40	Invandring
41	Flyttning
43	Utvandring
45	Särskild postadress
46	Fr.o.m. 2006-09-20 Avregistrerad som obefintlig Innan 2006-09-20 Avregistrering av annan anledning än dödsfall eller utvandring
56	Vigsel
59	Upplösning av äktenskap
62	Registrerat partnerskap
64	Upplösning av partnerskap

BILAGA 1

Datum
2011-02-15

Kod	Ärende
66	Dödsfall
74	Administrativ ändring av fastighet
75	Administrativ ändring av adress
81	Namnändring för person med tilldelat personnummer/samordningsnummer som lyder under svensk namnlag
83	Personnummerbyte för en person med tilldelat personnummer/samordningsnummer
84	Dubbla personnummer för en person med tilldelat personnummer/samordningsnummer, i vissa fall även hänvisning mellan samordningsnummer och personnummer
85	Postadress-SN
98	Utlandsadress
99	Övrigt

200 + ärendekoden är rättelse av en uppgift.

300 + ärendekoden är en annullering av hela ärendet.

Vid födelse är 306 rättelse av relationsperson i ärendet medan 506 är annullering av en födelse.

999	Teknisk rättelse. I detta läge sker avisering av personposten alltid som en totalpost.

Koden för alla ärendetyper utom 99 och 999 efterföljs av antingen H eller R. H betyder att denna person är huvudperson i det ärende som görs på det lokala skattekontoret. R innebär att denna person har en relation till huvudpersonen och har påverkats av ärendet för huvudpersonen.

BILAGA 2

Datum
2011-02-15

HANTERING AV INFIL

Kunder vars register har en population som inte motsvaras av ett visst geografiskt område kan inte aviseras på "det vanliga" sättet. De måste i stället skicka in sin population på en infil. Infilen kan vara på vilket magnetmedium som helst, det går även bra med linjeöverföring.

Det medium som kunden vill ha utfilen på anges på vanligt sätt som mediaformat på beställningen, däremot behöver inte infilens medium anges någonstans. Om SHS eller e-transport används för leverans av infiler måste samma format användas för utfiler.

Infil är möjlig att använda såväl vid laddning/urval som ändringsavisering. Normalt är en infil "förbrukad" när en körning har gjorts mot den. Det går att ange att infilen ska vara kvar och kunna fortsätta användas.

Ändringsavisering kan alltså ske löpande, exempelvis veckovis, mot en infil som ligger kvar. Kunden kan när som helst skicka in en ny uppdaterad infil, systemet använder då den infilen vid nästkommande uppdatering.

Några villkor (begränsningar) ska oftast inte anges vid infil. Sökning görs ju ändå bara mot de personer som finns på infilen. Det kan hända att kunden bara vill ha svar på de som är folkbokförda (för att minska kostnaden). I sådant fall kan kategorin Folkbokförda anges på beställningen.

Det är först när Navet känner av att infil (med rätt beställningsid) kommit in som körningen görs.

Kunden behöver veta beställningsid för att kunna upprätta en infil och måste därför först skicka in en beställning som ska registreras.

Av Tekniska beskrivningen, avsnitt 5, framgår hur infilen ska upprättas.

Det finns fyra olika infilsrutiner vid urval:

a) Enstaka urval
- endast en infil per dag kan tas om hand. Har flera infiler kommit in samma dag tas endast den senast inkomna om hand. Svarsfilen tas fram nattetid.

Körning görs automatiskt endast vid ett tillfälle. Systemet känner av vilken infil som är den sist inkomna från kunden. Ska den köras igen måste kunden meddela Navet detta.

b) Dagligt urval (eller annan periodicitet förutom enstaka)

Som a) ovan, med skillnaden att körning görs automatiskt varje gång kunden skickar in en ny infil. Navet behöver alltså inte meddelas.

Tidigare fanns endast rutin a) och b). Numera bör i allmänhet "Flera urval" användas. Att enstaka urval är kvar beror på att det kan finnas behov av att spara en infil för flera körningar, exempelvis för att kunna skriva ut uttaget på flera olika medier, t.ex. adressetiketter och cd.

c) Flera urval
- flera infiler per dag kan tas om hand. Svaren tas fram nattetid.

Körning görs automatiskt när infiler kommer in. Navet behöver inte meddelas i förväg.

d) Svar direkt
- flera infiler per dag kan tas om hand. Svar erhålls direkt (inom ca 10 minuter)

Vid denna rutin måste kunden kunna skicka och ta emot uppgifterna via SHS/e-transport.

När en infil kommit in till Navet enligt rutin a) - c) görs uttaget, beroende på periodicitet, normalt påföljande dag tisdag-lördag.

Förutom själva indatafilen måste även en informationsfil (info.nav) ligga på samma medium (detta gäller inte vid överföring via SHS/e-transport).

Exempel (om det var vi själva som var kund) enligt nedan.

#MEDIELEV_START
#TECKENPROV ÅÄÖÜåäöüÉé#_@
#ORGNR 2021000985
#NAMN SKATTEVERKET
#ADRESS
#POSTNR 171 94
#POSTORT Solna
#KONTAKT Björn Sjökvist
#AVDELNING Folkbokföringsenheten
#TELEFON 08-764 81 60
#MEDIELEV_SLUT
#DATABESKRIVNING_START
#PRODUKT NAVET
#FILNAMN datafil.txt
#DATABESKRIVNING_SLUT

Exempel på indatafilen:

#INFO_START
#FILTYP INDATAFIL
#BESTÄLLNINGSID 00002803-FO04-0037
#BESTÄLLNINGSTYP URVAL
#NAMN_INFIL datafil.txt
#GILTIG_TOM 19981231
#INFO_SLUT
#DATA_START
#PNR 192703308490
#PNR 192802286886
#PNR 193907189090
#DATA_SLUT
#AVST_START
#ANTAL_POSTER 00000003

#AVST_SLUT
#FIL_SLUT

Det namn som kunden själv hittar på och sätter i #NAMN_INFIL ska även sättas i #FILNAMN i informationsfilen. Det är först när maskinen hittar den upplysningen som den börjar låsa datafilen.

I detta fall ska #BESTÄLLNINGSID i indatafilen vara 00002803-FO04-0037. Observera att mellanledet FO04 är två bokstäver, FO, och två siffror, 04.

Det är viktigt att filerna ser ut exakt som ovan vad avser antal tecken (exempelvis 12 tecken för personnumret), mellanslag, nollutfyllnad etc. Varje #-tecken måste börja på ny rad, och varje rad måste börja med #-tecken! Det får heller inte vara blanktecken efter det sista tecknet i raden!

Glöm heller inte att ändra på giltighetsdatumet (#GILTIG_TOM). I exemplet är det satt till 19981231. Antingen ska datumet raderas och lämnas blankt (om man inte vill ha någon särskild giltighetstid för infilen) eller så ska ett datum framåt i tiden sättas.

Slutligen ska rätt antal personnummer anges i #ANTAL_POSTER med totalt 8 tecken.

Det medium infilerna finns på ska skickas till Skatteverkets inläsningscentral, Enhet 4300, 839 86 ÖSTERSUND, och vara märkt INFO.NAV.

Beställningen sätts igång så snart en infil har kommit in. Om det är ett engångsuttag som beställts måste Navet meddelas om den ska köras igen. Likaså om ett speciellt uttagsdatum önskas. Det är dock alltid den aktuella statusen på uppgifterna vid uttagstidpunkten som redovisas.

Hantering av filer då färre uppgifter beställts för sekretessmarkerade personer

Som framgår av avsnitt 9.5 så kan mottagaren välja om den vill ha endast vissa uppgifter (exempelvis personnummer och namn) för sekretessmarkerade personer.

Ett sådant val innebär att två olika aviseringsfiler skapas, en för ej sekretesskyddade personer och en för sekretesskyddade, eftersom uttagsrutinen inte kan välja olika mängd uppgifter för skilda personkategorier i en och samma fil.

Vid de tillfällen sekretess sätts respektive hävs för en person kommer personen att förekomma i bägge filerna. Tanken bakom detta är att ej sekretessmarkerade personer förutsätts finnas i ett register och de sekretessmarkerade personerna i ett annat register.

Eftersom de flesta mottagare ändå har alla personer i ett och samma register kan det uppstå problem med att avgöra i vilken ordning de båda filerna ska låsas in.

Det viktiga är att personen får rätt uppgiftsinnehåll efter uppdateringen. Detta innebär att filerna måste låsas in i rätt ordning för att det ska bli rätt. De olika aviseringsfilerna när sekretess sätts resp hävs ser ut enligt följande (A= fil med ej sekretessmarkerade, B= fil med sekretessmarkerade), dels vid posttypen ändringspost dels vid posttypen totalpost.

Då sekretess sätts

	Ändringspost	Totalpost
A	Pnr och 01003=J	Alla termer, inkl 01003=J
B	De färre termer som valts (totalpost), inkl 01003=J	De färre termer som valts, inkl 01003=J

Då sekretess hävs

	Ändringspost	Totalpost
A	Alla uppgifter (totalpost), ej J i 01003	Alla uppgifter, ej J i 01003
B	Pnr och 01003=$	De färre uppgifter som valts, ej J i 01003

Anledningen till att det kommer en totalpost i B-filen då sekretess sätts (även om det i och för sig är färre uppgifter) resp i A-filen då sekretess hävs är att personen förutsätts att inte sedan tidigare finnas i mottagarens register.

Förslag till hantering av fil med resp utan sekretessmarkerade personer:

Har man totalpost så räcker det med att efter inläsning av A-filen läsa in de poster i B-filen som har 01003=J. Personen får då alltid rätt uppgiftsmängd.

Detta räcker inte vid ändringspost eftersom 01003=J inte skickas med då en person bara finns med på B-filen, t.ex. vid namnbyte. Å andra sidan finns då inte heller 01003=$ med (hävning av sekretess). Man borde alltså efter inläsning av A-filen kunna läsa in de poster i B-filen som har 01003=J **eller** inte har 01003=$.

Det finns sedan maj 2000 möjlighet att välja en tilläggsfunktion för sekretessmarkerade, nämligen att alltid skicka med 01003=J vid ändringsavisering oavsett posttyp. Ändringspost kommer då att fungera som totalpost i detta avseende.

Exempel på ett annat förfarande:

1. Finns samma person i både A- och B-filen? (=för att se om sekretess sätts resp hävs för någon)

2. Om Ja, finns 01003=J i båda filerna? (=för att se om sekretess sätts)

3. Om Ja, läs bara in posten i B-filen. (=personen får då de färre uppgifterna)
   Om Nej, läs bara in posten i A-filen. (=personen får då alla uppgifterna)

4. Läs slutligen in poster för personer som bara finns på B-filen. (=exempelvis namn har ändrats för en person som redan har sekretess)

BILAGA 4

Datum
2011-02-15

Filsammansättning avseende olika ändringsdagar

Då en fil består av ändringar från flera dagar så kan innehållet se olika ut beroende på följande orsaker (denna beskrivning utgår från filutseendet innan möjligheten till brytposter och löpnumrering infördes).

1. Har Navet uppdaterats i normal ordning, men avisering inte kunnat göras någon dag av någon anledning, så kommer varje dag som ett skikt för sig i kronologisk ordning. Varje skikt börjar med det lägsta personnumret den dagen och slutar med det högsta personnumret. Det kan alltså komma flera personposter för en och samma person i en fil men från olika dagar. Dock i kronologisk ordning så det inte blir någon överlappning.

Den information som finns i början på filen #DATUM_ANDRING anger de uppdateringsdagar av Navet som filen innehåller. Det är alltså inte de dagar som en ändring registrerats i folkbokförings-registret som avses. Exempel: #DATUM_ANDRING 19981202-19981208 som enligt almanackan är ons-tis innebär att filen innehåller de uppgifter som uppdaterat Navet fr.o.m natten mot onsdag t.o.m. natten mot tisdag. Har det inte varit avbrott i uppdateringen ligger då dagarna uppdelade i 5 skikt. Detta är det normala vid veckoavisering om den aktuella veckan inte innehållit någon helgdag eller annan arbetsfri dag. Uppgiften #EFFEKTUERAD 19981208 innebär att aviseringen till kunden skett på tisdagen.

2. Har Navet av någon anledning inte uppdaterats någon dag så kommer den dagens ändringar i folk-bokföringsregistret att uppdatera Navet sammanslagna med ändringarna dagen efter, som ett enda skikt. Exempel: #DATUM_ANDRING 19981203-19981208, som betyder den uppdatering av Navet som skett fr.o.m. natten mot torsdag t.o.m natten mot tisdag, innebär förmodligen lokala ändringar från tis-mån. I sådant fall ligger tisdagens och onsdagens ändringar i ett skikt och de tre resterande dagarna i varsitt skikt. Det kan även vara så att Navet endast uppdaterats 1998-12-03 och 1998-12-08 eftersom datumangivelsen

BILAGA 4

Datum
2011-02-15

anger det intervall som det finns uppdateringar inom. Har Navet under perioden endast uppdaterats 1998-12-08 är det bara det datumet som anges. Skulle det hända att Navet inte uppdaterats alls avseende en mottagares område så aviseras en tom fil med #DATUM_ANDRING 00000000. I vilket fall är det ingen risk för att någon dag tappas bort. Alla ändringar aviseras ut när de väl har uppdaterat Navet.

Löpnumrering av aviseringsfilerna kan beställas. Detta underlättar för mottagarna att se att inte någon fil "tappats bort" och att de behandlar filerna i rätt ordning.

Vid regelbunden ändringsavisering går det även att beställa "brytposter". Då framgår var i filen det ena skiktet slutar och det andra börjar (startpost). För att ytterligare underlätta, kompletteras startposten med det datum posten blivit upplagd i Navet.

Skatteverket

1(1)

BILAGA 5

Datum
2011-02-15

ARBETSGÅNG VID ANVÄNDNING AV INTERNET

1. Kunden beställer certifikat hos Steria.
2. Kunden sänder in beställningsblanketten med något av medium Internet (Web Service, SHS, eTransport) till Navet.
3. Navet registrerar beställningen.
4. Navet skickar orderbekräftelse med beställningsid till kunden alternativt även till ev. servicebyrå.
5. Vid eventuella problem att hämta hem filer kan Navet kontaktas.

Skatteverket

AVISERINGSREGISTRET

PERSONAVI 800420-9295

Datum
2011-02-15

DENNA PERSON HAR SKYDD AV PERSONUPPGIFTER ENLIGT 22 KAP 1 § OFFENTLIGHETS- och SEKRETESSLAGEN

Personnummer	800420-9295
Hänvisningspersonnummer	820417-9298
Förnamn	Björn Hugo Alfsson
Mellannamn	Perssonperssonpersson
Efternamn	Bergström
Folkbokföringsdatum	1996-03-01
län	01
kommun	80
församling	20
fastighetsbeteckning	Liljan 3
Folkbokföringsadress	c/o Gustafsson Torsgatan 422222222222222222 22222222222222222222 113 62 STOCKHOLM
Särskild postadress	c/o Blomved Melongränd 4444444444444444 444444444444444444444 157 40 JÄRFÄLLA
Civilstånd, datum	Ogift, 1980-04-12
Födelselän	Skaraborgs län
Födelsehemort	Lidköping
Födelseort i utlandet	Paris
Födelseland	Frankrike
Medborgarskap, datum	Spanien, 1980-04-12 Tunisien, 1980-04-12 Bosnien-Hercegovina, 1984-01-20
Invandringsdatum	1993-03-01
Vårdnadshavare	200517-2859 213642-1889

Tidigare folkbokföring	1995-01-01	1994-04-01	1993-03-01
län	01	03	01
kommun	22	09	15

Föregående folk-bokföringsadress	Tritonvägen 21 171 94 SOLNA

Skatteverket

AVISERINGSREGISTRET

1(1)

PERSONLISTA

Datum
2011-02-15

Personer 16-18 år Hässleholms Kommun

Personnr	Efternamn, förnamn (tilltalsnamn understruket) Civilstånd,datum	Medb	FB-datum	Utdelningsadress Län Kom Förs	Postnr Postort Fastighetsbeteckning
	Avreg.orsak,datum			Vårdnadshavare,datum	Vårdnadshavare,datum
999999-9999	X----------x			X----------x	
				X----------x	
				X----------x	
				999 99 X----------x	
	Xx, 99-99-99	Xx	99-99-99	99 99 99 X----------x	
	X-------x, 00-00-99			999999-9999, 99-99-99	999999-9999, 99-99-99
999999-9999	X----------x			X----------x	
				X----------x	
				X----------x	
				999 99 X----------x	
	Xx, 99-99-99	Xx	99-99-99	99 99 99 X----------x	
	X-------x, 99-99-99			999999-9999, 99-99-99	999999-9999, 99-99-99
999999-9999	X----------x			X----------x	
				X----------x	
				X----------x	
				999 99 X----------x	
	Xx, 99-99-99	Xx	99-99-99	99 99 99 X----------x	
	X-------x, 99-99-99			999999-9999, 99-99-99	999999-9999, 99-99-99
999999-9999	X----------x			X----------x	
				X----------x	
				X----------x	
				999 99 X----------x	
	Xx, 99-99-99	Xx	99-99-99	99 99 99 X----------x	
	X-------x, 99-99-99			999999-9999, 99-99-99	999999-9999, 99-99-99

PERSONNUMMERÄNDRAD POST, NYTT PERSONNUMMER 999999-9999

Skatteverket

AVISERINGSREGISTRET

2(2)

PERSONLISTA

Datum
2011-02-15

Personer 5-6 år Hässleholms Kommun

Personnr	Efternamn, förnamn (tilltalsnamn understruket)	Utdelningsadress	Församling
999999-9999	X----------x	X----------x	
		X----------x	
		X----------x	
		999 99 X----------x	999999
999999-9999	X----------x	X----------x	
		X----------x	
		X----------x	
		999 99 X----------x	999999
999999-9999	X----------x	X----------x	
		X----------x	
		X----------x	
		999 99 X----------x	999999
999999-9999	X----------x	X----------x	
		X----------x	
		X----------x	
		999 99 X----------x	999999
999999-9999	X----------x	X----------x	
		X----------x	
		X----------x	
		999 99 X----------x	999999
999999-9999	X----------x	X----------x	
		X----------x	
		X----------x	
		999 99 X----------x	999999

Till målsman för
Adam Bertil Caesar Davidsson
Storgatan 1
123 45 STOCKHOLM

Erik Filipsson
Hamngatan 1 LGH 1001
123 45 STOCKHOLM

Gustav Harald Ivarsson
Storgatan 34
123 45 STOCKHOLM

Karla Ludvigsson
c/o Martinsson
Torpet
Box84
543 21 LANDET

Martinsson, Adam Bertil Caesar David
Gatan 1
123 46 Staden

Davidsson, Erika Filippa Gustava H I
Gatan 2
123 46 Staden

Filippa Eriksson
c/o syrran
Jättelångalångalångalångalånga-
långagatan 2
123 45 Staden

Filippa Eriksson
c/o brorsan
Jättelångalångalångalångalånga-
långagatan 2
123 45 Staden

Kalle Ivarsson
Korta gatan 1112345
987 65 Nånstans

Namn
Adress
Postnr Postort

Namn
c/o
Utdelningsadress
forts
Postnr Postort

Namn
c/o
Utdelningsadress
forts
Postnr Postort

Namn
c/o
Utdelningsadress
forts
Postnr Postort

osv.

Namn
c/o
Utdelningsadress
forts
Postnr Postort

Skatteverkets allmänna villkor för utnyttjande av Navet

Allmänt

Dessa allmänna villkor gäller vid myndighets utnyttjande av Navet, d.v.s. Skatteverkets system för distribution av folkbokföringsuppgifter till samhället för ändamål som avses i 1 kap. 4 § 5 och 6 lagen (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet, i den mån annat ej överenskommits.

Ansvarm.m.

Av "Avisering av folkbokföringsuppgifter - Teknisk beskrivning" framgår de villkor som gäller för att hämta och lämna datafiler. Mottagande myndighet bekostar och ansvarar själv för anslutningar, linjer och klientverktyg för att hämta och lämna datafiler.

Skatteverket ansvarar inte för fel i tele- eller datanätsförbindelse eller elförsörjning som utomstående part tillhandahåller.

Skatteverket kan komma att stänga av Navet för nödvändigt systemunderhåll. Skatteverket meddelar dock detta och hur länge uppehållet varar, i regel minst ett par dagar i förväg.

Skatteverket meddelar förändringar i fil- och postutseende minst tre månader i förväg.

Personuppgiftslagen

Mottagande myndighet garanterar att erhållna uppgifter ej behandlas i strid mot personuppgiftslagen (1998:204).

Mottagande myndighet garanterar att rättelser kan mottas och uppdatera felaktiga uppgifter som har erhållits från Navet.

Betalningsvillkor

För utnyttjandet gäller priser i enlighet med av Skatteverket fastställd prislista. Ändrade priser från Skatteverket tillämpas först tre månader efter det att mottagande myndighet meddelats.

Priserna är angivna netto exklusive mervärdesskatt eller andra därmed jämförliga tillägg och offentliga avgifter. Avgifterna faktureras kvartalsvis i efterskott.

Giltighet

För utnyttjandet gäller en ömsesidig uppsägningstid av tre månader såvida ej annat överenskommits. Uppsägning skall ske skriftligt.

Web Services

Skatteverket ansluter efter beställning myndigheten till Navet.

Skatteverket svarar för att innehållet i Navet motsvarar de specifikationer som utfästs. Skatteverket dimensionerar och anpassar den tekniska miljön vid Skatteverket så att god tillgänglighet till Navet garanteras. Öppethållandetider för Navet framgår nedan.

Skatteverket informerar om förändringar i system, driftprogram inklusive datakommunikation som kan påverka avtalade funktioner, minst tre månader i förväg.

Vid Web Services har myndigheten rätt att för eget bruk överföra material från Navet till annat datorbaserat system via dataförbindelsen.

Kommunikation via Internet

Den nyckel/certifikat som behövs för att koppla upp sig mot Navet får inte placeras på en enskild tjänstemans dator. Nyckeln/certifikatet ska placeras på en server till vilken endast en begränsad mängd personer har tillgång.

Öppethållandetider

Navet är normalt tillgängligt för direktåtkomst alla dagar dygnet runt utom lördag kl. 20.00-20.10. Andra planerade avbrott meddelas kunderna särskilt, f.n. genom e-post.

Support kan endast erhållas ordinarie arbetsdagar kl. 08:00 – 16:30.

SKRIVELSE

Datum 2012-10-17

Dnr 8 30 26577-12/124

Kronofogdens beskrivning av konsekvenser med anledning av dataintrånget.

1. Bakgrund

Kronofogden har av åklagaren fått i uppdrag att beskriva konsekvenserna av dataintrånget hos Logica.

2. Allmän beskrivning av REX och SUPRO

REX och SUPRO är de ärendehanteringssystem som Kronofogdens gäldenärer/svarande registreras i. REX (Redovisningssystemet för exekutionsväsendet) är ett transaktionsbaserat indrivnings- och redovisningssystem i stordatormiljö som innebär ett omfattande stöd för Kronofogdens handläggning av Allmänna och Enskilda mål.
SUPRO (Summarisk Process) är ett stordatorbaserat diarie- och målhanteringssystem för Kronofogdens handläggning av mål om betalningsföreläggande.
I systemen finns uppgift om personnummer, namn, adress och personens skulder. Har personen skyddade personuppgifter är det personnumret och skulderna som syns i Rex, i Supro syns även vem som är sökande i målet. Personuppgifterna i dessa datasystem beställer vi av Skatteverket.

3. Kort beskrivning av grundarkitektur

Kronofogden och Skatteverket delar datamiljö där Skatteverket är Kronofogdens driftpartner och Skatteverket i sin tur upphandlar datordrift i huvudsak från driftleverantören Logica.
Kronofogdens system är placerade i ett flertal olika driftcenter.
Stordatormiljön är placerad hos Logica i Bromölla. Denna stordatormiljö delas mellan flera kunder till Logica. Stordatormiljön är uppdelad i så kallade logiska partitioner (LPAR) där olika kunder till Logica har tillgång till olika LPAR.
Data transporteras i en infrastruktur som i flera delar delas mellan ett flertal aktörer, men datatrafiken ska vara hanterad på ett sådant sätt att integriteten för kunderna upprätthålls.
I Figl återfinns en översiktsbild av de nät/zoner som beskriver hur Kronofogdens system är placerade.

www.kronofogden.se E-postadress: kronofogdemyndigheten@kronofogden.se

Postadress	Besöksadress	Telefon	Telefax
Box 1050	Esplanaden 1	0771-73 73 00	08-29 26 14
172 21 SUNDBYBERG	172 67 SUNDBYBERG		

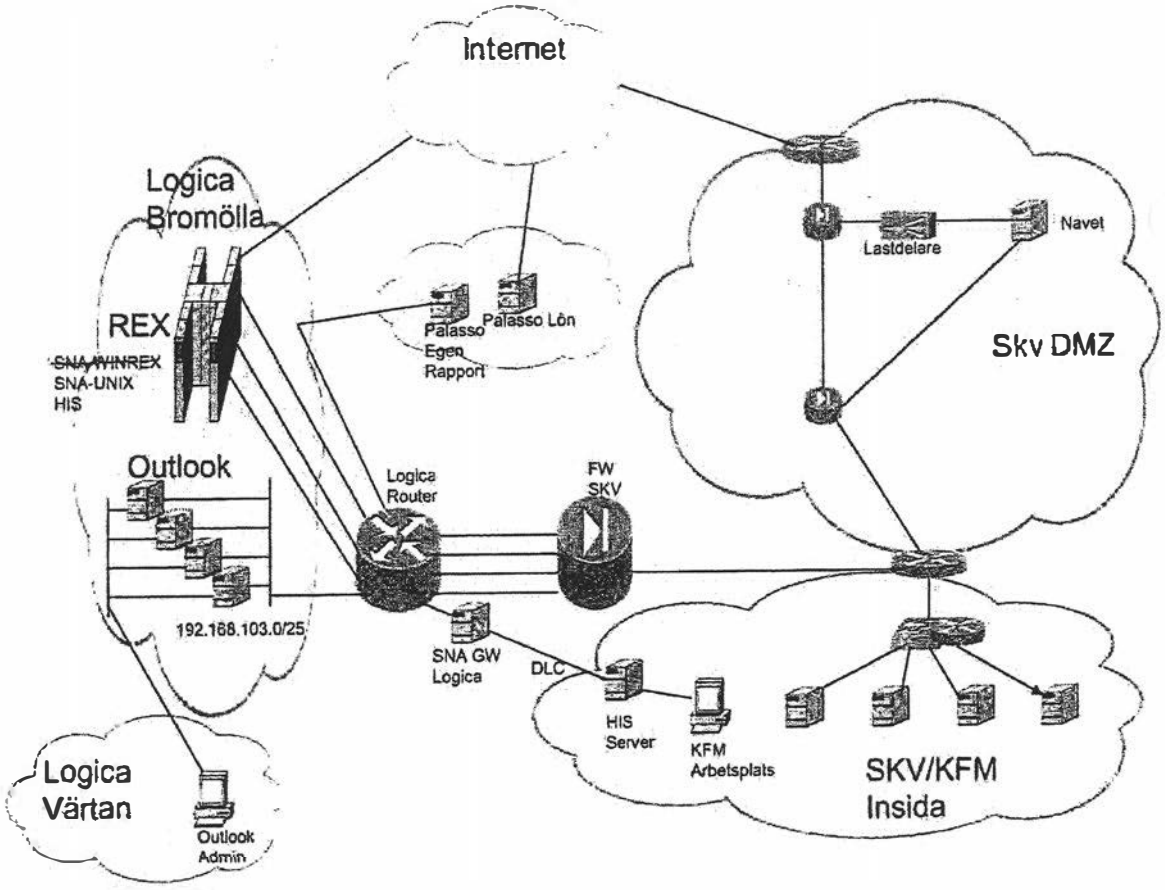


Fig 1

4. Konsekvenser

Kronofogden har hela tiden haft en höjd IT-beredskap och en höjd beredskap för kommunikation internt och externt samt samverkat regelbundet med andra myndigheter. En omfattande kartläggning av hur intrånget har gått till och framtagande av åtgärdsprogram har skett med hjälp av externa konsulter (en separat kostnadsredovisning kan tas fram).
För myndighetens IT-avdelning och säkerhetsfunktion har konsekvensen av händelsen varit en omprioritering av planerade projekt där främst CIO tvingats göra flera omprioriteringar (ingen kostnadsanalys eller tidsuppskattning har kunnat göras).

Efter intrånget har Kronofogden informerat de personer med skyddad identitet som drabbats. Eftersom dessa personer ofta kan känna oro för skyddet av sin

identitet, tog myndigheten omgående kontakt med de berörda för att de skulle få information om händelsen.
Medarbetare från Kronofogden deltog också i det KontaktCenter som Skatteverket startade. De gäldenärer som blev uppringda och ville ha ytterligare information hänvisades till Kronofogdens verkställighetsteam i Skellefteå som handlägger alla gäldenärer med skyddade personuppgifter (denna aktivitet har kunnat planeras inom den ordinarie verksamheten).

I bifbilaga finns ett antal filer uppräknade som Kronofogden bedömer ha blivit kopierade och som har olika känslighet.

- Filerna med redovisningsinformation (D044.EE52PROD.ABS.G0528V00 m fl) bedöms inte som känsliga. Det finns visserligen personuppgifter på dessa men informationen är offentlig om man begär ut den på vanligt sätt från myndigheten.

- Även när det gäller överföring av information till INIT (INIT är det nya IT-stödet för Kronofogdens indrivningsverksamhet. Systemet kommer successivt att ersätta dagens befintliga REX-system) för utskrift av krav (D044.IB25PROD.INITKRAV.G0398V00) är bedömningen att det inte handlar om känslig information i sig. Det är visserligen både skulduppgifter och namn och adress (dock inte skyddade), men informationen kan erhållas på begäran.
  Eftersom WinIT-filen (Urvals- och analysverktyg för sökning i de bakomliggande systemen INIT och REX) inte innehåller uppgifter om adresser till sökande eller ombud i mål är bedömningen att risken för att denna grupp ska kunna kartläggas på något mer ingående sätt liten..

- Den s k sigill-informationen (D044.GE42PROD.SIGILL)
  som inkräktaren fått tillgång till kan, såvitt Kronofogden kan bedöma, inte utan stor kunskap och inblick i verksamheten och dess rutiner användas för att styra om betalningar till andra betalningsmottagare än de avsedda. Nya sigill har ersatt de gamla och därefter är även den teoretiska möjligheten att påverka utbetalningar borta.

- De utbetalningsfiler (t ex D044.GE42PROD.SWBSIGB.G0012V00)
  som är berörda har redan effektuerats och kan inte påverkas. De utbetalningar som finns i filerna har nått rätt mottagare.

Sammanfattningsvis så anser Kronofogden att den skada som orsakats av intrånget handlar om myndighetens förtroende hos allmänheten och hos myndighetens kunder. Även om vissa uppgifter på begäran från allmänheten kan

SKRIVELSE

Datum
2012-10-17

lämnas ut så skadas myndighetens varumärke av att informationen finns tillgänglig på nätet.
Någon konkret återkoppling eller skadebeskrivning från någon kund, utöver information till de med skyddade personuppgifter, har inte rapporterats.
En fortsatt höjd beredskap råder hos Kronofogden och de samverkande myndigheterna.

Kontaktpersoner på Kronofogden för eventuella frågor är:

Pär Rasmusson, CIO	010-578 9936
Sven Kihlgren, Chef Verksamhetsområde 3	010-574 8209
Mats Kajler, Säkerhetschef	010-575 0174

Mats Kajler
Säkerhetschef

TDS_Table=TCP_FTP_SERVER_T								
LOCAL_USERID	TIMESTAMP	FTP_COMMAND	FULL_LOC_IP_ADDR	FULL_REM_IP_ADDR	DS_NAME		Verksamhetens bedömning	BYTE_COUNT
NUS	2012-03-19-21.52.28.570000	RETR	192.16.143.2	93.186.170.54	D044.AE75PROD.PG8OKDAT	Parameterdatum för kontroll av PG-band	Ointressant innehåll	18
NUS	2012-03-20-00.35.56.830000	RETR	192.16.143.2	93.186.170.54	D044.EE24PROD.NRAP.G3873V00	Tomfil		0
NUS	2012-03-20-00.35.57.090000	RETR	192.16.143.2	93.186.170.54	D044.EE24PROD.NRAP.G3874V00	Tomfil		0
NUS	2012-03-20-00.36.04.810000	RETR	192.16.143.2	93.186.170.54	D044.EE35PROD.ERAP.G2977V00	Tomfil		0
NUS	2012-03-20-00.36.05.050000	RETR	192.16.143.2	93.186.170.54	D044.EE35PROD.ERAP.G2978V00	Tomfil		0
NUS	2012-03-20-00.38.14.150000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.ABS.G0528V00	PRELIMINÄR REDOVISNING5HAND1ING TILL SÖKANDEN I E-MÅL, Innehåller målnummer och personnummer	Innehåller iofs personuppgifter på gäldenärer där utredning avslutats, men informationen är inte känslig - kan inhämtas av vem som helst på legal väg.	2500
NUS	2012-03-20-00.38.15.380000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.AEA.G0078V00			0
NUS	2012-03-20-00.38.17.070000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.AI.G0289V00			17250
NUS	2012-03-20-00.38.18.380000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.AIS.G0407V00			19750
NUS	2012-03-20-00.38.19.640000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.AKA.G0140V00			7000
NUS	2012-03-20-00.38.20.850000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.ALA.G0114V00			750
NUS	2012-03-20-00.38.22.050000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.ASK.G0078V00			0
NUS	2012-03-20-00.38.23.320000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.BEA.G0076V00			0
NUS	2012-03-20-00.38.24.600000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.BYA.G0101V00			0
NUS	2012-03-20-00.38.25.850000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.CIS.G0446V00			0
NUS	2012-03-20-00.38.27.180000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.CLL.G0183V00			1250
NUS	2012-03-20-00.38.28.440000	RETR	192.16.143.2	93.186.170.54	D 44.EE52PROD.CSN.G 251V00			750
NUS	2012-03-20-00.38.29.640000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.EAR.G0071V00			0
NUS	2012-03-20-00.38.31.270000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.EFJ.G0643V00			0
NUS	2012-03-20-00.38.31.940000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.ERAP.G2021V00			0
NUS	2012-03-20-00.38.33.290000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.FAA.G0121V00			500
NUS	2012-03-20-00.38.34.490000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.FAK.G1027V00			0
NUS	2012-03-20-00.38.35.760000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.FAR.G0069V00			0
NUS	2012-03-20-00.38.36.910000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.FEI.G0009V00			0
NUS	2012-03-20-00.38.38.230000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.FFC.G0623V00			1000
NUS	2012-03-20-00.38.39.430000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.FFS.G0074V00			0
NUS	2012-03-20-00.38.39.710000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.FILOMBUD			2592
NUS	2012-03-20-00.38.41.020	RETR	192.16.143.2	93.186.170.54	D 44.EE52PROD.FK.G0358V00			0
NUS	2012-03-20-00.38.42.330000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.FLF.G0101V00			1000
NUS	2012-03-20-00.38.43.570000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.FSA.G0114V00			0
NUS	2012-03-20-00.38.44.830000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.FTA.G0070V00			0
NUS	2012-03-20-00.38.46.090000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.GSA.G0080V00			0
NUS	2012-03-20-00.38.47.460000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.GTI.G0105V00			11500
NUS	2012-03-20-00.38.48.620000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.HAA.G0074V00			0
NUS	2012-03-20-00.38.49.940000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.HDS.G0080V00			3000
NUS	2012-03-20-00.38.51.170000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.HRA.G0070V00			0
NUS	2012-03-20-00.38.52.430000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.IFM.G0075V00			0
NUS	2012-03-20-00.38.53.690000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.JAK.G0079V00			0
NUS	2012-03-20-00.38.55.220000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.JIS.G0840V00			144000
NUS	2012-03-20-00.38.55.350000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.JJS.G0239V00			0
NUS	2012-03-20-00.38.56.740000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.JUG.G0626V00			55250
NUS	2012-03-20-00.38.57.890000	RETR	192.16.143.2	93.186.170.54	D 44.EE52PROD.KAH.G0070V00			0

NUS	2012-03-20-00.38.59.180000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.KDE.G0317V00			750
NUS	2012-03-20-00.39.00.550000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.KDI.G0482V00			19000
NUS	2012-03-20-00.39.01.930000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.KHS.G0780V00			81750
NUS	2012-03-20-00.39.03.230000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.KI.G0871V00			11500
NUS	2012-03-20-00.39.04.520000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.KTJ.G0385V00			10750
NUS	2012-03-20-00.39.05.690000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.LEK.G0079V00			0
NUS	2012-03-20-00.39.06.930000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.LIK.G0071V00			0
NUS	2012-03-20-00.39.08.230000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.LIN.G0386V00			0
NUS	2012-03-20-00.39.09.470000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.LRA.G0069V00			0
NUS	2012-03-20-00.39.11.000000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.LSA.G0114V00			138250
NUS	2012-03-20-00.39.12.150000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.MUS.G0070V00			0
NUS	2012-03-20-00.39.13.400000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.NMI.G0021V00			0
NUS	2012-03-20-00.39.14.650000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.NOJ.G0029V00			0
NUS	2012-03-20-00.39.15.890000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.PAK.G0069V00			0
NUS	2012-03-20-00.39.17.270000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.PIS.G0683V00			30000
NUS	2012-03-20-00.39.18.600000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.PRI.G1026V00			33500
NUS	2012-03-20-00.39.19.770000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.PRO.G0043V00			0
NUS	2012-03-20-00.39.21.040000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.PTJ.G0407V00			0
NUS	2012-03-20-00.39.22.350000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.RF.G0062V00			3750
NUS	2012-03-20-00.39.23.570000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.SAA.G0076V00			0
NUS	2012-03-20-00.39.24.810000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.SAK.G0114V00			0
NUS	2012-03-20-00.39.26.080000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.SEI.G1020V00			0
NUS	2012-03-20-00.39.27.390000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.SEK.G0745V00			3000
NUS	2012-03-20-00.39.28.620000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.SHA.G0079V00			0
NUS	2012-03-20-00.39.30.110000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.SIB.G0492V00			146000
NUS	2012-03-20-00.39.31.300000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.SJK.G0076V00			0
NUS	2012-03-20-00.39.32.750000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.SKT.G0528V00			31750
NUS	2012-03-20-00.39.33.920000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.SLK.G0071V00			0
NUS	2012-03-20-00.39.35.260000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.SRK.G0366V00			6500
NUS	2012-03-20-00.39.36.470000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.STJ.G0074V00			500
NUS	2012-03-20-00.39.37.710000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.STL.G0114V00			500
NUS	2012-03-20-00.39.38.920000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.TEA.G0069V00			0
NUS	2012-03-20-00.39.40.180000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.TFF.G0825V00			0
NUS	2012-03-20-00.39.41.420000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.TRA.G0075V00			0
NUS	2012-03-20-00.39.42.740000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.UNA.G0073V00			3250
NUS	2012-03-20-00.39.44.030000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.UNC.G0549V00			6750
NUS	2012-03-20-00.39.45.320000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.VI.G0616V00			20000
NUS	2012-03-20-00.39.46.480000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.VOK.G0528V00			0
NUS	2012-03-20-00.39.47.740000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.VOX.G0221V00			0
NUS	2012-03-20-00.39.48.890000	RETR	192.16.143.2	93.186.170.54	D044.EE52PROD.WAS.G0009V00			0
NUS	2012-03-20-00.41.20.630000	RETR	192.16.143.2	93.186.170.54	D044.EE93PROD.INIT.G2158V00	Tomfil		0
NUS	2012-03-20-00.41.20.860000	RETR	192.16.143.2	93.186.170.54	D044.EE93PROD.INIT.G2159V00	Tomfil		0
NUS	2012-03-20-00.47.32.300000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.EE30.G1938V00	Registrering av nya mål i XTRA. Oläslig info för utomstående	Ointressant innehåll	43120
NUS	2012-03-20-00.47.32.470000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.EE30.G1939V00			1232
NUS	2012-03-20-00.47.32.700000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.EE30.G1940V00			5544
NUS	2012-03-20-00.47.33.270000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.EE30.G1941V00			805728
NUS	2012-03-20-00.47.33.500000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.EE30.G1942V00			19712
NUS	2012-03-20-00.47.33.970000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.EE30.G1943V00			407176

NUS	2012-03-20-00.47.34.410000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.EE30.G1944V00			266112
NUS	2012-03-20-00.47.34.580000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.EE30.G1945V00			3696
NUS	2012-03-20-00.47.34.930000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.EE30.G1946V00			74536
NUS	2012-03-20-00.47.35.180000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.EE30.G1947V00			16016
NUS	2012-03-20-00.47.40.460000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.E30EMAL.G8992V00	Registrering av nya mål i XTRA. Oläslig info för utomstående	Ointressant innehåll	3086160
NUS	2012-03-20-00.47.42.720000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.E30EMAL.G8993V00			3352272
NUS	2012-03-20-00.47.48.730000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.E30EMAL.G8994V00			3355968
NUS	2012-03-20-00.47.54.860000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.E30EMAL.G8995V00			3430504
NUS	2012-03-20-00.48.02.810000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.E30EMAL.G8996V00			3446520
NUS	2012-03-20-00.48.36.560000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.FELLISTA.G7985V00	Ointressant, innehåller endast info om något gått vilket händer väldigt sällan	Ointressant innehåll	133
NUS	2012-03-20-00.48.38.930000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.FILKOLL.G1946V00	Filkoll för ingivareombud, ombkod, löpnr, senaste körningsdatum	Ointressant innehåll	1560
NUS	2012-03-20-00.48.41.100000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.LOGG.G7973V00	Logguppgifter vid kontroll av E-målsfil, inga personuppgifter	Ointressant innehåll	3990
NUS	2012-03-20-00.48.41.430000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.LOGG.G7975V00			3990
NUS	2012-03-20-00.48.42.420000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.LOGG.G7983V00			3990
NUS	2012-03-20-00.48.42.770000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.LOGG.G7985V00			3990
NUS	2012-03-20-00.48.43.050000	RETR	192.16.143.2	93.186.170.54	D044.E30EPROD.TOM	Tomfil		0
NUS	2012-03-20-00.50.04.870000	RETR	192.16.143.2	93.186.170.54	/web/websrv/conf/httpd.conf			24117
NUS	2012-03-20-00.50.11.970000	RETR	192.16.143.2	93.186.170.54	/web/websrv/cgi-bin/test.sh			443
NUS	2012-03-20-00.50.13.690000	RETR	192.16.143.2	93.186.170.54	/web/websrv/cgi-bin/XMNWEB			81920
NUS	2012-03-20-00.50.19.830000	RETR	192.16.143.2	93.186.170.54	/web/websrv/pub/index.html			70
NUS	2012-03-20-00.53.09.950000	RETR	192.16.143.2	93.186.170.54	D044.E60EPROD.KTJ.G0383V00	Tomfil		0
NUS	2012-03-20-00.55.12.630000	RETR	192.16.143.2	93.186.170.54	D044.FINANS.CINBETAL.G2220V00	Inbetalningsfil från Plusgiro till Supro	Enbart information om gjorda inbetalningar. Pengarna har redan kommit in.	1360
NUS	2012-03-20-00.55.12.860000	RETR	192.16.143.2	93.186.170.54	D044.FINANS.CINBETAL.G2221V00			880
NUS	2012-03-20-00.55.23.070000	RETR	192.16.143.2	93.186.170.54	/usr/lpp/cicsts/cicsts32/dafcicp9/wsdl/kfmpe			2147
NUS	2012-03-20-00.55.26.590000	RETR	192.16.143.2	93.186.170.54	/usr/lpp/cicsts/cicsts32/dafcicp9/wsdl/kfmpe			2147
NUS	2012-03-20-00.56.12.350000	RETR	192.16.143.2	93.186.170.54	/usr/lpp/cicsts/cicsts32/dafcicp9/wsdl/kfmpe			2147
NUS	2012-03-20-00.57.03.060000	RETR	192.16.143.2	93.186.170.54	/usr/lpp/cicsts/cicsts32/dafcicp9/config/sps			265
NUS	2012-03-20-00.57.09.150000	RETR	192.16.143.2	93.186.170.54	/usr/lpp/cicsts/cicsts32/dafcicp9/config/sps			274
NUS	2012-03-20-00.58.01.500000	RETR	192.16.143.2	93.186.170.54	/usr/lpp/cicsts/cicsts32/dafcicp9/wsbind/req			4208
NUS	2012-03-20-01.08.09.980000	RETR	192.16.143.2	93.186.170.54	D044.Y66JPROD.BINDSPAR.G5031V00	Intern bindfil vid programflytt. Ointressant	Ointressant innehåll	3034
NUS	2012-03-20-01.18.58.940000	RETR	192.16.143.2	93.186.170.54	D044.GE42PROD.SIGILL	Sigill för utbetalningar till Swebank	Se vidare beskrivning i PM	80
NUS	2012-03-20-01.18.59.150000	RETR	192.16.143.2	93.186.170.54	D044.GE42PROD.SIGILL.OLD	Gammalt (föregående) Sigill för utbetalningar till Swebank		80
NUS	2012-03-20-01.19.00.790000	RETR	192.16.143.2	93.186.170.54	D044.GE42PROD.SWBSIGB.G0012V00	Utbetalningsfil till Swebank		91080
NUS	2012-03-20-01.19.01.400000	RETR	192.16.143.2	93.186.170.54	D044.GE42PROD.SWBSIGB.G0013V00	Utbetalningsfil till Swebank		331020
NUS	2012-03-20-01.19.04.940000	RETR	192.16.143.2	93.186.170.54	D044.GE42PROD.SWBSIGB.KOPIA.G0966V0	Utbetalningsfil till Swebank		91080
NUS	2012-03-20-01.19.05.360000	RETR	192.16.143.2	93.186.170.54	D044.GE42PROD.SWBSIGB.KOPIA.G0967V0	Utbetalningsfil till Swebank		331020
NUS	2012-03-20-01.21.31.530000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.AKRED.G0013V00	Underlag för utbetalningsfiler till PG	Intern flyttning av pengar. Ingen risk att pengar kan försvinna	61790
NUS	2012-03-20-01.21.33.220000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.LKFMFIL.G0012V00			334180
NUS	2012-03-20-01.21.36.540000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.LKFMFIL.G0013V00			6082560

NUS	2012-03-20- 1.21.38.020000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.OREFIL.G0012V00			6201
NUS	2012-03-20-01.21.38.270000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.OREFIL.G0013V00			18073
NUS	2012-03-20-01.22.07.420000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.RFVFIL.G3729V00			560
NUS	2012-03-20-01.22.07.660000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.RFVFIL.G3730V00			1050
NUS	2012-03-20-01.22.12.200000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.SEKV.G3730V00			75
NUS	2012-03-20-01.22.12.420000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.SEKV.G3731V00			75
NUS	2012-03-20-01.22.19.150000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.SWEDBANK.G1410V00			0
NUS	2012-03-20-01.22.19.600000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.SWEDBANK.G1411V00			137060
NUS	2012-03-20-01.22.19.720000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.SWEDBANK.G1412V00			0
NUS	2012-03-20-01.22.46.170000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.UT ETE.G0013V00			34586784
NUS	2012-03-20-01.23.30.610000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.UTBETEL.G0013V00			74212000
NUS	2012-03-20-01.23.34.630000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.UTBETEZ.G3842V00			2385390
NUS	2012-03-20-01.23.36.310000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.UTBL2046.G0012V00			219345
NUS	2012-03-20-01.23.43.930000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.UTBL2046.G0013V00			3927210
NUS	2012-03-20-01.23.55.130000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.UTBL2047.G1971V00			9310875
NUS	2012-03-20-01.24.01.070000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.UTBL2049.G1970V00			210840
NUS	2012-03-20-01.24.05.950000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.UTBL2049.G1971V00			3182655
NUS	2012-03-20-01.24.20.990000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.UTBL2054.G1970V00			341565
NUS	2012-03-20-01.24.27.090000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.UTBL2054.G1971V00			7382235
NUS	2012-03-20-01.24.40.280000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.UTBL2055.G1971V00			10783080
NUS	2012-03-20-01.24.48.860000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.UTB45583.G1970V00			735
NUS	2012-03-20-01.24.49.080000	RETR	192.16.143.2	93.186.170.54	D044.GE50PROD.UTB45583.G1971V00			735
NUS	2012-03-20-01.30.01.510000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.PGUTB.G6130V00			4921
NUS	2012-03-20-01.30.01.750000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.PGUTB.G6131V00			4123
NUS	2012-03-20-01.30.01.980000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.PGUTB.G6132V00			4921
NUS	2012-03-20-01.30.02.210000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.PGUTB.G6133V00			4921
NUS	2012-03-20-01.30.02.460000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.PGUTB.G6134V00			4921
NUS	2012-03-20-01.30.02.710000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.PGUTB.G6135V00			4921
NUS	2012-03-20-01.30.02.990000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.PGUTB.G6136V00			4921
NUS	2012-03-20-01.30.04.900000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.UTBETEB.G0012V00			914900
NUS	2012-03-20-01.30.18.8200 0	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.UTBETEB.G0013V00			25128400
NUS	2012-03-20-01.30.20.460000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.UTBL2046.G0012V00			130600
NUS	2012-03-20-01.30.23.11000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.UTBL2046.G0013V00			2869500
NUS	2012-03-20-01.30.26.170000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.UTBL2047.G1970V00			247500
NUS	2012-03-20-01.30.32.030000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.UTBL2047.G1971V00			6761600
NUS	2012-03-20-01.30.37.960000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.UTBL2049.G1970V00			125800
NUS	2012-03-20-01.30.40.880000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.UTBL2049.G1971V00			2320800
NUS	2012-03-20-01.30.55.540000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.UTBL2054.G1970V00			209100
NUS	2012-03-20-01.31.01.580000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.UTBL2054.G1971V00			5405200
NUS	2012-03-20-01.31.04.640000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.UTBL2055.G1970V00			201800
NUS	2012-03-20-01.31.09.050000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.UTBL2055.G1971V00			7771200
NUS	2012-03-20-01.31.17.670000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.UTB45583.G1970V00			100
NUS	2012-03-20-01.31.17.900000	RETR	192.16.143.2	93.186.170.54	D044.GE51PROD.UTB45583.G1971V00			100
NUS	2012-03-20-01.32.31.300000	RETR	192.16.143.2	93.186.170.54	D044.GE52PROD.POSTGIR.KNR45583.TEMP.G1971V00			200
NUS	2012-03-20-01.32.38.150000	RETR	192.16.143.2	93.186.170.54	D044.GE52PROD.POSTGIRO.L2046.TEMP.G2003V00			2869600
NUS	2012-03-20-01.32.43.770000	RETR	192.16.143.2	93.186.170.54	D044.GE52PROD.POSTGIRO.L2047.TEMP.G1971V00			6761700
NUS	2012-03-20-01.32.47.230000	RETR	192.16.143.2	93.186.170.54	D044.GE52PROD.POSTGIRO.L2049.TEMP.G1971V00			2320900
NUS	2012-03-20-01.32.51.200000	RETR	192.16.143.2	93.186.170.54	D044.GE52PROD.POSTGIRO.L2054.TEMP.G1973V00			5405300
NUS	2012-03-20-01.32.59.070000	RETR	192.16.143.2	93.186.170.54	D044.GE52PROD.POSTGIRO.L2055.TEMP.G1971V00			7771300

NUS	2012-03-20-01.33.01.090000	RETR	192.16.143.2	93.186.170.54	D044.GE58PROD.SWBUT.G0012V00			90720
NUS	2012-03-20-01.33.01.570000	RETR	192.16.143.2	93.186.170.54	D044.GE58PROD.SWBUT.G0013V00			330660
NUS	2012-03-20-01.33.05.120000	RETR	192.16.143.2	93.186.170.54	D044.GE58PROD.SWBUT.KOPIA.G0965V00			90720
NUS	2012-03-20-01.33.05.590000	RETR	192.16.143.2	93.186.170.54	D044.GE58PROD.SWBUT.KOPIA.G0966V00			330660
NUS	2012-03-20-01.33.09.060000	RETR	192.16.143.2	93.186.170.54	D044.GE59PROD.DEBBMUT.G0012V00			3440
NUS	2012-03-20-01.33.09.290000	RETR	192.16.143.2	93.186.170.54	D044.GE59PROD.DEBBMUT.G0013V00			3440
NUS	2012-03-20-01.34.50.940000	RETR	192.16.143.2	93.186.170.54	D044.GE70PROD.UTBETEL.G0013V00			47158368
NUS	2012-03-20-01.34.57.210000	RETR	192.16.143.2	93.186.170.54	D044.GE71PROD.LKFML.G0013V00			39501
NUS	2012-03-20-01.36.11.720000	RETR	192.16.143.2	93.186.170.54	D044.GE72PROD.OREL.G0012V00			21147
NUS	2012-03-20-01.36.12.020000	RETR	192.16.143.2	93.186.170.54	D044.GE72PROD.OREL.G0013V00			54264
NUS	2012-03-20-01.36.17.600000	RETR	192.16.143.2	93.186.170.54	D044.GE75PROD.KTOT2046.G0033V00			47775
NUS	2012-03-20-01.36.21.390000	RETR	192.16.143.2	93.186.170.54	D044.GE75PROD.KTOT2047.G0033V00			169680
NUS	2012-03-20-01.36.25.170000	RETR	192.16.143.2	93.186.170.54	D044.GE75PROD.KTOT2049.G0033V00			187425
NUS	2012-03-20-01.36.28.820000	RETR	192.16.143.2	93.186.170.54	D044.GE75PROD.KTOT2054.G0033V00			47250
NUS	2012-03-20-01.36.32.550000	RETR	192.16.143.2	93.186.170.54	D044.GE75PROD.KTOT2055.G0033V00			126000
NUS	2012-03-20-01.36.36.030000	RETR	192.16.143.2	93.186.170.54	D044.GE75PROD.KTO45583.G0033V00	Tomfil		0
NUS	2012-03-20-02.34.20.930000	RETR	192.16.143.2	93.186.170.54	D610.SPARHSM.DAFA.D610.ML1	Tomfil		0
NUS	2012-03-20-04.20.37.570000	RETR	192.16.143.2	93.186.170.54	D044.IB10PROD.LOGG.G1963V00	Loggfil 2pc-logg, ointressant, internt bruk	Ointressant innehåll	2527
NUS	2012-03-20-04.20.37.800000	RETR	192.16.143.2	93.186.170.54	D044.IB10PROD.LOGG.G1964V00	Loggfil 2pc-logg, ointressant, internt bruk	Ointressant innehåll	2527
NUS	2012-03-20-04.20.43.430000	RETR	192.16.143.2	93.186.170.54	D044.IB10PROD.UTFIL.G1963V00	Tomfil		0
NUS	2012-03-20-04.20.43.670000	RETR	192.16.143.2	93.186.170.54	D044.IB10PROD.UTFIL.G1964V00	Tomfil		0
NUS	2012-03-20-04.21.25.960000	RETR	192.16.143.2	93.186.170.54	D044.IB20PROD.INITFIL.G1375V00	FIL TILL INIT MED SIGNAL OM NÄR ALL MÅL I ETT UTMÄTNINGSBESLUT GJORT AV INIT BLIVIT NOLLADE. Innehåller pnr	Ointressant innehåll	27690
NUS	2012-03-20-04.21.26.250000	RETR	192.16.143.2	93.186.170.54	D044.IB20PROD.INITFIL.G1376V00	FIL TILL INIT MED SIGNAL OM NÄR ALL MÅL I ETT UTMÄTNINGSBESLUT GJORT AV INIT BLIVIT NOLLADE. Innehåller pnr	Ointressant innehåll	28184
NUS	2012-03-20-04.21.28.620000	RETR	192.16.143.2	93.186.170.54	D044.IB21PROD.FELLISTA.G0228V00	fellista, ointressant	Ointressant innehåll	532
NUS	2012-03-20-04.21.34.150000	RETR	192.16.143.2	93.186.170.54	D044.IB21PROD.LOGG.G0228V00	Logg med antalsuppgifter, ointressant	Ointressant innehåll	1596
NUS	2012-03-20-04.21.34.950000	RETR	192.16.143.2	93.186.170.54	D044.IB21PROD.PARM.G0228V00	Parameterkort med datum	Ointressant innehåll	20
NUS	2012-03-20-04.21.40.050000	RETR	192.16.143.2	93.186.170.54	D044.IB22PROD.LOGG.G0229V00	Körlogg, oimressant	Ointressant innehåll	1197
NUS	2012-03-20-04.21.43.850000	RETR	192.16.143.2	93.186.170.54	D044.I823PROD.INITFIL.G0499V00	Rapportfil till Init med packade pnr (59(comp-3))	Visserligen personuppgifter (packade) men inga känsliga uppgifter i övrigt.	2184
NUS	2012-03-20-04.21.47.390000	RETR	192.16.143.2	93.186.170.54	D044.I823PROD.RAPPFIL.G0499V00	Tomfil		0
NUS	2012-03-20-04.21.49.150000	RETR	192.16.143.2	93.186.170.54	D044.I824PROD.INITFIL.G0013V00	Signalfil till Init, pnr i klartext	Visserligen personuppgifter (packade) men inga känsliga uppgifter i övrigt.	3944

NUS	2012-03-20-04.22.29.290000	RETR	192.16.143.2	93.186.170.54	D044.IB25PROD.INITKRAV.G0398V00	XML-fil till Init med kravposter, pnr, namn, adress, skuld m.m.	Daglig fil med uppgift om vilka udnerrättelser som skaskapas på nya mål - Informationen är inte känslig, men bad will om det blir känt att den är på vift.	55995152
NUS	2012-03-20-04.22.30.400000	RETR	192.16.143.2	93.186.170.54	D044.IB25PROD.PARM.G0399V00			80
NUS	2012-03-20-04.22.30.640000	RETR	192.16.143.2	93.186.170.54	D044.IB25PROD.PARM.G0400V00			80
NUS	2012-03-20-08.15.55.470000	RETR	192.16.143.2	93.186.170.54	E077.CERTNAVP			2566
NUS	2012-03-20-08.21.06.050000	RETR	192.16.143.2	93.186.170.54	E077.NAVET.SRCE			160
NUS	2012-03-20-08.21.06.300000	RETR	192.16.143.2	93.186.170.54	E077.NAVET.SRCE			1760
NUS	2012-03-20-08.21.06.540000	RETR	192.16.143.2	93.186.170.54	E077.NAVET.SRCE			1920
NUS	2012-03-20-08.21.06.790000	RETR	192.16.143.2	93.186.170.54	E077.NAVET.SRCE			1920
NUS	2012-03-20-08.21.07.080000	RETR	192.16.143.2	93.186.170.54	E077.NAVET.SRCE			10240
NUS	2012-03-20-08.21.07.470000	RETR	192.16.143.2	93.186.170.54	E077.NAVET.SRCE			53840
NUS	2012-03-20-08.21.07.800000	RETR	192.16.143.2	93.186.170.54	E077.NAVET.SRCE			33280
NUS	2012-03-20-08.21.08.140000	RETR	192.16.143.2	93.186.170.54	E077.NAVET.SRCE			29920
NUS	2012-03-20-08.21.08.510000	RETR	192.16.143.2	93.186.170.54	E077.NAVET.SRCE			79120
NUS	2012-03-20-08.21.08.760000	RETR	192.16.143.2	93.186.170.54	E077.NAVET.SRCE			240
NUS	2012-03-20-08.33.29.380000	RETR	192.16.143.2	93.186.170.54	E077.WMBEBRR.CERT.P12			2566
NUS	2012-03-20-08.35.25.450000	RETR	192.16.143.2	93.186.170.54	E077.WMBEBRR.CERT.EXP2			0
NUS	2012-03-20-08.35.25.730000	RETR	192.16.143.2	93.186.170.54	E077.WMBEBRR.CERT.P12			2566
NUS	2012-03-20-08.36.32.960000	RETR	192.16.143.2	93.186.170.54	E077.WMBEBRR.CERTCA.TXT			3584
NUS	2012-03-20-08.36.33.980000	RETR	192.16.143.2	93.186.170.54	E077.WMBEBRR.CERTCA.VB			1704
NUS	2012-03-20-08.36.34.510000	RETR	192.16.143.2	93.186.170.54	E077.WMBEBRR.CERTCAI.VB			1700
NUS	2012-03-20-08.36.35.030000	RETR	192.16.143.2	93.186.170.54	E077.WMBEBRR.CERTCAS.VB			2080
NUS	2012-03-20-08.36.35.580000	RETR	192.16.143.2	93.186.170.54	E077.WMBEBRR.CERTCA1			5376
NUS	2012-03-20-08.36.36.140000	RETR	192.16.143.2	93.186.170.54	E077.WMBEBRR.CERTCA1.CERTPZO1.TXT			2816
NUS	2012-03-20-08.36.36.950000	RETR	192.16.143.2	93.186.170.54	E077.WMBEBRR.CERTCA1.CERTPZ●1.VB			1288
NUS	2012-03-20-08.37.37.270000	RETR	192.16.143.2	93.186.170.54	E077.WMBEBRR.CERTPNAV.VB			1200
NUS	2012-03-20-08.38.27.550000	RETR	192.16.143.2	93.186.170.54	E077.WMBEBRR.CERTPNAV.VB.NEW			1200
NUS	2012-03-20-08.38.28.090000	RETR	192.16.143.2	93.186.170.54	E077.WMBEBRR.CERTPNAV.VB.OLD			1108
NUS	2012-03-20-09.26.54.170000	RETR	192.16.143.2	93.186.170.54	D044.KOP2PROD.LOGG			13107
NUS	2012-03-20-09.36.43.370000	RETR	192.16.143.2	93.186.170.54	D044.LE65PROD.BLANKETT.G5469V00			4850000
NUS	2012-03-20-09.36.53.030000	RETR	192.16.143.2	93.186.170.54	D044.LE65PROD.INITAVI.G0358V00			11254800
NUS	2012-03-20-09.36.57.150000	RETR	192.16.143.2	93.186.170.54	D044.LE65PROD.LRAP.G5589V00			0
NUS	2012-03-20-09.37.05.940000	RETR	192.16.143.2	93.186.170.54	D044.LE66PROD.BLANKE .G3961V00			7966000
NUS	2012-03-20-10.16.31.230000	RETR	192.16.143.2	93.186.170.54	/tmp/../D955.ARON.BTL.BINAVT04			30691
NUS	2012-03-20-10.16.31.460000	RETR	192.16.143.2	93.186.170.54	/tmp/../D955.ARON.BTL.NAV05			860
NUS	2012-03-20-10.16.31.670000	RETR	192.16.143.2	93.186.170.54	/tmp/../D955.ARON.BTL.NAV09			538
NUS	2012-03-20-10.16.31.890000	RETR	192.16.143.2	93.186.170.54	/tmp/../D955.DAF1367.NAVETT.READREAD			2756
NUS	2012-03-20-10.16.34.230000	RETR	192.16.143.2	93.186.170.54	/tmp/../D955.NAV.KONTLIST			1932557
NUS	2012-03-20-10.16.39.030000	RETR	192.16.143.2	93.186.170.54	/tmp/../D955.NAV.KONTLIST.D080704			3124176
NUS	2012-03-20-10.16.40.710000	RETR	192.16.143.2	93.186.170.54	/tmp/../D955.NAV.KONTLIST.G25			1992289
NUS	2012-03-20-10.16.41.010000	RETR	192.16.143.2	93.186.170.54	/tmp/../D955.R5V.NAVET.G25V0●			20124
NUS	2012-03-20-11.07.50.700000	RETR	192.16.143.2	93.186.170.54	D044.N57SPROD.INITFIL.G3717V00			0
NUS	2012-03-20-11.07.51.100000	RETR	192.16.143.2	93.186.170.54	D044.N57SPROD.INITFIL.G3718V00			40688
NUS	2012-03-20-11.07.51.240000	RETR	192.16.143.2	93.186.170.54	D044.N57SPROD.INITFIL.G3719V00			0
NUS	2012-03-20-11.07.52.380000	RETR	192.16.143.2	93.186.170.54	D044.N57SPROD.NRAP.G3756V00			0
NUS	2012-03-20-11.07.52.640000	RETR	192.16.143.2	93.186.170.54	D044.N57SPROD.NRAP.G3757V00			0

NUS	2012-03-20-11.07.52.860000	RETR	192.16.143.2	93.186.170.54	D044.N57SPROD.NRAP.G3758V00			0
NUS	2012-03-20-11.07.54.290000	RETR	192.16.143.2	93.186.170.54	D044.N57SPROD.PARM.G1063V00			20
NUS	2012-03-20-11.07.54.560000	RETR	192.16.143.2	93.186.170.54	D044.N57SPROD.PARM.G1064V00			20
NUS	2012-03-20-11.07.56.170000	RETR	192.16.143.2	93.186.170.54	D044.N57SPROD.STATFIL.G0012V00			80
NUS	2012-03-20-11.07.56.400000	RETR	192.16.143.2	93.186.170.54	D044.N57SPROD.STATFIL.G0013V00			80
NUS	2012-03-20-11.53.30.080000	RETR	192.16.143.2	93.186.170.54	D044.O714PROD.GELDAR.G0016V00			37264224
NUS	2012-03-20-11.53.33.860000	RETR	192.16.143.2	93.186.170.54	D044.O715PROD.O715PARM.G3555V00			80
NUS	2012-03-20-11.53.34.080000	RETR	192.16.143.2	93.186.170.54	D044.O715PROD.O715PARM.G3556V00			80
NUS	2012-03-20-11.53.40.030000	RETR	192.16.143.2	93.186.170.54	D044.O718PROD.SJVFIL.G2583V00			13440
NUS	2012-03-20-11.53.40.200000	RETR	192.16.143.2	93.186.170.54	D044.O718PROD.SJVKOLL			80
NUS	2012-03-20-11.57.15.580000	RETR	192.16.143.2	93.186.170.54	D044.O90WPROD.GELD.G1545V00	O90U-O94Ufiler innehåller hasch värden med personnummer i packat format (59-comp-3) för uttag av gäldenärsinformation. O90W - O94W innehåller gäldenärsinformation till Winit	Se skrivning i PM	357913600
NUS	2012-03-20-12.00.28.260000	RETR	192.16.143.2	93.186.170.54	D044.O90WPROD.GELD.G1546V00			357925376
NUS	2012-03-20-12.03.43.910000	RETR	192.16.143.2	93.186.170.54	D044.O90WPROD.GELD.G1547V00			357925376
NUS	2012-03-20-12.03.45.930000	RETR	192.16.143.2	93.186.170.54	D044.O91WPROD.GRAS			2982720
NUS	2012-03-20-12.03.46.100000	RETR	192.16.143.2	93.186.170.54	D044.O91WPROD.GRA1S			0
NUS	2012-03-20-12.04.26.650000	RETR	192.16.143.2	93.186.170.54	D044.O91WPROD.GRBS			61832128
NUS	2012-03-20-12.04.28.980000	RETR	192.16.143.2	93.186.170.54	D044.O91WPROD.GRCS			3203720
NUS	2012-03-20-12.06.11.930000	RETR	192.16.143.2	93.186.170.54	D044.O91WPROD.GRDS			173874608
NUS	2012-03-20-12.07.09.960000	RETR	192.16.143.2	93.186.170.54	D044.O91WPROD.GRES			94520656
NUS	2012-03-20-12.08.03.060000	RETR	192.16.143.2	93.186.170.54	D044.O92WPROD.GTAS.G1545V00			86701296
NUS	2012-03-20-12.08.49.970000	RETR	192.16.143.2	93.186.170.54	D044.O92WPROD.GTAS.G1546V00			86705584
NUS	2012-03-20-12.09.40.320000	RETR	192.16.143.2	93.186.170.54	D044.O92WPROD.GTAS.G1547V00			86707536
NUS	2012-03-20-12.10.34.350000	RETR	192.16.143.2	93.186.170.54	D044.O92WPROD.GTASF.G0755V00			86707536
NUS	2012-03-20-12.10.34.860000	RETR	192.16.143.2	93.186.170.54	D044.O92WPROD.GTBS.G1545V00			16480
NUS	2012-03-20-12.10.35.140000	RETR	192.16.143.2	93.186.170.54	D044.O92WPROD.GTBS.G1546V00			16480
NUS	2012-03-20-12.10.35.410000	RETR	192.16.143.2	93.186.170.54	D044.O92WPROD.GTBS.G1547V00			16640
NUS	2012-03-20-12.10.35.840000	RETR	192.16.143.2	93.186.170.54	D044.O92WPROD.GTBSF.G0755V00			400
NUS	2012-03-20-12.13.56.150000	RETR	192.16.143.2	93.186.170.54	D044.O93UPROD.SKULD.G1545V00			367519744
NUS	2012-03-20-12.17.18.360000	RETR	192.16.143.2	93.186.170.54	D044.O93UPROD.SKULD.G1546V00			367519744
NUS	2012-03-20-12.20.50.100000	RETR	192.16.143.2	93.186.170.54	D044.O93UPROD.SKULD.G1547V00			367519744
NUS	2012-03-20-12.20.50.860000	RETR	192.16.143.2	93.186.170.54	D044.O93VPROD.SKULDUT.G0756V00			648040
NUS	2012-03-20-12.20.51.130000	RETR	192.16.143.2	93.186.170.54	D044.O93WPROD.A1S			14941
NUS	2012-03-20-12.20.51.390000	RETR	192.16.143.2	93.186.170.54	D044.O93WPROD.A1SX			12730
NUS	2012-03-20-12.20.51.650000	RETR	192.16.143.2	93.186.170.54	D044.O93WPROD.A1SY			13333
NUS	2012-03-20-12.20.53.780000	RETR	192.16.143.2	93.186.170.54	D044.O93WPROD.A2S			2772120
NUS	2012-03-20-12.20.56.270000	RETR	192.16.143.2	93.186.170.54	D044.O93WPROD.A2SX			2725120
NUS	2012-03-20-12.20.58.900000	RETR	192.16.143.2	93.186.170.54	D044.O93WPROD.A2SY			2700160
NUS	2012-03-20-12.21.45.210000	RETR	192.16.143.2	93.186.170.54	D044.O93WPROD.SKTS			76449280
NUS	2012-03-20-12.22.35.630000	RETR	192.16.143.2	93.186.170.54	D044.O93WPROD.SKTSX			80411232
NUS	2012-03-20-12.23.19.150000	RETR	192.16.143.2	93.186.170.54	D044.O93WPROD.SKTSY			77113152
NUS	2012-03-20-12.30.27.890000	RETR	192.16.143.2	93.186.170.54	D044.O93WPROD.SKUS			761394944
NUS	2012-03-20-12.37.54.080000	RETR	192.16.143.2	93.186.170.54	D044.O93WPROD.SKUSX			765579776
NUS	2012-03-20-12.44.38.400000	RETR	192.16.143.2	93.186.170.54	D044.O93WPROD.SKUSY			743000832
NUS	2012-03-20-12.52.51.520000	RETR	192.16.143.2	93.186.170.54	D044.O93WPROD.SR1S			763511552

NUS	2012-03-20-13.00.56.520000	RETR	192.16.143.2	93.186.170.54	D044.O93WPROD.SR1SX			761029888
NUS	2012-03-20-13.08.09.790000	RETR	192.16.143.2	93.186.170.54	D044.O93WPROD.SR1SY			743078912
NUS	2012-03-20-13.08.11.690000	RETR	192.16.143.2	93.186.170.54	D044.O93WPROD.SR2S			2024820
NUS	2012-03-20-13.08.16.100000	RETR	192.16.143.2	93.186.170.54	D044.O93WPROD.SR2SX			1966230
NUS	2012-03-20-13.08.18.130000	RETR	192.16.143.2	93.186.170.54	D044.O93WPROD.SR2SY			1908340
NUS	2012-03-20-13.08.46.750000	RETR	192.16.143.2	93.186.170.54	D044.O94UPROD.EMAL.G1542V00			35399968
NUS	2012-03-20-13.09.08.250000	RETR	192.16.143.2	93.186.170.54	D044.O94UPROD.EMAL.G1543V00			35417408
NUS	2012-03-20-13.09.32.610000	RETR	192.16.143.2	93.186.170.54	D044.O94UPROD.EMAL.G1544V00			35417408
NUS	2012-03-20-13.09.33.410000	RETR	192.16.143.2	93.186.170.54	D044.O94VPROD.EMALUT.G0755V00			503670
NUS	2012-03-20-13.12.00.160000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.EMLS			227902800
NUS	2012-03-20-13.12.05.160000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.EMLSF			5036700
NUS	2012-03-20-13.13.16.480000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.EMLSX			126096896
NUS	2012-03-20-13.13.16.630000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.EMLSY			0
NUS	2012-03-20-13.31.27.360000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ER1S			1929720064
NUS	2012-03-20-13.31.58.420000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ER1SF			44609024
NUS	2012-03-20-13.41.16.990000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ER1SX			1069690880
NUS	2012-03-20-13.41.17.150000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ER1SY			0
NUS	2012-03-20-13.41.36.540000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ER2S			27531248
NUS	2012-03-20-13.41.37.260000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ER2SF			1212640
NUS	2012-03-20-13.41.47.950000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ER2SX			15521616
NUS	2012-03-20-13.41.48.100000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ER2SY			0
NUS	2012-03-20-13.42.33.180000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ET1S			76010656
NUS	2012-03-20-13.42.34.540000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ET1SF			1717170
NUS	2012-03-20-13.43.01.010000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ET1SX			42040432
NUS	2012-03-20-13.43.01.150000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ET1SY			0
NUS	2012-03-20-13.45.13.580000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ET3S			227963056
NUS	2012-03-20-13.45.18.080000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ET3SF			5182275
NUS	2012-03-20-13.46.31.990000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ET3SX			126063872
NUS	2012-03-20-13.46.32.150000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ET3SY			0
NUS	2012-03-20-13.46.38.210000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ET5S			6160392
NUS	2012-03-20-13.46.38.620000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ET5SF			213304
NUS	2012-03-20-13.46.41.050000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ET5SX			3372432
NUS	2012-03-20-13.46.41.210000	RETR	192.16.143.2	93.186.170.54	D044.O94WPROD.ET5SY			0
NUS	2012-03-20-13.52.54.590000	RETR	192.16.143.2	93.186.170.54	D044.PROTEC.CINBETAL.G4807V00			880
NUS	2012-03-20-13.56.16.820000	RETR	192.16.143.2	93.186.170.54	D044.QN46PROD.BLANKETP.G2049V00			43435808
NUS	2012-03-20-14.02.22.090000	RETR	192.16.143.2	93.186.170.54	D044.Q49IPROD.PARM			80
NUS	2012-03-21-03.35.51.150000	RETR	192.16.143.2	93.186.170.54	D044.RS46PROD.KKSTAT.G0234V00			1716
NUS	2012-03-21-03.35.59.510000	RETR	192.16.143.2	93.186.170.54	D044.RS47PROD.LISTA.G0071V00			4640
NUS	2012-03-21-03.36.53.010000	RETR	192.16.143.2	93.186.170.54	D044.RS53PROD.RAPPFIL.G4810V00			0
NUS	2012-03-21-03.37.05.910000	RETR	192.16.143.2	93.186.170.54	D044.RS91PROD.DAGNR.G0848V00			11
NUS	2012-03-21-03.37.06.690000	RETR	192.16.143.2	93.186.170.54	D044.RS91PROD.SAN.G0851V00			120
NUS	2012-03-21-03.37.07.510000	RETR	192.16.143.2	93.186.170.54	D044.RS92PROD.LISTA.G0850V00			4292

logica

Status rapport 2010-02-19
Säkerhetsincident

Innehåll

Inledning

Säkerhetsincidenten kommer efter denna vecka att övergå från incidentprocessen till problemprocessen i vilken utredning kommer att drivas vidare.

Det akuta arbetet med att implementera en tillfällig lösning för att säkerställa den löpande produktionen har bara delvis lyckats. Tillkommande åtgärder redovisas sist i denna statusrapport.

Nedan summariska händelselogg lämnar många obesvarade frågor. Dessa kommer vi att söka förklaring till men det finns begränsningar för vad som är möjligt att belägga. Att kartlägga hur detta har gått till är viktigt för oss men kommer som prioritet 2 då vi i första hand nu lägger resurser på att säkerställa att det inte finns någon inbyggd trojan för eventuella framtida intrångsförsök.

Händelseförlopp

Nedan finns de tre viktigaste händelserna eller milstolparna, i denna säkerhetsincident beskrivna. Utan att ha kommit igenom hela utredningsmaterialet har dock nedanstående utkristalliserats men kan komma att omvärderas när mer fakta läggs till.

29/1 tankas systemet via FTP på information, ett antal dataset kopieras till okänd slutadress. Användaridentiteten som användes för detta hade vid tillfället rätt behörighet och ett giltigt lösenord. Användaren använde vid detta tillfälle "NYTTPW"-funktionen för att kvittera ut giltigt lösenord. Utöver hämtning av information sker även en del övriga aktiviteter i systemet från denna användare.
Logica har konstaterat att efter september 2008 har detta konto inte förändrats. Det är så långt tillbaks som det finns racf-loggar sparade.

2/2 lyckas en person logga på ett konto i TPX som inte var skyddat av behörighetssystemet, racf. Med detta konto kan andra aktiva sessioner tas över och personen har med det kapat en annan individs behörigheter fullt ut med alla de risker det innebär.
Utifrån det oskyddade kontot har personen haft full administrativ behörighet i TPX-systemet och även nytjat det för manipulation. Pga racf-skydd har detta i sig inte inneburit några risker för bakomliggande system.
Den oskyddade användaridentiteten i TPX har varit uppsatt på detta sätt sedan den senaste installationen för ca ett år sedan. Detta är dock det första kända tillfälle någon har använt sig av möjligheten att genom detta konto olovligen ta över en annan persons session.
I den information som lämnade systemet den 29/1 fanns en förteckning över användaridentiteter dock utan lösenord. Det kan varit den informationen som

gjorde detta möjligt. Detta är dock inte styrkt. Alternativet är att detta faktum sedan tidigare var känt för den personen som nyttjat möjligheten.

4/2 stängdes möjligheten för alla att kunna logga på TPX utan racf-kontroll. Efter detta datum har vi inte sett något lyckat försök att ta över en aktiv session i TPX men det är inte fullt ut samma sak som att det inte skett.

Åtgärder för att minimera risk för intrång

Vår ambition är att minimera möjligheten till otillåten åtkomst. I det material som lämnade systemet genom FTP den 29/1 kan det finnas information som gör det möjligt att ta sig vidare in i systemet när man väl är ansluten. Utifrån detta är vår rekommendation att snabbt begränsa möjligheten till att ansluta sig till systemet till befintliga kunder. Kortsiktigt filtrera port 23 för att sedan se över hela lösningen så att en säker och lättillgänglig tjänst skapas för marknaden.
Racf-skyddet behöver ses över för FTP-användare i sys19.

logica

Händelselogg

Datum/Tid	Händelse	Åtgärd
2010-02-03 09:00	Ärende rings in från Applicate. Felsökning påbörjas, man tappar sessioner i TPX samt att userid blir revokade utan att användaren själv varit inloggad.	Kontakt tas med Volvo IT och också involveras i felsökningen. Utesluter förändringar i RACF och TPX.
2010-02-03 13:00	Genomgång av loggar i SYS3 från ca 18:00 den 2/2 till 08:00 den 3/2 visar att påloggningsförsök gjorts mot ett antal userid, tillhörande Applicate, Logica och Volvo IT.	Volvo IT får i uppdrag att ta fram lista på TPX-userid som har funktionen NONE definierat på userid.
2010-02-03 13.30 – 16.15	Userid FRNT242 och SEMA290 verkar bete sig på ett oriktigt sätt. Kontroll av ip-adress visar att den kommer från ett nät som ej är via Applicate kund. IP-adress 202.84.75.138, den ägs av "CITY LINK KAMBODJA"	IP-adressen från Kambodja stoppas in mot SYS19 (och SYS3) av Volvo IT.
2010-02-03 17.10	Applicate upptäcker att SEMA290 har gjort "resume" och kan logga på igen. Mailadressen som användes var noone@cyber-rights.net.	Applicate spärrar användare och tar bort mailadressen.
2010-02-04 01.00	Framtagen lista från Volvo IT visar att påloggning via TPX utan password är möjlig.	Ändrar parameter för påloggning mot TPX till att kräva password för samtliga användarid.
2010-02-04 8.00-12.00 12.00-16.00	Undersökning i FW-Primus-DMZ efter telnetsessioner från internet mot 217.150.160.172 (SYS3 publik IP) Visar på ett flertal sessioner mot SYS3, verkar inte vara kundtrafik, att döma av reverse på IP. Se listan för alla IP-adresser nedan.	Stängning av port 23 görs mot SYS3 kl 13:38. Parallelt utökas loggning till att innefatta Applicates samtliga firewalls (FW-Infodata1, FW-Infodata2, FW-Primus-DMZ) samt alla kända IP. Lägger en generell block, samtliga kända SRC-IP blockeras helt mot firewallarna (FW-Primus-DMZ, FW-Infodata1).
2010-02-04 21.00	Ser att många användare har hög behörighet i TPX.	Volvo IT har gått igenom alla användare med TPX-admin behörighet och begränsat detta

		till ett fåtal personer.
2010-02-05 19.00-19.40	Misstänkt attack sker från följande adress. 213.145.177.83 www.oriska.org Misstänkt är att man körde ftp, via http – mycket trafik. Påloggningsförsök görs mot ett antal userid mellan 19.00 – 20.00.	Stoppar IP-adressen.
2010-02-06 10.00	Försök har gjorts mot port 992. Analyseras av Applicate.	Port 992 spärras mot SYS19 med undantag ip-adressen 85.228.49.117 som fortfarande får köra.
2010-02-07	Misstänkt connect mot ftp, SYS19. Verkar ej ha koppling till tidigare försök, ingen påloggning har skett. Trolig orsak portscanning.	Stänger följande adresser: IP Adress 124.114.130.149 Host 124.114.130.149
20100212 20:50	Uppringd av Volvo IT, om meddelade att deras system fått larm om misstänkt intrång. Undersökning av FW visar en host, (84.200.208.98) som kör trafik vid detta tillfället. Har skapat ~20 telnet sessioner mot både SYS3 och SYS19 inom 30min. 212.117.166.110	Stänger IP-adress

Lista med kända SRC-IP

Lista med kända SRC-IP		
130.240.204.195	crap.campus.luth.se.	Placerad i Lueå, på campus för Lueå Tekniska Universitet
202.84.75.138		Placerad I Kambodja, troligen proxunätverk
213.21.78.250	213-21-78-250.bon.t3.se.	Placerad I Sverige, Umeå, bredbandskund,
88.80.6.23	eduardo.prq.se.	Placerad i Sverige, Sthlm, Solna
194.71.126.18	flatline.pteah.estoykh.com.	Placerad I Kambodja
83.183.82.6	d83-183-82-6.cust.tele2.se.	Placerad I Sverige, Tele2 ADSL kund
85.17.146.78	hosted-by.leaseweb.com.	Placerad I Holland, Amsterdam, colo/hosting center,
88.80.28.72	host-72.prq.se.	Placerad I Sverige, Sthlm, Solna
88.80.20.41	thefinn.knark.net.	Placerad I Sverige, Sthlm, Solna
88.80.5.155	pluto.qualitum.net.	Placerad I Sverige, Sthlm, Solna
88.80.13.103	host-13-103-cust.prq.se.	Placerad I Sverige, Sthlm, Solna

Genomförda Analyser

Userid SEMA290 och SEMA105

Summerat händelser för dessa userid sedan 2008-09, SYS19. Rapporten visar på password violations som inträffat för dessa userid samt alla förändringar i RACF. Vad vi ser är att vissa tidpunkter sticker ut eftersom de är vid onormala tider.

Vi kan även notera att försöken att logga på båda dessa userid startar den 29/1 efter kl 19.00, först via SEMCICA3 och därefter via ftp.

SYS19_sammanst_SEMA290-105.txt

Genomsökning av loggar har gjorts via en funktion som kallas RACREP.

Revokade userid i SYS19,2010-01

Tagit fram en rapport på userid som blivit revokade i SYS19 efter den 17 januari.

Detta ger en bild över vilka system som påloggningsförsök gjorts i och vid vilka tidpunkter. Ser även vilka userid som testats och i vilken ordning.

Sist i rapporten visas en lista över userid som testats men ej finns upplagda i RACF. Dessa påloggningsförsök är från den 5/2.

SYS19_Intressanta_not.txt

Testade userid den 30-31/1

Bilagan visar vilka userid som testats att användas den 30-31/1, via SEMCICA3 och ftp.

Från 2010-01-30 17:24:10 börjar man göra 2 påloggningsförsök per userid och fortsätter sedan på detta sätt fram till den 2010-01-31 kl 00:20:10.

SYS19_TE.TXT

Jämför man denna lista med resultatet från listade filer via ftp (se rubrik *Tester körda med FTP, spegelmiljö*) kan man hitta mönster i testade userid.

FTP mot SYS19 och SYS3

Den 29/1 vid 23.00 loggar SEMA290 på via ftp och startar hämtning av ett antal filer.

Datum	Tid	System	Beskrivning
2010-01-29	20:39:21	SYS3	Påloggningsförsök görs med ftp. Misslyckas pga revoked user.
2010-01-29	20:59:42	SY19	Resume password görs genom user E484RACF med rutin NYTTPW
2010-01-29	22:58:28	SYS3	Påloggningsförsök med FTP görs Misslyckas pga revoked user.
2010-01-29	22:58:28	SYS3	Påloggning med ftp görs i SYS3. Misslyckas pga revoked user.
2010-01-29	22:58:32	SYS3	Påloggningsförsök med FTP görs Misslyckas pga revoked user.
2010-01-29	23:02:46	SY19	Invalid password via ftp
2010-01-29	23:17:48	SY19	Går via FTP in och hämtar ner en stor mängd dataset/filer. Se bilaga. Försök till hämtning dataset som stoppats: Se bilaga
2010-01-29	23:37:39	SYS3	Påloggningsförsök med FTP görs Misslyckas pga revoked user.
2010-01-29	23:38:50	SYS3	Påloggningsförsök görs Misslyckas pga revoked user.

Tester körda med FTP, spegelmiljö

Att det är möjligt att logga på via ftp har testats med tre userid i den spegelmiljö som finns i Bromölla, SYS19. Följande userid har testats:

SEMA290
NIXTE22
ITP0257

Har endast testat att logga på och göra listning av hela masterkatalogen.

SYS19_FTP_SEMA290.zip

Tester körda med FTP, produktionsmiljö

Följande userid har testats:

WMSTOTT

SYS19_FTP_WMSTOTT.TXT

Har endast testat att logga på och göra listning av hela masterkatalogen – se jobblogg WMSTOTTB, job09531, i SYS19.

Bilagor

Hämtade filer via ftp från SYS19, de försök som gjorts i SYS3 har misslyckats.

SYS3+SY19_FTP_server_25jan-03feb.txt

Filer som misslyckades att hämtas i SYS19.

Sys19_RACF_Access_fail_2010.txt

Summering

Tester har körts i spegelmiljön i Bromölla, SYS19, för att se vad man vid påloggning mot ftp kan få fram för information.

Listning av samtliga dataset på i USS-delen och under TSO kan göras. Detta gör att viss information som t ex usernamn blir tillgänglig trots att dessa bibliotek är skyddade via RACF.

Stor del av informationen som försöker nås är behörighetsskyddad vilket gör att den inte kan läsas/hämtas.

FTP Tester SYS19 i Bromölla.txt

TPX-påloggning

Påloggning i TPX görs av SEMA290 den 29/1, DAFATPX2.

TPX_påloggning_SEMA290.txt

Påloggningar som gjorts med userid V018150. Dessa har undersökts sedan den 3/1-2010 och första påloggningen var den 2/2 enligt tidpunkterna nedan.

DAFATPX3 – första påloggning 2/2 19:41
DAFATPX2 – första påloggning 2/2 19:50
SEMTPX19 – första påloggning 2/2 19:59

TPX_påloggning_V018150.txt

DAFATPX3, listning av userid från den 2010-02-02. Visar att nya userid har lagts upp och behörighet ändrats på flera.

TSO	RACF	N	N	N	N	V018150	02/02/10 20:16:42
END	RACF	N	N	N	N	V018150	02/02/10 20:20:19
FRNT242	NONE	N	N	N	N	V018150	02/02/10 20:46:32
MACHRUN	TPX	Y	Y	Y	Y	V018150	02/02/10 21:09:12
DAF1520	NONE	Y	Y	Y	Y	MACHRUN	02/02/10 21:11:19
VX31749	NONE	N	N	N	N	V018150	02/02/10 22:46:27
DACRACF	RACF	N	N	N	N	V018150	02/02/10 22:48:42
DAFRACF	NONE	N	N	N	N	V018150	02/02/10 22:49:10
DAF1488	NONE	N	N	N	N	V018150	02/02/10 22:50:45
VX22617	NONE	N	N	N	N	V018150	02/02/10 22:56:05
CANCEL	RACF	N	N	N	N	V018150	02/02/10 22:56:16
CANEL	ACF	N	N	N	N	V018150	02/02/10 22:56:21

Det är nu möjligt att använda de userid ovan för att ta över pågående sessioner från dessa användare. Går dock ej att starta nya då lösenord krävs.

Denna öppning finns till den 4/2 ca 01.00 då det ändras tillbaka till RACF.

Undersökning i racf i SYS3 och SYS19 på förändringar gjorda av dessa userid visar att inga behörigheter ändrats som ej är godkända samt inga upplägg av nya userid.

Userid FRNT242 har varit upplagt i TPX – ej RACF. Undersökningar i SYS3 och SYS19 visar att enda loggningarna vi har på detta userid är – UNDEFINED USERID – dvs det finns och har inte funnits något userid som heter FRNT242 i RACF.

Under tiden 2/2 efter kl 20.00 fram till 4/2 01.00 har möjligheten funnits att ta över ett userid, i SYS3 enligt listan ovan och i SYS19 – se nedan. När detta sker får man då samma behörighet som den användare som man tar över – i pågående session, det går ej att starta nya. Undersökningar i RACF visar att inga förändringar skett (se ovan). Lyckade accesser finns ej lagrade i systemet.

Utredning om vad som exakt har skett med dessa userid är ej kartlagt ännu. Detta arbete kommer att fortgå.

racfSYS3_sys19.xls

Summering

När påloggning via TPX startas kan vi idag inte se vilka userid som testats att logga på och var denna information kommit ifrån. Misstänkt är att den blivit tillgänglig via ftp-påloggningarna men kan ej garanteras.

Rapporter visar även på att inga nya userid skapats som kan användas vid nya påloggningsförsök men om information blivit tillgänglig på annat sätt via övertag av pågående sessioner saknas.

Efter möjligheten att ta över andras sessioner utan att behöva ange password ser vi inga lyckade påloggningsförsök denna väg.

Kort summering i kronologisk ordning vad som hänt i SYS3 och SYS19.

Sammanfattning SYS3 och SYS19.txt

Slutsatser

Därför detta kunnat inträffat

Userid samt möjlighet att byta password för ett par demousers blir kända av icke behörig person. Denna möjlighet utnyttjas sedan för att logga på och hämta uppgifter via webben. Samma userid används sedan för att köra ftp mot SYS19 och hämta information.

Att det går att logga på via ftp med en demouser beror på att racf-användare i miljön får ett automatiskt UID tilldelat vid påloggning. Att man tilldelar en användare UID beror på att de ska kunna köra resurser som går under USS (ftp, telnet, sftp, webserver osv) krävs ett OMVS-segment.

Användare som ej behöver dessa funktioner ska ej tilldelas ett UID.

Eftersom verksamheten bygger på att systemet ska vara tillgängligt från samtliga nät kan man då via en ftp-klient logga på om man har ett userid och password.

TPX-påloggning via ett userid där man ej behövt ange password har kunnat ske på grund av en ändrad parameter i TPX. Denna parameter ändrade i samband med uppgradering av produkten, den 8 februari 2009. Detta ställdes om via ettjobb som kördes SYS3 och SYS19, jobbnamn ADMIN.

När denna möjlighet upptäcktes utnyttjades den genom att tilldela flera userid samma funktion och att då även kunna ta över pågående sessioner.

FTP och OMVS-segment

Vid övergång till någon av de senare releaserna av OS/390 i slutet av 90-talet, fick vi en ny IP-stack som flyttades från MVS till USS.

Detta innebar att man var tvungen att ha ett s k OMVS-segment definierat för varje user för att kunna köra Ftp.

Det blev ett krav på IBM att man var tvungen att fixa så att detta blev transparant mot tidigare versioner av OS/390 (dvs vi ska inte behöva definiera OMVS-segment för att köra Ftp).

Då skapade IBM möjligheten att i RACF sätta upp så att samtliga användare som saknade OMVS-segment automatiskt tilldelades ett. Detta sätts upp per lpar och gäller sedan för samtliga RACF-användare.

Genom att aktivera FACILITY BPX.DEFAULT.USER fick man denna möjlighet.

Teknisk uppsättning av miljön

I SYS19 är definitionen följande:

```
CLASS      NAME
-----      ----
FACILITY   BPX.DEFAULT.USER

LEVEL  OWNER      UNIVERSAL ACCESS  YOUR ACCESS  WARNING
-----  --------   ----------------  -----------  -------
 00    BPXDFLTG        NONE              NONE     NO

INSTALLATION DATA
-----------------
*** OPEN EDITION DEFAULT USER AND GROUP ***

APPLICATION DATA
----------------
BPXDFLTU/BPXDFLTG
```

Det är APPLDATA som talar om vilka user och grupp ids som används. Dessa måste finnas, precis som vanliga users/groups, med omvs segment

```
INFORMATION FOR GROUP BPXDFLTG
    SUPERIOR GROUP=STCGROUP     OWNER=STCGROUP    CREATED=00.131
    INSTALLATION DATA=*** OPEN EDITION DEFAULT GROUP ***
    NO MODEL DATA SET
    TERMUACC
    SUBGROUP(S)= BPXTTY
    USER(S)=      ACCESS=      ACCESS COUNT=      UNIVERSAL ACCESS=
      BPXDFLTU      USE           000000               NONE
        CONNECT ATTRIBUTES=NONE
        REVOKE DATE=NONE                 RESUME DATE=NONE
      PUBLIC        USE           000147               NONE
        CONNECT ATTRIBUTES=NONE
        REVOKE DATE=NONE                 RESUME DATE=NONE

OMVS INFORMATION
----------------
GID= 2147483647


USER=BPXDFLTU  NAME=OE DEFAULT USER       OWNER=BPXDFLTG  CREATED=00.131
 DEFAULT-GROUP=BPXDFLTG PASSDATE=00.000 PASS-INTERVAL=N/A PHRASEDATE=N/A
 ATTRIBUTES=NONE
 REVOKE DATE=NONE   RESUME DATE=NONE
 LAST-ACCESS=00.131/15:30:30
 CLASS AUTHORIZATIONS=NONE
 INSTALLATION-DATA=*** OPEN EDITION DEFAULT USER ***
 NO-MODEL-NAME
 LOGON ALLOWED    (DAYS)          (TIME)
 ---------------------------------------------
 ANYDAY                           ANYTIME
  GROUP=BPXDFLTG  AUTH=USE      CONNECT-OWNER=BPXDFLTG  CONNECT-DATE=00.131
    CONNECTS=     00  UACC=NONE     LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=NONE
    REVOKE DATE=NONE   RESUME DATE=NONE
SECURITY-LEVEL=NONE SPECIFIED
CATEGORY-AUTHORIZATION
 NONE SPECIFIED
```

```
SECURITY-LABEL=NONE SPECIFIED

OMVS INFORMATION
----------------
UID= 2147483647
HOME= /
PROGRAM= /bin/echo
CPUTIMEMAX= NONE
```

logica
be brilliant together

Dokumenttyp
Rapport

Område
Säkerhet

Rapport externa leverabler

Sammanfattning

Detta dokument avser besvara ett antal specifika frågor ställda av Rikspolisstyrelsens verksamhetsskyddsenhet. Innan frågeställningarna avhandlas så ges en allmän bakgrundsbeskrivning.

Ärendet gäller ett datorintrång med tillhörande informationsläckage i en såkallad stordatormiljö som drivs av infrastrukturleverantören Logica. Stordatorn består av flera s.k. partitioner där två stycken av dessa (SYS19 och SYS3) idag är konstaterat utsatta för intrånget. Den ena av partitionerna (SYS19) används exklusivt av företaget Applicate som är förmedlare och förädlare av stora informationsmängder, bland annat personregister. Denna information tillhandahålls från företag och myndigheter samt säljs till företag och myndigheter. Den andra partitionen SYS3 är delad mellan flera verksamheter, bland annat Logica internt, Applicate, Skatteverket/Kronofogden samt ett antal andra företag.

Onsdagen den 7e mars upptäcker Applicate och Logica att det sker ovanliga aktiviteter i datormiljön. Efter att en liten grupp personer utfört en snabbutredning och samordnad aktivitet under natten så spärras vissa konton i systemet. På morgonen utökas gruppen och mer ansvariga informeras. Under de därpå kommande dagarna utförs incidentinsatser samt olika typer av forensisk undersökningar för att förstå innebörd och omfattning av incidenten. Den 13e mars har utredningen konstaterat att händelserna pågått sedan redan den 25e februari 2012.

Den 16 mars kopplar Logica in IBMs internationella incidentutredare och säkerhetsspecialist. Den 19 mars är bilden såpass klar att en polisanmälan inlämnas från Applicate till SÄPO.

Intrången har skett dels via existerande filöverföringstjänster baserade på FTP-funktionen, dels via interaktiv inloggning via ordinarie fjärrinloggningsfunktion, samt slutligen via av angriparna placerade bakdörrar. Intrången har varit ofta skett i kombination med stora datauttag ur systemen. Vidare har intrång och missbruk skett via Applicate webbtjänster. Missbruket har bland annat omfattat obehöriga kreditupplysningar.

Utredningen konstaterar att det finns beröringspunkter, såsom vissa gemensamma konton mellan de två stordatorpartitionerna, vilket möjliggör att angripare kan komma åt information i bägge partitionerna i de fall angriparen haft turen att komma över just ett av dessa konton. Vilket de tyvärr hade gjort.

Uppskattningsvis 10000 filer/dataset[1]:s har hämtats ut från SYS19 av obehöriga personer. Uppskattningsvis 600 filer/dataset:s har hämtats ut från SYS3 av obehöriga personer. Bland filerna/dataset som hämtats ut finns olika typer av företagsuppgifter, systemfiler inklusive certifikat, källkod samt personuppgifter, inklusive lista från 2007 över personnummer där filnamnet var "E897.SPAR.SKYDD".

Över 120 000 konton som från början fanns i användardatabasen RACF. Uttag har skett av användarinformation, av vilka utredningen från kvarglömda filer kunnat fastslå att uttagen saknat den viktiga lösenordsinformationen. Det kan dock inte uteslutas att denna information kommit ut. Via incidenthanteringsåtgärder så har ett stort av dessa konton kunnat spärras eller inaktiveras. Ca aktiva 70000 kundkonton finns idag kvar i systemet, samtidigt som vidare skyddsåtgärder och rensningar fortsätter.

Särskilt intressant att notera rörande kontouppgifterna är:

- *Det första kontot som idag har konstaterats vara knäckt och använts den 25e februari tillhör ett filöverföringsjobb från Sveriges riksdag. Hur någon obehörig kommit över denna inloggningsuppgift är inte klarlagt.*
- *Ett av kontona som använt flitigt av angriparna tillhörde ursprungligen Monique Wadsted, advokat som företrädde rättighetshavarna i den s.k. piratebayrättegången*
- *Flera av kontona som använts, inklusive Wadsted:s, har manipulerats i RACF-databasen att för få utökad behörighet.*

Arbetet med såväl incidentutredning samt systemuppsäkringar fortgår.

[1] Ett dataset kan innehålla en eller fler filer

logica
be brilliant together

Innehållsförteckning

Förklaringar

Applicate. IT-företag som är specialister på kundunika IT-lösningar innehållande stora datamängder.

Dataset. IBM-benämning för sparad data. Kan ses som ett arkivformat där själva dataset:et kan innehålla en eller fler filer.

Brandvägg. Nätverkssäkerhetsfunktion som används för att spärra, filtrera ut, släppa igenom samt logga nätverkstrafik. I Logic:a-miljön runt stordatorn finns ett stort antal brandväggar, vilka används bland annat för att hantera nätverkstrafik till/från de olika stordatorpartitionerna och kunders åtkomst till dessa.

FTP. File Transfer Protocol. Funktion för överföring av filer och s.k. dataset till och från Logica:s miljö. Denna filöverföringsfunktion har används av obehöriga för att hämta ut information från stordatorn. Likväl har funktionen används för att skicka upp filer till de två olika partitionerna.

Logica. IT-tjänste- och infrastrukturleverantör som tillhandahåller bland annat stordatortjänster.

Partition. Logisk segmentering och uppdelning av stordatorn i mindre enheter, vilka även kallas för LPARs (Logical Partitions). En LPAR innehåller definitionsmässigt RAM-minne, CPU, kringutrustning samt operativsystem[2]. Logica:s stordator är uppdelad i ca 25 partitioner.

PI. Påloggning InfoTorg**.** Behörighetsdatabas för webbgränssnittet som är kopplad mot RACF.

RACF. Behörighetsdatabas i stordatormiljön som innehåller användarnamn, lösenordsinformation, behörighetsinformation, kopplingar mot system och applikationer med mera.

SMF. System Management Facility är en IBM-metod för att övervaka och ta ut aktivitetslogg.

Stordator är en större och kraftfull datorresurs av märket IBM. Stordatorn är logiskt uppdelad i s.k. partitioner för att kunna hantera resurser, kunder, användning, etc. Logica:s stordator är fysiskt placerad i Logica:s anläggning i Bromölla.

2

http://publib.boulder.ibm.com/infocenter/zos/basics/topic/com.ibm.zos.zmainframe/zconc_mfhwsyspart.htm

Svartlistning. Lista över explicit spärrade IP-adresser som förhindras komma in till bestämda nättjänster i stordatormiljön. *Se även vitlistning.*

SYS3. Partition i stordatorn som delas av ett antal olika verksamheter, däribland Logicakunder och Logica internt. Bland de kunder som återfinns i SYS3 är Skatteverket/Kronofogden. SYS3 används till bland annat hantering av stora utskriftsjobb, vilka överförs från kunder.

SYS19. Partition i stordatorn som används av Applicate för sin informationsbehandling.

TSO. Time Sharing Option. Interaktivt exekveringsmiljö i IBM stordatorn under z/OS.

TPX. En sessionshanterare/menysystem som används för att koppla sig mot olika IBM applikationer.

USS. UnixSystemServices. Exekveringsmiljö i stordatorn som baseras på operativsystemet UNIX med IBMs tillägg för att integreras

- med traditionella IBM-funktioner ,såsom RACF-behörighetssystemet eller spårdatafunktionen SMF
- andra IBM exekveringsmiljöer (exempelvis TSO och CICS)

Vitlistning. Lista över explicit tillåtna IP-adresser som tillåts komma in till bestämda nättjänster i stordatormiljön. *Se även svartlistning.*

zOS. Operativsystem för IBM stordatormiljö vilken är värdmiljö för andra IBM-system såsom USS, TSO, CICS, mfl. Är en vidareutveckling av IBMs traditionella operativsystem OS/390 och MVS.

Status om intrånget är stoppat eller pågående

Attackytan har minskats genom ett antal tekniska skyddsåtgärder.

Intrångsförsök mot SYS19 är hanterat genom whitelistning av FTP-trafik från godkända IP-adresser samt bortfiltrering av protokoll som tidigare använts för intrång (telnet-trafik samt trafik på port 443). Övrig trafik som inte konstaterats som legitim har filtrerats bort.

Intrångsförsök mot SYS3 är hanterade genom whitelistning av trafik mot FTP samt bortfiltrering av övrig trafik som inte är legitim.

Alla systemadministratörskonton har bytt lösenord, komprometterade administratörskonton är utbytta.

Senast konstaterade intrång i SYS3 inträffade morgonen 23/3 via FTP och telnet. Senast konstaterade intrång mot SYS19 skedde den 16/3 via Telnet.

Fortsatta intrångsförsök sker mot webbtjänster baserat på den lista med användarnamn som kopierats ut ur SYS19.

Vilka åtgärder har gjorts när

Se bifogad händelse och åtgärdslogg.

Vilka delar är fortfarande inte utredda

Kommunikation

- I syfte att identifiera adekvata åtgärder sker egna portscanningar av publikt åtkomliga nät rörande SYS3 och SYS19 löpande. En portscanning har genomförts av det nät i vilket SYS19 ingår, men skall återupprepas. Med information om brister skall aktiviteter identifieras, planeras och exekveras.

- Utredning skall ske i syfte att förbättra brandväggsskyddet för det nät där SYS3 ingår. Inom ramen för denna utredning skall aktiviteter identifieras, planeras och exekveras.

Windows, Unix och Linux-miljöerna

- Grundläggande scanning efter sårbarheter i de Windows, Unix och Linux-miljöer som i första hand ligger inom Applicates systemlösning skall ske i syfte att identifiera eventuella säkerhetsrisker. Med information om brister skall aktiviteter identifieras, planeras och exekveras.

Mainframe-miljö

- Analys skall ske av den totala mängden RACF-konton och den kända mängd RACF-konton som tillskansats för att klargöra hur ytterligare avgränsningar i behörigheter skall tillämpas.

- Det är ännu inte utrett vilken passwordpolicy som bör tillämpas för Applicates kunder.

- Utredning skall ske av den totala RACF-databasen för att klargöra vilka konton som skall tas bort resp kan inaktiveras.

- Borttag av av ftp-behörigheter på konton som inte kör ftp, t.ex. itwebaccess konton, planerat till måndag.

- Endast en del av de användarid som använts för utkopiering av information har utretts, återstående skall utredas.

Den rapport, med åtgärdsförslag, som tagits fram av IBM skall, värdera och åtgärdsplan tas fram.

Relaterat till SKV

Under den 18/2, 20-21/2 sker höga volymer (3-8 ggr normala volymer) av slagningar i Navet webservice, i dagsläget oklart vilka dessa slagningar är. Loggar är under framtagning.

Den 18/3 konstateras onormalt hög nätverkstrafik på kommunikationslänken från Logica till SKV. Eventuell koppling är under utredning.

Detaljinformation om känd information som är avslöjad

Beskrivning av innehåll i de filer som kopierats ut ur respektive system.

SYS19

- SPAR (Statens person och adressregister) information, lista på urval av personnummer för personer födda 1964 och senare.
- InfoTorg faktureringsinformation – Fakturering antal transaktioner per kund.
- PI (påloggning InfoTorg) – Filer som skickas in till LIME (CRM system). All information om kunder i InfoTorg och dess behörigheter.
- Infodata (Posten) – Adressmatchingar
- InfoTorg(PWC) – Spec på projektmärkning för vidarefakturering
- Polisen – 2 miljoner personnummer, enbart.
- Applicate (Radiotjänst) – Faktureringsinformation
- InfoTorg/Infodata/Polisen – Faktureringsinformation, transaktionstyp och antal.
- Polisen – Transaktionsstatistik från 2006
- Infodata – tre(3) dataset där filnamnet innehåller texten "skyddade". Dataseten är från år 2007. 10 793 personnummer total i filerna, en kopia och två original har hämtats ut. Dvs tre dataset.
- Applicate (blandade kunder) – Faktureringsstatistik
- Infodata – dataset innehållande personnummer i relation till varandra
- InfoTorg – BASUN (företagsinformation från SCB). Grundinfo, namn, juridisk form, storlek på företag etc.

SYS3

- FLISTEST – Handelsbankens fakturor till sina kunder 2006 och 2007 (test mtrl.)

- Enligt Kronofogdemyndigheten har ca 40 klartextfiler innehållande kunder och gäldenärer som normalt skickas till unixsystemen kopierats ut från SYS3. Filerna innehåller personnummer, skuld, vem som personen är skyldig. Filerna innehåller även uppgifter som gäldenärer med skyddade identiteter.
- Vidare har betalningsfiler till Swedbank samt sigill för signering av utbetalningsfiler kopierats ut ur SYS3, sigillet är dock utbytt.

- Cobolkoden till programmet Navet har kopierats ut tillsammans med KFM's Navet-certifikat. Koden kan användas av inkräktaren för hitta svagheter och sårbarheter i applikationen Navet. Applikationen är dock endast tillgänglig från SKV nät och är inte publikt tillgänglig.

Vilken information som kan vara påverkad – samverkan med berörda parter

Skyddade personnummer dataseten måste utredas tillsammans med Skatteverket och övriga myndigheter.
Datasetet innehållande 2 miljoner personnummer måste utredas tillsammans med Skatteverket och eventuellt andra myndigheter.
Personer från 1964 och senare.
Skatteverket äger rådatat och har kompetensen runt detta.

Information om filer som kan vara manipulerade

Angriparna har haft tillräcklig behörighet att manipulera all data, system och applikatoriskt. Man har haft en teoretisk möjlighet att manipulera system och funktioner i zOS, USS etc. Men IBMs bedömning är att angriparna saknat adekvata kunskaper inom zOS för att genomföra det samma. Det finns idag inte tillräckligt med loggar för att gå tillbaka i tid för att säkerställa att man inte manipulerat system etc.

Det har konstaterats att angriparna haft tillräcklig kunskap för att elevera kontons behörigheter.

Information om hur eskaleringen gått till vid intrånget

Applicate och Logica konstaterade den 7/3 ett ovanlig högt cpu uttag för SEMCICA3 i SYS19, dvs. många transar som kördes av användare som ifrågasattes. Aktiviteten ansågs som otillåten, en säkerhetsincident konstaterades 8/3 varvid utredning påbörjades. (IM3107818).

Den 16/3 konstaterar Applicate att angriparen etablerat starkare fotfäste i systemet och kallar till krismöte. Logica etablerar Major Incident Manager och kallar in specialistkunskap från IBM.

Applicate registrerar anmälan hos Säpo 19/3.

Intrång konstateras i SYS3 varvid Logica kontaktar Säpo för en anslutningsanmälan 21/3.

Information om de ca 10 administratörskontona

I samband när intrånget skedde och User's med "special behörigheter" kapades ändrades behörigheten till att enbart 2 User hade kvar special i SYS3 samt i SYS19 togs special bort hos alla och två nya User skapades med special

Listningen nedan omfattar användaridentiteter som har behörighetsnivån Special.

'*' = Revokerad

SYS3 innan intrånget:

CEA	Common Event Adapter
*DAFRACF	Superior Racf Admin
E927REFR	E927REFR
*JDAUSER	Säkerhetsadm
*VX17501	Mats Wikensten
*VX18150	Svante Sundelin
*VX18171	Bengt Björkqvist
*VX19133	Bengt Gellingskog
*VX21836	Christer Hedlund
*VX21841	Kalle Aronsson
*VX22617	Claes Borgh
*VX31749	Örjan Lindholm
WMALHUN	Alan Hunter
WMROCAR	Roland Carlsson
WMSTOTT	Staffan Ottosson
WMTHOHR	Thomas Ohrås

SYS3 efter:

*DAFRACF
*JDAUSER
*VX17501
*VX18150
*VX18171
*VX19133
*VX21836

*VX21841
*VX22617
*VX31749
WMALHUN
WMTHOHR

SYS19 innan intrånget:

CEA	Common Event Adapter
DAFRACF	Superior Racf Admin
E927REFR	E927REFR
WMALHUN	Alan Hunter
WMROCAR	Roland Carlsson
WMSTOTT	Staffan Ottosson
WMTHOHR	Thomas Ohrås

SYS19 efter:

WMXLOG1
WMXLOG2

Information om vilka konton som användes vid utskickning av data

25/2 Första kända användarkonto som användes var ett konto från Riksdagen (AVIY356). Denna användare har via zOS och USS börjat FTP'a dataset och filer från/till Logica ca 400 st.
Vi har konstaterat att en mängd konton använts över tid och att många manipulerats till att erhålla special och superuser behörighet i systemen. Mer runt detta beskrivs i händelserapport och tidslinje beskrivningen.

Information om vilka IP-adresser som användes vid utskickning och vilken ISP som användes

Information har transporterats till VPS (Virtual private server) providers i bl.a. Tyskland (t ex 178.18.243.27) men företrädesvis har IP-adresser i Kambodja (Pnomh Pen) använts. Bland annat har man använt ett superuser-konto (högsta behörighet på systemen) från 27.109.118.33 och 123.108.250.50 samt ett reguljärt systemkonto från

203.176.141.205 (alla adresser finns i Kambodja). Enligt uppgift ska en stor del av denna aktivitet pågått runt perioden 10-15 mars 2012. Det finns även informationstransaktioner mot den svenska ISPn Bahnhof.

IP-adresser som accessat och överfört information:
46.50.183.5 (JSC "Zap-Sib TransTeleCom", Novosibirsk, Ryssland)
203.176.141.205 (MEKONGNET INTERNET SERVICE PROVIDER, Kambodja)
27.109.118.33 (DTV-STar Co.,Ltd, Kambodja)
123.108.250.50 (Neocomisp, Kambodja)
178.18.243.27 (QQ-Nova, Tyskland)
46.59.51.181 - h-51-181.a328.priv.bahnhof.se (Bahnhof, Sverige)
85.228.54.229 (Bredbandsbolaget)
178.174.180.144 (Tyfon Svenska AB)
202.120.189.223 (Tongji University, Shanghai)
93.186.170.54 (Inline Internet Online Dienste GmbH, Tyskland)

Ytterligare IP-adresser, oklart accessmöjligheter (loggats i brandvägg):
124.248.174.161 (Cogitel, Kambodja)
124.248.187.100 (Cogitel, Kambodja)

Reflektion:
Även om det gjorts ett större antal på loggningar på storsystemen från exempelvis Tyska ip-adresser så är Riksdagen, Kambodja och Bahnhof mer intressant än något annat och bör prioriteras i den mån det går. Övriga IP-adresser i Ryssland och Tyskland tillhör troligtvis server-/vps-provider.

Vilken sorts trafik som utgjorde slagningarna mot dalarna

En översiktlig undersökning har genomförts av ett urval av sökbegreppen som använts på Infotorg. Som tidigare nämnts har det genomförts sökningar på Jim Keyzer, Gottfrid, PRQ Kommanditbolag, RPS registrerade bilar i bilregistret m.m.

Nedan följer ett kort urval med förklaring:

Lennart Nordh: svensk representant i rymdstyrelsen Cospar
Mer info: http://www.snsb.se/sv/Mediebank/Forskare/SRS/

Joacim Engvall: Kan vara en av angriparna som söker på sig själv (?)
Se: https://www.facebook.com/groups/92072346644/members/

Martin Bergström: Polis som ingrep mot filmare och tvingade till radering

Fredrik Jeanson: Arbetar på supporten hos MOSMS

Håkan Marklund: Robinsondeltagare

Mikael Persbrandt: Skådespelare

Robin Åström: Verkar vara en tekniker som certifierar sig, se länk:
Mer info: http://robinastrom.blogspot.se/

Liisa Bernadt: Kattägare och förskolelärare, möjligtvis i Norrtälje.
Mer info: http://www.rexringen.nu/utstallningar/titelkatter/crx-bis.html

Erik Turlen: Åtalades för knivhugg i Ludvika, bor i Smedjebacken.
Mer information: http://vgnt.se/tre-man-atalade-for-knivhugg-i-ludvika/

Angelika Brorström: Bloggerska i 17-årsåldern
Mer info: (omnämns)
http://emiliamagdalena.blogg.se/2012/january/utkast-jan-8-2012.html

Reflektion:
Troligtvis unga personer som fått information om inloggningskonton på infotorg av de mer kompetenstunga huvudaktörerna. Dessa unga personer som sökt på kändisar, en bloggerska och personer i Ludvika/Smedjebacken har troligtvis inte haft en susning om de eventuella konsekvenserna av sökningarna. Troligtvis förankring i Ludvika/Smedjebacken.

Vilka andra organisationer är påverkade

Efter genomgång av utkopierade dataset har hittils kunnat konstateras att berörda organisationer begränsas till:

- Logica
- Applicate
- Skatteverket
- Kronofogdemyndigheten

logica
be brilliant together

Dokumenttyp
Rapport
Område
Säkerhet

Händelse och åtgärdslogg

	Datum	Tidpunkt	Händelse	System	Typ
Lö	2012-02-25				
		04.55 - 06.47	user **AVIY356** från IP **178.18.243.27** hämtar USS filer	SYS19	Händelse
Sö	2012-02-26				
		13.45....23.51	samma user/IP hämtar USS and ZOS filer	SYS19	Händelse
To	2012-03-01				
		10.45....15.34	samma user/IP hämtar/lagrar USS filer + hämtar ZOS filer	SYS19	Händelse
Sö	2012-03-04				
		02.25....09.15	user **BSN0058** på IP **85.228.54.229** hämtar ZOS filer	SYS19	Händelse
		07.09 – 10.42	user **BSN0058** på IP **178.174.180.144** hämtar ZOS filer	SYS19	Händelse
		08.13....08.59	user **BSN0058** på IP **178.18.243.27** hämtar ZOS filer	SYS19	Händelse
		10.25....12.58	user **BSN0058** på IP **46.59.51.181** hämtar ZOS filer	SYS19	Händelse
Må	2012-03-05				
		12.55....19.28	user **BSN0058** på IP **178.18.243.27** hämtar USS filer	SYS19	Händelse
Ti	2012-03-06				
		03.18....03.59	user **BSN0058** på IP **46.59.51.181** hämtar ZOS filer	SYS19	Händelse
		17.59....20.45	user **BSN0058** på IP **46.59.51.181** hämtar ZOS filer	SYS19	Händelse
On	2012-03-07				
		-	Logica/Applicate konstaterar högt CPU-uttag	SYS19	Händelse
		23.27 - 23.34	user **SPRBI45** på IP **46.59.51.181** hämtar ZOS/USS filer	SYS19	Händelse
		-	Applicate kontaktar Anki Nordin för uppgifter om **BSN0058** (infotorg)	SYS19	Åtgärd

		12:35	**BSN0058** revokerad av Applicate	SYS19	Åtgärd
To	**2012-03-08**				
		09:20	Racf – **SPRBI45** revokerad avApplicate	SYS19	Åtgärd
		-	Telefonmöte Logica Applicate, säkerhetsutredning startas		Åtgärd
		13.40 - 13.46	user **SPRBI08** på IP **46.59.51.181** hämtar USS filer	SYS19	Händelse
		14.01 –14.06	user **SPRBI01** på IP **D64** hämtar USS filer	SYS19	Händelse
		14.02	många **SPRBInn** users revokerad av Applicate	SYS19	Åtgärd
		14.23 –14.42	user **ASI0936** på IP **46.59.51.181** hämtar USS filer	SYS19	Händelse
		14.50	Racf – **ASI0936** revokerad av Logica	SYS19	Åtgärd
Fr	**2012-03-09**				
		fm	Logica identifierar under förmiddagen misstänkt trafik med tillhörande IP-adresser i brandväggsloggar.		Åtgärd
		16:00	Blacklistning i SYS19 FW - deny any för vissa nät	SYS19	Åtgärd
		em	Möte Applicate/Logicaresurser efterfrågas under helgen som övervakar brandvägg och CICS efter misstänkt beteende.		
		em	En kommunkationsresurs samt en CICS resurs allokeras för att övervaka systemet under helgen	SYS19	Åtgärd
		20:30	Ytterligare blacklistning i SYS19 FW	SYS19	Åtgärd
		kväll-natt	Applicate kör en batch för att revokera ett större antal userids	SYS19	Åtgärd
Lö	**2012-03-10**				
			Logica informerar Applicate om konto **AVIY356** och utreder konto **NUS.**		Åtgärd
			Applicate begär lista på IP som kör FTP mot systemet.		Åtgärd
			Logica tar fram begärd IP lista och delger Applicate.		Åtgärd
		01.00....07.01	userid **AVIY356** på IP **203.176.141.205** hämtar/lagrar USS filer	SYS19	Händelse

		06.32 – 07.30	Senare information pekar på att inetd.conf startade en telnetjänst på port 443 vilken användes av **AVIY356** kl 17.09.	SYS19	Händelse
		09.34....12.15	userid **AVIY354** på IP **203.176.141.205** hämtar USS filer	SYS19	Händelse
		12.39....15.04	userid **NUS** på IP **203.176.141.205** hämtar ZOS filer	SYS19	Händelse
		12.42	Misslyckade påloggning med ftp och användare **NUS** från **124.248.187.150**	SYS3	Händelse
		12.45	RACF Violations vid listning av kataloger	SYS3	Händelse
		13.02	Racf– flera AVI users revokerade av Applicate	SYS19	Åtgärd
		15.10	Ett par USS filer hämtas från **93.186.170.54**	SYS3	Händelse
		16.35	Racf- userid **NUS** revokerad av Applicate	SYS19	Åtgärd
		17.09	Racf– **AVIY356** misslyckas att ändra /etc/inetd.conf	SYS19	Händelse
		17.10	/etc/inetd.conf ändrad till att använda port 443 så den körs som SUPERUSER utan att kräva lösenord, oklart när den senare användes.	SYS19	Händelse
		17.20	Misslyckade påloggningar från **194.23.61.151**	SYS3	Händelse
		18.59	Racf- user **AVIY356** revokerad av Applicate	SYS19	Åtgärd
		19.22....19.57	Racf- 4 försök att logga på som **WMOVLAE** – misslyckas	SYS19	Händelse
		19.30 –19.31	user **AVIY357** på IP **27.109.118.33** lagrar /var USS filer Filen /var/a finns fortfarande och visar att användaren inte körde som uid(0)	SYS19	Händelse
		19.47	Ett stort antal USS-filer hämtas från **194.23.61.151**	SYS3	Händelse
		23:18	Racf - user **ASI0930** revokerad av Applicate	SYS19	Åtgärd
Sö	**2012-03-11**				
			Logica ser att någon försöker logga in med en serie av konton och informerar Applicate. Applicate kontaktar Logica och ber om hjälp med att implementera en IP-adress whitelist för FTP.		Åtgärd
			Logica informerar Applicate om inloggningsförsök med en serie av konton.		Åtgärd

		10:30	restore av RACF-databasbackup från 03/09 av Logica på beställning av Applicate då batchen hade tagit bort för många users)	SYS19	Åtgärd
		11:36	Racf– flera AV och AS users revokerade av Applicate	SYS19	Åtgärd
		23:00	Whitelistning av SYS19 för FTP införs (modiferades löpande under veckan)	SYS19	Åtgärd
Må	**2012-03-12**				
			Möte under förmiddagen med Applicate som säger att de identifierat att systemfiler från USS har läckt ut. Applicate har sammanställt en lista på konton som misstänks vara kapade. Logica analyserar de läckta systemfilerna men anser inte att det utgör någpå direkt fara. Alla konton på Applicates lista har vid olika tillfällen spärrats.		Åtgärd
		19.33	Racf– 5 försök att logga på userid **WMOVLAE** mislyckas, id revokerat av Logica	SYS19	Händelse
Ti	**2012-03-13**				
			Avstämningsmöte med Applicate under förmiddagen. Samordningsmöte hos Applicate under eftermiddagen. Applicate har sett misstänkta aktiviteter i sina loggar från den 25 februari. Applicate ber Logica analysera loggar bakåt i tiden för att identifiera när intrånget skedde med kontolistan som grund. Den gemensamma bilden är att vi med de spärrade kontonen och whitelist har lyckats stänga ute angriparna. Logica sätter upp dagligen återkommande avstämningsmöte med Applicate. Analys av Applicates konton på listan bakåt i tiden för att identifiera när intrånget började samt allmän wildcard analys		Åtgärd
On	**2012-03-14**				
			Avstämningsmöte med Applicate under förmiddagen. Logica kan i sina loggar verifiera misstänkta aktiviteter från den 24 februari. Den gemensamma analysen fortgår.		Åtgärd

To	**2012-03-15**				
		11.21	2 USS-filer hämtas från **93.186.170.54**	SYS3	Händelse
		19.03	RACF - **WAHS006** eleveras till System-special, operations och UID(0). Detta gjordes av inkräktaren genom SU authority av SUPERUSER för att ändra ID till **WMROCAR** (utan att behöva använda lösenord) och sedan köra RACF-kommandon för att ändra **WAHS006.**	SYS19	Händelse
		19.19....21.05	Inkräktaren försöker köra TSO - utan framgång	SYS19	Händelse
		19.50 + 20.54	Racf-userid **WMROCAR** ändrar lösenord på **RPHAI30** och **KVV015**	SYS19	Händelse
		20.25....	userid **WAHS006** på IP **217.150.174.80** hämtar ZOS filer	SYS19	Händelse
		20.44	**WAHS006** skriver group och user-information från RACF-databasen till /var/users.txt och hämtar den. antalet grupper (481) antyder att listan skapades av groups-special userif för gruppen RYÅSY	SYS19	Händelse
		21.04	Racf - elevering av userid **DAF1017** till systemspecial, operations och uid(0)	SYS19	Händelse
		21.14	Inkräktaren lyckas logga på TSO med userid **DAF1017 –** testar oper cmds	SYS19	Händelse
		22.21	hämtar /u/d610/rfvftp/1.tgz – skapad 22:20	SYS19	Händelse
		23:45	User **WAHS006** från IP **217.150.174.80** hämtar E897.SPAR.SKYDD	SYS19	Händelse
Fr	**2012-03-16**				
			Onödiga portar stängs i brandvägg (inkommande) och på systemet.		Åtgärd
			Applicate kallar till krismöte där de informerar att de sett att angriparen har använt administratörskonton i RACF för att tilldela kapade konton högsta behörighet samt flyttat 1,7 MB data från MVS till USS. Hela RACF databasen anses härmed kompromitterad.		Åtgärd
			Applicate och Logica påbörjar ett gemensamt arbete för att begränsa skadan och åtkomst till systemet. Flertalet möten hålls under dagen/kvällen.		Åtgärd
			Logica Incident Manager inkopplad.		Åtgärd

			Existerande whitelist i brandväggen krymps ytterligare.		Åtgärd
			Låga tröskelvärden för larmsättning över lag konfigureras.		Åtgärd
		08.06	Mycket många dataset kopieras ut	SYS19	Händelse
		07.21	Racf– **WAHS006** revokerad av Applicate	SYS19	Åtgärd
		09.35	Racf– **WMROCAR** (och andra med Special) Racf authority borttagna av Logica	SYS19	Åtgärd
		10.02	Racf– **WAHS006** och **DAF1017** Racf authority borttagna av Logica	SYS19	Åtgärd
		10.55 – 11.30	Racf– 2 nya racf admin ids skapade av Logica, gamla admin ids– auth borttagna	SYS19	Åtgärd
		13.00	OPS– alarm på logon på nya Racf-admin ids	SYS19	Åtgärd
		13:40	Blockering av trafik mot SYS19 port 443 för any	SYS19	Åtgärd
		19:00	IBM specialist inkopplad och arbete med IBM påbörjas	SYS19	Åtgärd
		-	Säkerhetsfunktipåen SERVERAUTH implementeras på systemet.	SYS19	Åtgärd
		20:00	Whitelistning av SYS19 klar för alla protokoll från internet	SYS19	Åtgärd
		-	Ett tiil nät med misstänkta IP:n spärras i brandväggen. ISP:n för dessa meddelas.		Åtgärd
		-	Kommunikationsförbindelsen mellan SYS3 och SKV överbelastad	SYS3	Händelse
Må	**2012-03-19**				
		21:52	Ett stort antal filer/dataset hämtas av user **NUS** från **93.186.170.54**	SYS3	Händelse
		kväll	Applicate registrerar polisanmälan hos Säpo		Åtgärd
Ti	**2012-03-20**				
		08:30	Applicates anmälan kompletteras		
On	**2012-03-21**				
		03:37	Sista kompletta datasetet hämtas	SYS3	Händelse
		08:20	Inloggningar i SYS3 identifieras av Logica	SYS3	Händelse
		08:42	Session "droppas" och användare **NUS** revoca's	SYS3	Åtgärd

		-	Blacklistning av SYS3 påbörjas	SYS3	Åtgärd
		14:30	Logica identifierar att filer med känslig information tillhörande SKV lämnat Logica	SYS3	Händelse
		15:00	Applicate informeras om att intrånget ökat i omfattning		Åtgärd
		17:00	SKV + KFM säkerhetschef informerad		Åtgärd
		17:50	Logica har kontakt med Säpo, Logica vill göra egen polisanmälan.		Åtgärd
		16:38	Nytt misslyckat påloggningsförsök av **NUS** från **111.92.242.65**	SYS3	Händelse
		20:00	förnyade intrångsförsök från nya source-adresser identifierade	SYS3	Händelse
		20:45	Ok från Applicate (Stefan) att köra nätscanning av de adresser som routas till Applicate.		Åtgärd
		Kväll	Portscanning av Applicates publika IP		Åtgärd
To	**2012-03-22**				
		10:15	Material (listor över dataset) skickat till KFM		
		11:30	Info från SKV om att navet kan vara omfattat		
		11:40	Eskaleringsmöte Logica SE management, kontakt med Gerald + Steve		
		12:15	Logica har kontakt med Säpo ang ny riskbild		
		12:40	Starta sammanställning av vidtagna åtgärder		
		12:42	Preliminär bedömning att itwebbarna är sunda		
		-	Kontakt med SKV, troligen Navet-filer och certifikat men inte applkatipåsdata.		
		-	Kontakt SKV, man har verifierat att källkod och certifikat är berörda men inte applikationsdata.		

		15:00	Möte med SKV/KFM: Filer har gått ut med personuppgifter kopplade till gäldenärer, de med skyddad identitet är särskilt flaggade SKYDDAD Källkod och certifikat till Navet har gått ut, certifikatet skulle kunna användas för falsk autenticering, källkoden för att identifiera säkerhetsbrister. Betalningsfiler och sigill mot Swedbank har kopierats ut, nytt sigill är beställt. Kritiskt är att integritet i filer inte påverkats.		
		15:50	Kontakt med säpo ang förändrad riskbild, inga särskilda krav från säpo på hantering av loggar eller information för närvarande		
Fr	**2012-03-23**				
		04:49 - 06:18	**DAF5648** hämtar ZOS filer från **202.120.189.223**	SYS3	Händelse
		09:00	Möte hos Säpo		
		08:00	Adderade nät till blacklistningen av SYS3	SYS3	Åtgärd
		13.00	Möte hos Säpo		
		14:30	Revokering av 14000 RACF-kpåto genomförd	SYS19	Åtgärd
		15:30	Revoke av 13 Logica user samt byte av passord på 40 Logica user	SYS3, SYS19	Åtgärd
Lö	**2012-03-24**				
		-	Arbete Logica/Applicate med framtagande av rapport		
		04:49 - 06:18	user DAF5648 hämtar ZOS filer	SYS3	Händelse
		06:00	User DAF5648 loggar in på TPX via Telnet	SYS3	Händelse
		19:00	FTP blockerat helt från internet	SYS3	Åtgärd
		20.30	FTP whitelisting etablerad	SYS3	Åtgärd

		20:30	Utökad filtrering från internet till SYS3 etablerad	SYS3	Åtgärd

logica
be brilliant together

Dokumenttyp
Rapport
Område
Säkerhet

Utredningsrapport

Sammanfattning

Detta dokument avser besvara ett antal specifika frågor ställda av Rikspolisstyrelsens verksamhetsskyddsenhet. Innan frågeställningarna avhandlas så ges en allmän bakgrundsbeskrivning.

Ärendet gäller ett datorintrång med tillhörande informationsläckage i en såkallad stordatormiljö som drivs av infrastrukturleverantören Logica. Stordatorn består av flera s.k. partitioner där två stycken av dessa (SYS19 och SYS3) idag är konstaterat utsatta för intrånget. Den ena av partitionerna (SYS19) används exklusivt av företaget Applicate som är förmedlare och förädlare av stora informationsmängder, bland annat personregister. Denna information tillhandahålls från företag och myndigheter samt säljs till företag och myndigheter. Den andra partitionen SYS3 är delad mellan flera verksamheter, bland annat Logica internt, Applicate, Skatteverket/Kronofogden samt ett antal andra företag.

Onsdagen den 7e mars upptäcker Applicate och Logica att det sker ovanliga aktiviteter i datormiljön. Efter att en liten grupp personer utfört en snabbutredning och samordnad aktivitet under natten så spärras vissa konton i systemet. På morgonen utökas gruppen och mer ansvariga informeras. Under de därpå kommande dagarna utförs incidentinsatser samt olika typer av forensisk undersökningar för att förstå innebörd och omfattning av incidenten. Den 13e mars har utredningen konstaterat att händelserna pågått sedan redan den 25e februari 2012.

Den 16 mars kopplar Logica in IBMs internationella incidentutredare och säkerhetsspecialist. Den 19 mars är bilden såpass klar att en polisanmälan inlämnas från Applicate till SÄPO.

Intrången har skett dels via existerande filöverföringstjänster baserade på FTP-funktionen, dels via interaktiv inloggning via ordinarie fjärrinloggningsfunktion, samt slutligen via av angriparna placerade bakdörrar. Intrången har varit ofta skett i kombination med stora datauttag ur systemen. Vidare har intrång och missbruk skett via Applicate webbtjänster. Missbruket har bland annat omfattat obehöriga kreditupplysningar.

Utredningen konstaterar att det finns beröringspunkter, såsom vissa gemensamma konton mellan de två stordatorpartitionerna, vilket möjliggör att angripare kan komma åt information i bägge partitionerna i de fall angriparen haft turen att komma över just ett av dessa konton. Vilket de tyvärr hade gjort.

Uppskattningsvis 10000 filer/dataset[1]:s har hämtats ut från SYS19 av obehöriga personer. Uppskattningsvis 600 filer/dataset:s har hämtats ut från SYS3 av obehöriga personer. Bland filerna/dataset som hämtats ut finns olika typer av företagsuppgifter, systemfiler inklusive certifikat, källkod samt personuppgifter, inklusive lista från 2007 över personnummer där filnamnet var "E897.SPAR.SKYDD".

Över 120 000 konton som från början fanns i användardatabasen RACF. Uttag har skett av användarinformation, av vilka utredningen från kvarglömda filer kunnat fastslå att uttagen saknat den viktiga lösenordsinformationen. Det kan dock inte uteslutas att denna information kommit ut. Via incidenthanteringsåtgärder så har ett stort av dessa konton kunnat spärras eller inaktiveras. Ca aktiva 70000 kundkonton finns idag kvar i systemet, samtidigt som vidare skyddsåtgärder och rensningar fortsätter.

Särskilt intressant att notera rörande kontouppgifterna är:

- *Det första kontot som idag har konstaterats vara knäckt och använts den 25e februari tillhör ett filöverföringsjobb från Sveriges riksdag. Hur någon obehörig kommit över denna inloggningsuppgift är inte klarlagt.*
- *Ett av kontona som använt flitigt av angriparna tillhörde ursprungligen Monique Wadsted, advokat som företrädde rättighetshavarna i den s.k. piratebayrättegången*
- *Flera av kontona som använts, inklusive Wadsted:s, har manipulerats i RACF-databasen att för få utökad behörighet.*

Arbetet med såväl incidentutredning samt systemuppsäkringar fortgår.

[1] Ett dataset kan innehålla en eller fler filer

logica
be brilliant together

Dokumenttyp
Rapport
Område
Säkerhet

Innehållsförteckning

Förklaringar

Applicate. IT-företag som är specialister på kundunika IT-lösningar innehållande stora datamängder.

Dataset. IBM-benämning för sparad data. Kan ses som ett arkivformat där själva dataset:et kan innehålla en eller fler filer.

Brandvägg. Nätverkssäkerhetsfunktion som används för att spärra, filtrera ut, släppa igenom samt logga nätverkstrafik. I Logic:a-miljön runt stordatorn finns ett stort antal brandväggar, vilka används bland annat för att hantera nätverkstrafik till/från de olika stordatorpartitionerna och kunders åtkomst till dessa.

FTP. File Transfer Protocol. Funktion för överföring av filer och s.k. dataset till och från Logica:s miljö. Denna filöverföringsfunktion har används av obehöriga för att hämta ut information från stordatorn. Likväl har funktionen används för att skicka upp filer till de två olika partitionerna.

Logica. IT-tjänste- och infrastrukturleverantör som tillhandahåller bland annat stordatortjänster.

Partition. Logisk segmentering och uppdelning av stordatorn i mindre enheter, vilka även kallas för LPARs (Logical Partitions). En LPAR innehåller definitionsmässigt RAM-minne, CPU, kringutrustning samt operativsystem[2]. Logica:s stordator är uppdelad i ca 25 partitioner.

PI. Påloggning InfoTorg**.** Behörighetsdatabas för webbgränssnittet som är kopplad mot RACF.

RACF. Behörighetsdatabas i stordatormiljön som innehåller användarnamn, lösenordsinformation, behörighetsinformation, kopplingar mot system och applikationer med mera.

SMF. System Management Facility är en IBM-metod för att övervaka och ta ut aktivitetslogg.

Stordator är en större och kraftfull datorresurs av märket IBM. Stordatorn är logiskt uppdelad i s.k. partitioner för att kunna hantera resurser, kunder, användning, etc. Logica:s stordator är fysiskt placerad i Logica:s anläggning i Bromölla.

2

http://publib.boulder.ibm.com/infocenter/zos/basics/topic/com.ibm.zos.zmainframe/zconc_mfhwsyspart.htm

Svartlistning. Lista över explicit spärrade IP-adresser som förhindras komma in till bestämda nättjänster i stordatormiljön. *Se även vitlistning*.

SYS3. Partition i stordatorn som delas av ett antal olika verksamheter, däribland Logicakunder och Logica internt. Bland de kunder som återfinns i SYS3 är Skatteverket/Kronofogden. SYS3 används till bland annat hantering av stora utskriftsjobb, vilka överförs från kunder.

SYS19. Partition i stordatorn som används av Applicate för sin informationsbehandling.

TSO. Time Sharing Option. Interaktivt exekveringsmiljö i IBM stordatorn under z/OS.

TPX. En sessionshanterare/menysystem som används för att koppla sig mot olika IBM applikationer.

USS. UnixSystemServices. Exekveringsmiljö i stordatorn som baseras på operativsystemet UNIX med IBMs tillägg för att integreras

- med traditionella IBM-funktioner ,såsom RACF-behörighetssystemet eller spårdatafunktionen SMF
- andra IBM exekveringsmiljöer (exempelvis TSO och CICS)

Vitlistning. Lista över explicit tillåtna IP-adresser som tillåts komma in till bestämda nättjänster i stordatormiljön. *Se även svartlistning*.

zOS. Operativsystem för IBM stordatormiljö vilken är värdmiljö för andra IBM-system såsom USS, TSO, CICS, mfl. Är en vidareutveckling av IBMs traditionella operativsystem OS/390 och MVS.

Status om intrånget är stoppat eller pågående

Attackytan har minskats genom ett antal tekniska skyddsåtgärder.

Intrångsförsök mot SYS19 är hanterat genom whitelistning av FTP-trafik från godkända IP-adresser samt bortfiltrering av protokoll som tidigare använts för intrång (telnet-trafik samt trafik på port 443). Övrig trafik som inte konstaterats som legitim har filtrerats bort.

Intrångsförsök mot SYS3 är hanterade genom whitelistning av all trafik mot systemet samt bortfiltrering av övrig trafik som inte är legitim.

Alla systemadministratörskonton har bytt lösenord, kompromitterade administratörskonton är utbytta.

Kontinuerlig övervakning av systemadministratörers inloggningar sker där larm går direkt till logicas övervakning, övervakning av misslyckade inloggningar (6st fel inom 30 sekunder).

Senast konstaterade intrång i SYS3 inträffade morgonen 23/3 via FTP och telnet. Senast konstaterade intrång mot SYS19 skedde den 16/3 via Telnet.

Inga nya intrångsförsök mot webbservrarna har kunnat identiferats.

Mot bakgrund av att den tillgängliga attackytan minskats avsevärt samt att utökad övervakning etableras bedömer Logica risken för nya oupptäckta intrångsförsök som liten.

I TSO görs följande loggning:
- SYSLOG, på/av loggning, utförda kommandon (begränsad)
- SMF, Förbrukning, tider etc.
- RACF, På/Av loggning, Loggning mot data set med AUDIT påslagen
- OPS/MVS, jobbinforamtion, påloggningar larm mm.

Vilka åtgärder har gjorts när

Se bifogad händelse och åtgärdslogg.

Vilka delar är fortfarande inte utredda

Se separat handlingsplan

Detaljinformation om känd information som är avslöjad

Beskrivning av innehåll i de filer som kopierats ut ur respektive system.

SYS19

- SPAR (Statens person och adressregister) information, lista på urval av personnummer för personer födda 1964 och senare.
- InfoTorg faktureringsinformation – Fakturering antal transaktioner per kund.
- PI (påloggning InfoTorg) – Filer som skickas in till LIME (CRM system). All information om kunder i InfoTorg och dess behörigheter.
- Infodata (Posten) – Adressmatchingar
- InfoTorg(PWC) – Spec på projektmärkning för vidarefakturering
- Polisen – 2 miljoner personnummer, enbart.
- Applicate (Radiotjänst) – Faktureringsinformation
- InfoTorg/Infodata/Polisen – Faktureringsinformation, transaktionstyp och antal.
- Polisen – Transaktionsstatistik från 2006
- Infodata – tre(3) dataset där filnamnet innehåller texten ”skyddade”. Dataseten är från år 2007. 10 793 personnummer total i filerna, en kopia och två original har hämtats ut. Dvs tre dataset.
- Applicate (blandade kunder) – Faktureringsstatistik
- Infodata – dataset innehållande personnummer i relation till varandra
- InfoTorg – BASUN (företagsinformation från SCB). Grundinfo, namn, juridisk form, storlek på företag etc.

- Filer med lösenord och användarnamn – en fil med vissa användarnamn och grupptillhörigheter har skapats av angriparen och kopierats ut ur systemet. I stordatorsystemen ligger lösenord lagrade, krypterat, i en stor binärfil. Under undersökningen av systemet kan Logica konstatera att en komprimerad fil med ett namn liknande binärfilens har kopierats ut från systemet. Den

komprimerade filen har sedan raderats. Logica har inte kunnat återfinna den komprimerade filen på backuper etc men gör bedömningen att det är sannolikt att lösenordsfilen i komprimerad form kopierats ut ur systemet.

SYS3

- FLISTEST – Handelsbankens fakturor till sina kunder 2006 och 2007 (test mtri.)

- Enligt Kronofogdemyndigheten har ca 40 klartextfiler innehållande kunder och gäldenärer som normalt skickas till unixsystemen kopierats ut från SYS3. Filerna innehåller personnummer, skuld, vem som personen är skyldig. Filerna innehåller även uppgifter som gäldenärer med skyddade identiteter.
- Vidare har betalningsfiler till Swedbank samt sigill för signering av utbetalningsfiler kopierats ut ur SYS3, sigillet är dock utbytt.
- Cobolkoden till programmet Navet har kopierats ut tillsammans med KFM's Navet-certifikat. Koden kan användas av inkräktaren för hitta svagheter och sårbarheter i applikationen Navet. Applikationen är dock endast tillgänglig från SKV nät och är inte publikt tillgänglig.

Vilken information som kan vara påverkad – samverkan med berörda parter

Skyddade personnummer dataseten måste utredas tillsammans med Skatteverket och övriga myndigheter.
Datasetet innehållande 2 miljoner personnummer måste utredas tillsammans med Skatteverket och eventuellt andra myndigheter.
Personer från 1964 och senare.
Skatteverket äger rådatat och har kompetensen runt detta.

Information om filer som kan vara manipulerade

Angriparna har under en period haft tillräcklig behörighet att i SYS19 manipulera all data, system och applikatoriskt. Man har haft en teoretisk möjlighet att manipulera system och funktioner i zOS, USS

etc. Men IBMs bedömning är att angriparna saknat adekvata kunskaper inom zOS för att genomföra det samma. Det finns idag inte tillräckligt med loggar för att gå tillbaka i tid för att säkerställa att man inte manipulerat system etc.

Det har konstaterats att angriparna haft tillräcklig kunskap för att elevera kontons behörigheter.

Manipulation av filer kan dels ha skett via FTP och dels via de TSO-sessioner som angriparen upprättat. FTP-sessionerna är loggade och i dessa kan konstateras att filer inte förändrats. I TSO-sessionerna skedde vid tillfället för intrånget inte loggning av åtgärder varför Logica inte med säkerhet kan säga om förändringar skedde i dessa sessioner.

SYS3:
De filer som kopierats ut ur systemet via FTP har listats och skickats till berörda verksamheter.

Angriparen hade TSO-sessioner upprättade mellan 04:12 och 05:40 den 23/3 med usern DAF5648, under perioden hade usern tillgång till:

Dataset	Volume	Behörighet	Senaste Ref
D904.SONG.TEXT	MIGRAT2	READ	2009/05/26
E484.DAF1460.ISPCLIB	STN185	ALTER	2012/03/27
E484.DAF1460.TSOINIT.CLIST	STN207	ALTER	2012/03/27
E484.DAF1489.TPXLOAD	STN190	ALTER	2009/02/05
E484.DRK.JLIB.BKP.D111101	SYS304	ALTER	2012/03/24
E484.DSS.DCOLLECT	??????	ALTER	
E484.DSS.DCOLLECT.E769	STN904	ALTER	2012/03/23
E484.DSS.DCOLLECT.G0230V00	MIGRAT2	ALTER	2012/03/19
E484.DSS.DCOLLECT.G0231V00	STN204	ALTER	2012/03/26
E487.DAF1490.INFOAVT1.READREAD	MIGRAT2	UPDATE	2012/03/10
E487.DAF1492.ADMGDF	MIGRAT2	UPDATE	2011/04/18
E487.DAF1492.ISPF.PLUSOPT	MIGRAT2	UPDATE	2007/12/06
E487.DAF1492.SAS9.DSSKEYS	MIGRAT2	UPDATE	2007/12/06
E487.DAF1492.SAS9.SASUSER	MIGRAT2	UPDATE	2008/01/03
E487.DAF1492.SRCHFOR.LIST	MIGRAT2	UPDATE	2011/04/19
E487.DAF1492.SRCHFOR.LIST.SASJOBB	MIGRAT2	UPDATE	2009/02/11
E487.DAF1492.TSOINIT.CLIST	MIGRAT2	UPDATE	2011/04/19
E487.DAF1572.ADMGDF	STN204	UPDATE	2012/03/26
E487.DAF1572.CNTL	STN214	UPDATE	2012/03/14
E487.DAF1572.CNTL.X19	MIGRAT2	UPDATE	2010/11/03
E487.DAF1572.CNTL.Y19	MIGRAT2	UPDATE	2010/11/03

E487.DAF1572.DOK	MIGRAT2	UPDATE	2011/07/07
E487.DAF1572.ISPF.PLUSOPT	MIGRAT2	UPDATE	2008/02/07
E487.DAF1572.JCL	MIGRAT2	UPDATE	2012/02/21
E487.DAF1572.JCL.S19.F084	MIGRAT2	UPDATE	2012/02/21
E487.DAF1572.JCLSVDC	MIGRAT2	UPDATE	2009/10/01
E487.DAF1572.JCLS19	MIGRAT2	UPDATE	2012/02/20
E487.DAF1572.JUL.DOK	MIGRAT2	UPDATE	2009/10/01
E487.DAF1572.JUL.PGM	MIGRAT2	UPDATE	2009/10/01
E487.DAF1572.JULJCL	MIGRAT2	UPDATE	2009/10/01
E487.DAF1572.KYRKAN.CNTL	MIGRAT2	UPDATE	2008/02/07
E487.DAF1572.PROGRAM	MIGRAT2	UPDATE	2011/04/06
E487.DAF1572.SAS.CNTL.SYS12	MIGRAT2	UPDATE	2008/02/07
E487.DAF1572.SAS.DRK.JLIB	MIGRAT2	UPDATE	2011/11/15
E487.DAF1572.SAS.E897JCL	MIGRAT2	UPDATE	2011/11/15
E487.DAF1572.SOURCLIB.MODLIB	MIGRAT2	UPDATE	2008/02/07
E487.DAF1572.SPFLOG5.LIST	STN903	UPDATE	2012/03/27
E487.DAF1572.SRCHFOR.LIST	STN178	UPDATE	2012/03/27
E487.DAF1572.SRCHFOR.LISTX	MIGRAT2	UPDATE	2006/11/27
E487.DAF1572.S19.D120221	MIGRAT2	UPDATE	2012/02/22
E487.DSS.DOC	MIGRAT2	UPDATE	2011/04/06
E487.DSS.DOK	MIGRAT2	UPDATE	2011/04/06
E487.DSS.DOKUMENT	MIGRAT2	UPDATE	2011/04/06
E487.FAKTPER	MIGRAT2	UPDATE	2008/01/03
E487.LOG.MISC	MIGRAT1	UPDATE	2012/03/20
E487.PRODTRAN.BATTSOPR	??????	UPDATE	
E487.PRODTRAN.BATTSOPR.G0061V00	MIGRAT2	UPDATE	2005/12/19
E487.PRODTRAN.BATTSOPR.G0062V00	MIGRAT2	UPDATE	2006/01/23
E487.PRODTRAN.BATTSOPR.G0063V00	MIGRAT2	UPDATE	2006/02/20
E487.PRODTRAN.BATTSOPR.G0064V00	MIGRAT2	UPDATE	2006/03/20
E487.PRODTRAN.BATTSOPR.G0065V00	MIGRAT2	UPDATE	2006/04/21
E487.PRODTRAN.BATTSOPR.G0066V00	MIGRAT2	UPDATE	2006/05/22
E487.PRODTRAN.BATTSOPR.G0067V00	MIGRAT2	UPDATE	2006/06/19
E487.PRODTRAN.BATTSOPR.G0068V00	MIGRAT2	UPDATE	2006/07/24
E487.PRODTRAN.BATTSOPR.G0069V00	MIGRAT2	UPDATE	2006/08/21
E487.PRODTRAN.BATTSOPR.G0070V00	MIGRAT2	UPDATE	2006/09/22
E487.PRODTRAN.BATTSOPR.G0071V00	MIGRAT2	UPDATE	2006/10/23
E487.PRODTRAN.BATTSOPR.G0072V00	MIGRAT2	UPDATE	2006/11/20
E487.PRODTRAN.DEB420	??????	UPDATE	
E487.PRODTRAN.FAKTURA.DB	MIGRAT2	UPDATE	2006/11/20
E487.PRODTRAN.INFODATA	??????	UPDATE	
E487.PRODTRAN.PROGRAM	MIGRAT2	UPDATE	2011/04/06

E487.QZ3.PGM MIGRAT2 UPDATE 2010/08/30

SYS19
De filer som kopierats ut ur systemet via FTP har listats och skickats till Applicate och myndigheterna.

Angriparen hade TSO-sessioner upprättade mellan 10/3 17:00 och den 16/3 07:30 med en user som enbart hade tillgång till USS-filsystemet men med höga behörigheter. Kartläggning av filer som vid tiden för angreppet låg i USS-filsystemet pågår, klart såhär långt är:

USS-delarna av SYS19 används för filöverföring via bland annat sftp.

Alla delar i USS-operativsystemet som innehåller binärer är monterade read-only och kan därför inte lätt ändras. Inga user-kataloger (hemkataloger) är normalt synliga eftersom dessa monteras upp vid försök till åtkomst, för att få tillgång till userkataloger behöver angriparen först veta vilka dessa är.

Angriparen har kopierat delar (hur stor del?) av användardatabasen till en textfil och därmed fått tillgång till vissa userid vilkat kunnat användas till att leta igenom dessa användares userkataloger efter intressant information.

Angriparen hade via TSO tillgång till zOS mellan 15/3 19.00 och 16/3 10.00 med usrarna WMROCAR, DAF1017, WAHS006. Via dessa usrar har angriparen tillskansat sig mycket höga behörigheter (operation och system special) i SYS19 vilka ger tillgång till behörighetsadministration och dataåtkomst för större delen av SYS19.

Information om hur eskaleringen gått till vid intrånget

SYS19
Mellan den 25/2 och den 10/3 17.10 har inkräktaren haft möjlighet att med olika usrar använda FTP för åtkomst till systemet.

Den 10/3 kl 17.10 görs en förändring av /etc/initd.conf som leder till att en telnet-demon svarar på port 443 vilken är tillgänglig från Internet.

I USS görs en förändring av inetd.conf så att det går att köra att shell (när hände detta?) som SUPERUSER direkt vilket innebär att angriparen

får höga behörigheter för behörighetsadministration men inte dataåtkomst utan att ange lösenord.

Genom att ändra ID till WMROCAR kan angriparen använda RACF-kommandon för att ge WAHS006 system-special, operation samt uid0 vilket ger mycket höga behörigheter i systemet.

21:14 lyckas angriparen logga på systemet med TSO vilket inte ger mer behörigheter men tillgång till ett menysystem.

Klockan 07:21 revokeras WAHS006, klockan 09:35 revokeras alla users med system-special och 10:02 tas RACF authority bort från WAHS006 och DAF1017.

SYS3
På SYS3 har vad Logica i dagsläget känner till, ingen elevering av behörigheter skett.

Information om de ca 10 administratörskontona

I samband när intrånget skedde och User's med "special behörigheter" kapades ändrades behörigheten till att enbart 2 User hade kvar special i SYS3 samt i SYS19 togs special bort hos alla och två nya User skapades med special

Listningen nedan omfattar användaridentiteter som har behörighetsnivån Special.

'*' = Revokerad

SYS3 innan intrånget:

CEA	Common Event Adapter
*DAFRACF	Superior Racf Admin
E927REFR	E927REFR
*JDAUSER	Säkerhetsadm
*VX17501	Mats Wikensten
*VX18150	Svante Sundelin
*VX18171	Bengt Björkqvist
*VX19133	Bengt Gellingskog
*VX21836	Christer Hedlund
*VX21841	Kalle Aronsson
*VX22617	Claes Borgh

*VX31749	Örjan Lindholm
WMALHUN	Alan Hunter, +46 733 984301
WMROCAR	Roland Carlsson, +46 73 3984570
WMSTOTT	Staffan Ottosson, +46 73 3984255
WMTHOHR	Thomas Ohrås, +46 73 3984279

SYS3 efter:

*DAFRACF
*JDAUSER
*VX17501
*VX18150
*VX18171
*VX19133
*VX21836
*VX21841
*VX22617
*VX31749
WMALHUN
WMTHOHR

SYS19 innan intrånget:

CEA	Common Event Adapter
DAFRACF	Superior Racf Admin
E927REFR	E927REFR
WMALHUN	Alan Hunter
WMROCAR	Roland Carlsson
WMSTOTT	Staffan Ottosson
WMTHOHR	Thomas Ohrås

SYS19 efter:

WMXLOG1
WMXLOG2

Information om vilka konton som användes vid utskickning av data

25/2 Första kända användarkonto som användes var ett konto från Riksdagen (AVIY356). Denna användare har via zOS och USS börjat FTP'a dataset och filer från/till Logica ca 400 st.

Vi har konstaterat att en mängd konton använts över tid och att några manipulerats till att erhålla special och superuser behörighet i systemen. Mer runt detta beskrivs i händelserapport och tidslinje beskrivningen.

FTP-usrar – SYS19

ASI0930	NILSSON PER
ASI0936	STÅHL PER
AVIY356	RIKSDAGSF-ODIN
AVIY357	KONSUM-MALMFÄLTEN
BSN0058	SUNDELIUS JEN
NUS	SPARDRIFT
SPRBI01	SALES PARTNER PGM T
SPRBI08	SALES PARTNER PGM P
SPRBI45	SALES PARTNER PGM HE
WAHS006	WADSTED MONIQUE

Usrar som använts för TSO-sessioner – SYS19

WAHS006	WADSTED MONIQUE
DAF1017	KARLSSON ROSITA

FTP-usrar – SYS3

NUS	SPARDRIFT

Usrar som använts för TSO-sessioner – SYS3

DAF5648	STÅLSTIERNA CARINA

Information om vilka IP-adresser som användes vid utskickning och vilken ISP som användes

Information har transporterats till VPS (Virtual private server) providers i bl.a. Tyskland (t ex 178.18.243.27) men företrädesvis har IP-adresser i Kambodja (Pnomh Pen) använts. Bland annat har man använt ett superuser-konto (högsta behörighet på systemen) från 27.109.118.33 och 123.108.250.50 samt ett reguljärt systemkonto från 203.176.141.205 (alla adresser finns i Kambodja). Enligt uppgift ska en stor del av denna aktivitet pågått runt perioden 10-15 mars 2012. Det finns även informationstransaktioner mot den svenska ISPn Bahnhof.

IP-adresser som accessat och överfört information:

46.50.183.5 (JSC "Zap-Sib TransTeleCom", Novosibirsk, Ryssland)
203.176.141.205 (MEKONGNET INTERNET SERVICE PROVIDER, Kambodja)
27.109.118.33 (DTV-STar Co.,Ltd, Kambodja)
123.108.250.50 (Neocomisp, Kambodja)
178.18.243.27 (QQ-Nova, Tyskland)
46.59.51.181 - h-51-181.a328.priv.bahnhof.se (Bahnhof, Sverige)
85.228.54.229 (Bredbandsbolaget)
178.174.180.144 (Tyfon Svenska AB)
202.120.189.223 (Tongji University, Shanghai)
93.186.170.54 (Inline Internet Online Dienste GmbH, Tyskland)

Ytterligare IP-adresser, oklart accessmöjligheter (loggats i brandvägg):
124.248.174.161 (Cogitel, Kambodja)
124.248.187.100 (Cogitel, Kambodja)

Reflektion:
Även om det gjorts ett större antal på loggningar på storsystemen från exempelvis Tyska ip-adresser så är Riksdagen, Kambodja och Bahnhof mer intressant än något annat och bör prioriteras i den mån det går. Övriga IP-adresser i Ryssland och Tyskland tillhör troligtvis server-/vps-provider.

Vilken sorts trafik som utgjorde slagningarna mot dalarna

En översiktlig undersökning har genomförts av ett urval av sökbegreppen som använts på Infotorg. Som tidigare nämnts har det genomförts sökningar på Jim Keyzer, Gottfrid, PRQ Kommanditbolag, RPS registrerade bilar i bilregistret m.m.

Nedan följer ett kort urval med förklaring:

Lennart Nordh: svensk representant i rymdstyrelsen Cospar
Mer info: http://www.snsb.se/sv/Mediebank/Forskare/SRS/

Joacim Engvall: Kan vara en av angriparna som söker på sig själv (?)
Se: https://www.facebook.com/groups/92072346644/members/

Martin Bergström: Polis som ingrep mot filmare och tvingade till radering

Fredrik Jeanson: Arbetar på supporten hos MOSMS

Håkan Marklund: Robinsondeltagare

Mikael Persbrandt: Skådespelare

Robin Åström: Verkar vara en tekniker som certifierar sig, se länk:
Mer info: http://robinastrom.blogspot.se/

Liisa Bernadt: Kattägare och förskolelärare, möjligtvis i Norrtälje.
Mer info: http://www.rexringen.nu/utstallningar/titelkatter/crx-bis.html

Erik Turlen: Åtalades för knivhugg i Ludvika, bor i Smedjebacken.
Mer information: http://vgnt.se/tre-man-atalade-for-knivhugg-i-ludvika/

Angelika Brorström: Bloggerska i 17-årsåldern
Mer info: (omnämns)
http://emiliamagdalena.blogg.se/2012/january/utkast-jan-8-2012.html

Reflektion:
Troligtvis unga personer som fått information om inloggningskonton på infotorg av de mer kompetenstunga huvudaktörerna. Dessa unga personer som sökt på kändisar, en bloggerska och personer i Ludvika/Smedjebacken har troligtvis inte haft en susning om de eventuella konsekvenserna av sökningarna. Troligtvis förankring i Ludvika/Smedjebacken.

Vilka andra organisationer är påverkade

Efter genomgång av utkopierade dataset har hittils kunnat konstateras att berörda organisationer begränsas till:

- Logica
- Applicate
- Skatteverket
- Kronofogdemyndigheten

logica
be brilliant together

Dokumenttyp
Rapport
Område
Säkerhet

Händelse och åtgärdslogg

	Datum	Tidpunkt	Händelse	System	Typ
Lö	2012-02-25				
		04.55 - 06.47	user **AVIY356** från IP **178.18.243.27** hämtar USS filer	SYS19	Händelse
Sö	2012-02-26				
		13.45....23.51	samma user/IP hämtar USS and ZOS filer	SYS19	Händelse
To	2012-03-01				
		10.45....15.34	samma user/IP hämtar/lagrar USS filer + hämtar ZOS filer	SYS19	Händelse
Sö	2012-03-04				
		02.25....09.15	user **BSN0058** på IP **85.228.54.229** hämtar ZOS filer	SYS19	Händelse
		07.09 – 10.42	user **BSN0058** på IP **178.174.180.144** hämtar ZOS filer	SYS19	Händelse
		08.13....08.59	user **BSN0058** på IP **178.18.243.27** hämtar ZOS filer	SYS19	Händelse
		10.25....12.58	user **BSN0058** på IP **46.59.51.181** hämtar ZOS filer	SYS19	Händelse
Må	2012-03-05				
		12.55....19.28	user **BSN0058** på IP **178.18.243.27** hämtar USS filer	SYS19	Händelse
Ti	2012-03-06				
		03.18....03.59	user **BSN0058** på IP **46.59.51.181** hämtar ZOS filer	SYS19	Händelse
		17.59....20.45	user **BSN0058** på IP **46.59.51.181** hämtar ZOS filer	SYS19	Händelse
On	2012-03-07				
		-	Logica/Applicate konstaterar högt CPU-uttag	SYS19	Händelse
		23.27 - 23.34	user **SPRBI45** på IP **46.59.51.181** hämtar ZOS/USS filer	SYS19	Händelse
		-	Applicate kontaktar Anki Nordin för uppgifter om **BSN0058** (infotorg)	SYS19	Åtgärd

		12:35	**BSN0058** revokerad av Applicate	SYS19	Åtgärd
To	**2012-03-08**				
		09:20	Racf– **SPRBI45** revokerad avApplicate	SYS19	Åtgärd
		-	Telefonmöte Logica Applicate, säkerhetsutredning startas		Åtgärd
		13.40 - 13.46	user **SPRBI08** på IP **46.59.51.181** hämtar USS filer	SYS19	Händelse
		14.01 –14.06	user **SPRBI01** på IP **D64** hämtar USS filer	SYS19	Händelse
		14.02	många **SPRBInn** users revokerad av Applicate	SYS19	Åtgärd
		14.23 –14.42	user **ASI0936** på IP **46.59.51.181** hämtar USS filer	SYS19	Händelse
		14.50	Racf– **ASI0936** revokerad av Logica	SYS19	Åtgärd
Fr	**2012-03-09**				
		fm	Logica identifierar under förmiddagen misstänkt trafik med tillhörande IP-adresser i brandväggsloggar.		Åtgärd
		16:00	Blacklistning i SYS19 FW - deny any för vissa nät	SYS19	Åtgärd
		em	Möte Applicate/Logicaresurser efterfrågas under helgen som övervakar brandvägg och CICS efter misstänkt beteende.		
		em	En kommunkationsresurs samt en CICS resurs allokeras för att övervaka systemet under helgen	SYS19	Åtgärd
		20:30	Ytterligare blacklistning i SYS19 FW	SYS19	Åtgärd
		kväll-natt	Applicate kör en batch för att revokera ett större antal userids	SYS19	Åtgärd
Lö	**2012-03-10**				
			Logica informerar Applicate om konto **AVIY356** och utreder konto **NUS.**		Åtgärd
			Applicate begär lista på IP som kör FTP mot systemet.		Åtgärd
			Logica tar fram begärd IP lista och delger Applicate.		Åtgärd
		01.00....07.01	userid **AVIY356** på IP **203.176.141.205** hämtar/lagrar USS filer	SYS19	Händelse

		06.32 – 07.30	Senare information pekar på att inetd.conf startade en telnetjänst på port 443 vilken användes av **AVIY356** kl 17.09.	SYS19	Händelse
		09.34....12.15	userid **AVIY354** på IP **203.176.141.205** hämtar USS filer	SYS19	Händelse
		12.39....15.04	userid **NUS** på IP **203.176.141.205** hämtar ZOS filer	SYS19	Händelse
		12.42	Misslyckade påloggning med ftp och användare **NUS** från **124.248.187.150**	SYS3	Händelse
		12.45	RACF Violations vid listning av kataloger	SYS3	Händelse
		13.02	Racf – flera AVI users revokerade av Applicate	SYS19	Åtgärd
		15.10	Ett par USS filer hämtas från **93.186.170.54**	SYS3	Händelse
		16.35	Racf - userid **NUS** revokerad av Applicate	SYS19	Åtgärd
		17.09	Racf – **AVIY356** misslyckas att ändra /etc/inetd.conf	SYS19	Händelse
		17.10	/etc/inetd.conf ändrad till att använda port **443** så den körs som SUPERUSER utan att kräva lösenord, oklart när den senare användes.	SYS19	Händelse
		17.20	Misslyckade påloggningar från **194.23.61.151**	SYS3	Händelse
		18.59	Racf - user **AVIY356** revokerad av Applicate	SYS19	Åtgärd
		19.22....19.57	Racf - 4 försök att logga på som **WMOVLAE** – misslyckas	SYS19	Händelse
		19.30 –19.31	user **AVIY357** på IP **27.109.118.33** lagrar /var USS filer Filen /var/a finns fortfarande och visar att användaren inte körde som uid(0)	SYS19	Händelse
		19.47	Ett stort antal USS-filer hämtas från **194.23.61.151**	SYS3	Händelse
		23:18	Racf - user **ASI0930** revokerad av Applicate	SYS19	Åtgärd
Sö	**2012-03-11**				
			Logica ser att någon försöker logga in med en serie av konton och informerar Applicate. Applicate kontaktar Logica och ber om hjälp med att implementera en IP-adress whitelist för FTP.		Åtgärd
			Logica informerar Applicate om inloggningsförsök med en serie av konton.		Åtgärd

		10:30	restore av RACF-databasbackup från **03/09** av Logica på beställning av Applicate då batchen hade tagit bort för många users)	SYS19	Åtgärd
		11:36	Racf– flera AV och AS users revokerade av Applicate	SYS19	Åtgärd
		23:00	Whitelistning av SYS19 för FTP införs (modiferades löpande under veckan)	SYS19	Åtgärd
Må	**2012-03-12**				
			Möte under förmiddagen med Applicate som säger att de identifierat att systemfiler från USS har läckt ut. Applicate har sammanställt en lista på konton som misstänks vara kapade. Logica analyserar de läckta systemfilerna men anser inte att det utgör någpå direkt fara. Alla konton på Applicates lista har vid olika tillfällen spärrats.		Åtgärd
		19.33	Racf– 5 försök att logga på userid **WMOVLAE** mislyckas, id revokerat av Logica	SYS19	Händelse
Ti	**2012-03-13**				
			Avstämningsmöte med Applicate under förmiddagen. Samordningsmöte hos Applicate under eftermiddagen. Applicate har sett misstänkta aktiviteter i sina loggar från den 25 februari. Applicate ber Logica analysera loggar bakåt i tiden för att identifiera när intrånget skedde med kontolistan som grund. Den gemensamma bilden är att vi med de spärrade kontonen och whitelist har lyckats stänga ute angriparna. Logica sätter upp dagligen återkommande avstämningsmöte med Applicate. Analys av Applicates konton på listan bakåt i tiden för att identifiera när intrånget började samt allmän wildcard analys		Åtgärd
On	**2012-03-14**				
			Avstämningsmöte med Applicate under förmiddagen. Logica kan i sina loggar verifiera misstänkta aktiviteter från den 24 februari. Den gemensamma analysen fortgår.		Åtgärd

To	**2012-03-15**				
		11.21	2 USS-filer hämtas från **93.186.170.54**	SYS3	Händelse
		19.03	RACF - **WAHS006** eleveras till System-special, operations och UID(0). Detta gjordes av inkräktaren genom SU authority av SUPERUSER för att ändra ID till **WMROCAR** (utan att behöva använda lösenord) och sedan köra RACF-kommandon för att ändra **WAHS006.**	SYS19	Händelse
		19.19....21.05	Inkräktaren försöker köra TSO - utan framgång	SYS19	Händelse
		19.50 + 20.54	Racf-userid **WMROCAR** ändrar lösenord på **RPHAI30** och **KVV015**	SYS19	Händelse
		20.25....	userid **WAHS006** på IP **217.150.174.80** hämtar ZOS filer	SYS19	Händelse
		20.44	**WAHS006** skriver group och user-information från RACF-databasen till /var/users.txt och hämtar den. antalet grupper (481) antyder att listan skapades av groups-special userif för gruppen RYÅSY	SYS19	Händelse
		21.04	Racf- elevering av userid **DAF1017** till systemspecial, operations och uid(0)	SYS19	Händelse
		21.14	Inkräktaren lyckas logga på TSO med userid **DAF1017**– testar oper cmds	SYS19	Händelse
		22.21	hämtar /u/d610/rfvftp/1.tgz – skapad 22:20	SYS19	Händelse
		23:45	User **WAHS006** från IP **217.150.174.80** hämtar E897.SPAR.SKYDD	SYS19	Händelse
Fr	**2012-03-16**				
			Onödiga portar stängs i brandvägg (inkommande) och på systemet.		Åtgärd
			Applicate kallar till krismöte där de informerar att de sett att angriparen har använt administratörskonton i RACF för att tilldela kapade konton högsta behörighet samt flyttat 1,7 MB data från MVS till USS. Hela RACF databasen anses härmed kompromitterad.		Åtgärd
			Applicate och Logica påbörjar ett gemensamt arbete för att begränsa skadan och åtkomst till systemet. Flertalet möten hålls under dagen/kvällen.		Åtgärd
			Logica Incident Manager inkopplad.		Åtgärd

			Existerande whitelist i brandväggen krymps ytterligare.		Åtgärd
			Låga tröskelvärden för larmsättning över lag konfigureras.		Åtgärd
		08.06	Mycket många dataset kopieras ut	SYS19	Händelse
		07.21	Racf – **WAHS006** revokerad av Applicate	SYS19	Åtgärd
		09.35	Racf – **WMROCAR** (och andra med Special) Racf authority borttagna av Logica	SYS19	Åtgärd
		10.02	Racf – **WAHS006** och **DAF1017** Racf authority borttagna av Logica	SYS19	Åtgärd
		10.55 – 11.30	Racf – 2 nya racf admin ids skapade av Logica, gamla admin ids – auth borttagna	SYS19	Åtgärd
		13.00	OPS – alarm på logon på nya Racf-admin ids	SYS19	Åtgärd
		13:40	Blockering av trafik mot SYS19 port 443 för any	SYS19	Åtgärd
		19:00	IBM specialist inkopplad och arbete med IBM påbörjas	SYS19	Åtgärd
		-	Säkerhetsfunktipåen SERVERAUTH implementeras på systemet.	SYS19	Åtgärd
		20:00	Whitelistning av SYS19 klar för alla protokoll från internet	SYS19	Åtgärd
		-	Ett till nät med misstänkta IP:n spärras i brandväggen. ISP:n för dessa meddelas.		Åtgärd
		-	Kommunikationsförbindelsen mellan SYS3 och SKV överbelastad	SYS3	Händelse
Må	**2012-03-19**				
		21:52	Ett stort antal filer/dataset hämtas av user **NUS** från **93.186.170.54**	SYS3	Händelse
		kväll	Applicate registrerar polisanmälan hos Säpo		Åtgärd
Ti	**2012-03-20**				
		08:30	Applicates anmälan kompletteras		
On	**2012-03-21**				
		03:37	Sista kompletta datasetet hämtas	SYS3	Händelse
		08:20	Inloggningar i SYS3 identifieras av Logica	SYS3	Händelse
		08:42	Session "droppas" och användare **NUS** revoca's	SYS3	Åtgärd

		-	Blacklistning av SYS3 påbörjas	SYS3	Åtgärd
		14:30	Logica identifierar att filer med känslig information tillhörande SKV lämnat Logica	SYS3	Händelse
		15:00	Applicate informeras om att intrånget ökat i omfattning		Åtgärd
		17:00	SKV + KFM säkerhetschef informerad		Åtgärd
		17:50	Logica har kontakt med Säpo, Logica vill göra egen polisanmälan.		Åtgärd
		16:38	Nytt misslyckat påloggningsförsök av **NUS** från **111.92.242.65**	SYS3	Händelse
		20:00	förnyade intrångsförsök från nya source-adresser identifierade	SYS3	Händelse
		20:45	Ok från Applicate (Stefan) att köra nätscanning av de adresser som routas till Applicate.		Åtgärd
		Kväll	Portscanning av Applicates publika IP		Åtgärd
To	**2012-03-22**				
		10:15	Material (listor över dataset) skickat till KFM		
		11:30	Info från SKV om att navet kan vara omfattat		
		11:40	Eskaleringsmöte Logica SE management, kontakt med Gerald + Steve		
		12:15	Logica har kontakt med Säpo ang ny riskbild		
		12:40	Starta sammanställning av vidtagna åtgärder		
		12:42	Preliminär bedömning att itwebbarna är sunda		
		-	Kontakt med SKV, troligen Navet-filer och certifikat men inte applkatipåsdata.		
		-	Kontakt SKV, man har verifierat att källkod och certifikat är berörda men inte applikationsdata.		

logica
be brilliant together

Dokumenttyp
Rapport
Område
Säkerhet

		15:00	Möte med SKV/KFM: Filer har gått ut med personuppgifter kopplade till gäldenärer, de med skyddad identitet är särskilt flaggade SKYDDAD Källkod och certifikat till Navet har gått ut, certifikatet skulle kunna användas för falsk autenticering, källkoden för att identifiera säkerhetsbrister. Betalningsfiler och sigill mot Swedbank har kopierats ut, nytt sigill är beställt. Kritiskt är att integritet i filer inte påverkats.		
		15:50	Kontakt med säpo ang förändrad riskbild, inga särskilda krav från säpo på hantering av loggar eller information för närvarande		
Fr	**2012-03-23**				
		04:49 - 06:18	**DAF5648** hämtar ZOS filer från **202.120.189.223**	SYS3	Händelse
		09:00	Möte hos Säpo		
		08:00	Adderade nät till blacklistningen av SYS3	SYS3	Åtgärd
		13.00	Möte hos Säpo		
		14:30	Revokering av 14000 RACF-kpåto genomförd	SYS19	Åtgärd
		15:30	Revoke av **13** Logica user samt byte av passord på 40 Logica user	SYS3, SYS19	Åtgärd
Lö	**2012-03-24**				
		-	Arbete Logica/Applicate med framtagande av rapport		
		04:49 - 06:18	user DAF5648 hämtar ZOS filer	SYS3	Händelse
		06:00	User DAF5648 loggar in på TPX via Telnet	SYS3	Händelse
		19:00	FTP blockerat helt från internet	SYS3	Åtgärd
		20.30	FTP whitelisting etablerad	SYS3	Åtgärd

logica
be brilliant together

Dokumenttyp
Rapport
Område
Säkerhet

		20:30	Utökad filtrering från internet till SYS3 etablerad	SYS3	Åtgärd

logica
be brilliant together

Type of document
Utredningsrapport

Subject
Sammanfattning

Utredningsrapport
Dataintrång Mainframe

logica
be brilliant together

Type of document
Utredningsrapport
Subject
Sammanfattning

Innehållsförteckning

Sammanfattning

Ett användarkonto som Riksdagen använder för dagliga transaktioner användes för det första intrånget. Angriparen exporterade då inloggingsuppgifter som sedan har använts vid upprepade intrång. Angriparen har efter att ha tillskansat sig hög systembehörighet kunnat hämta känslig information via bl a FTP. Attackerna har skett från IP-adresser belägna i ett större antal länder.

Atackerna har omfattat partitionerna SYS19 och SYS3. Viss trafik har gått via webbservrar som används för tjänsten InfoTorg. Angriparen har under viss tid haft tillgång till högsta möjliga behörighet för både SYS19 och SYS3.

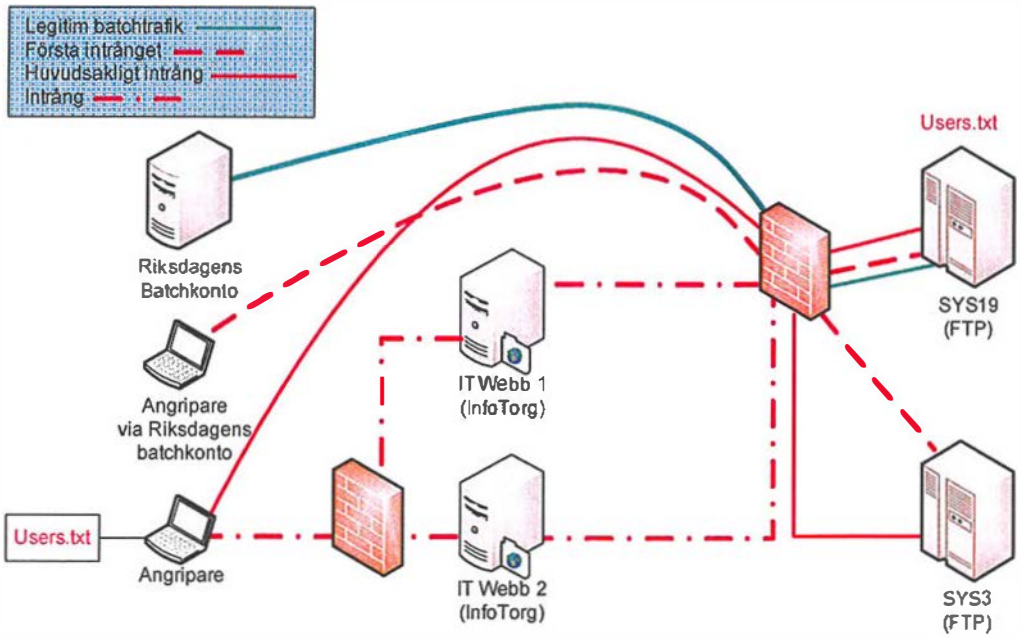
Attacken upptäcktes genom ett larm om hög CPU-belastning med okänt ursprung eskalerades efter inledande analyser till berörda kunder. SYS19 och SYS3 har därefter säkrats så att attacken har avvärjts. Analyser har visat att applikationsdata och systemfiler har hämtats via FTP. Attacken har avvärjts framför allt genom s k blacklistning och whitelistning av IP-adresser.

Sårbarheter och brister har identifierats i bland annat hantering av behörigheter, brandväggsfiltrering samt i konfigurationen av stordatorns operativsystem. Genomförda kortsiktiga åtgärder har syftat till att begränsa attackytan minska sårbarheten och inkluderar förutom nämnda black- och whitelistning översyn av användarkonton hos berörda organisationer, analyser av loggar och åtgärder för att höja systemets säkerhet. Kod som angriparen har lämnat efter sig har avlägsnats. Logica håller på att ta fram förslag för mer långsiktiga åtgärder. Jämförelser görs också med en tidigare säkerhetsincident i samma mainframemiljö.

Logica rekommenderar att de långsiktiga åtgärderna genomförs inklusive en översyn av systemdesignen.

1 Tillvägagångssätt

1.1Det inledande intrånget



Riksdagen har ett batchkonto som används för dagliga transaktioner till SYS19. Detta konto användes för det första intrånget i SYS19. Väl inne kunde angriparen bygga upp filen users.txt genom systematiska alfabetiska wildcard-sökningar. Filen innehåller ett extrakt av delar av RACF-databasen och hämtades från SYS19 via bl a FTP. Med hjälp av users.txt har angriparen därefter kunnat göra intrång i SYS19 och SYS3 samt webbservrarna IT Web1 och IT Web2 som hostar tjänsten InfoTorg.

1.2Aktiviteter under intrånget

Sedan det första intrånget har angriparen försökt och lyckats att elevera rättigheter/behörigheter för användarkonton i mainframe-miljön. På detta sätt har man fått ökad tillgång till de båda partitionerna. Man har lyckats roota först SYS19 och sedan SYS3. Detta innebär att man har tagit full kontroll över SYS19 och USS-delarna av SYS3. Angriparen har därefter genomsökt systemen, kopierat filer till temp-kataloger och exporterat ut filerna via bl a FTP.

Försök till intrång pågår fortfarande från IP-adresser som Logica har spårat till olika delar av världen, till exempel Tyskland, Ryssland Kina, Mongoliet och Kambodja. Logica har löpande arbetat med whitelistning och blacklistning för att minska sårbarheten och reducera attackytan.

1.3Trafikflöden under angreppet

Under intrånget gick trafik i huvudsak baserat på filöverförings-protokollet FTP mellan SYS3/SYS19 och de datorer som angriparen utnyttjade för intrånget, vilka nät angriparens datorer kom ifrån är dokumenterat under punkten som behandlar IP-adresser och IP-nät.

Mellan SYS19 och angriparens dator har utöver FTP en liten mängd Telnet-trafik utväxlats, denna trafik härrör till de sessioner under vilka angriparen eskalerade sina behörigheter i SYS19.

Mellan SYS3 och angriparens dator har uteslutande FTP-trafik utväxlats, inloggning via TSO har konstaterats men inga kommandon har körts. Den bakdörr som angriparen etablerade den 20/3 har medfört att viss kommunikation etablerats från SYS3 mot adresser på Internet bland annat de adresser i Tyskland som angriparen tidigare använt. En fullständig kartläggning av trafiken pågår.

1.4SYS19

25/2, Första kända användarkonto som användes var ett konto från Riksdagen (AVIY356). Denna användare har via zOS och USS börjat FTP:a dataset och filer från/till Logica, totalt ca 400 st.

Intrånget påbörjas den 25/2 då angriparen med ett konto tillhörande Riksdagen via FTP kopierar ut ett relativt stort antal filer ur SYS19 samt laddar upp ett mindre antal filer. Filerna kopieras bland annat ut till en dator med en IP-adress hos den Tyska internet-leverantören QQ-Nova. Filhämtningarna pågår, med olika användaridentiteter, i omgångar fram till den 16/3.

Den 10/3 kl 17.10 görs en förändring av /etc/initd.conf som leder till att en Telnet-service svarar på port 443 vilken är tillgänglig från Internet. Förändringen av inetd.conf kräver root-behörighet, det finns ett flertal hypoteser till hur angriparen skaffat sig dessa vilka för närvarande är under utredning.

I USS görs ytterligare en förändring av inetd.conf som medger åtkomst till en kommandoprompt med behörigheter motsvarande SUPERUSER direkt vilket innebär att angriparen får höga behörigheter för behörighetsadministration men inte dataåtkomst utan att ange lösenord.

Genom att starta kommandoprompten och ändra ID till WMROCAR kan angriparen använda RACF-kommandon för att ge WAHS006 behörigheterna system-special, operation samt uid0 vilket ger mycket höga behörigheter i systemet.

15/3 21:14 lyckas angriparen logga på systemet med TSO vilket inte ger mer behörigheter men tillgång till ett menysystem.

16/3 klockan 07:21 revokeras WAHS006, klockan 09:35 revokeras alla användarkonton med system-special och 10:02 tas RACF authority bort från WAHS006 och DAF1017.

Huvudsakliga användarkonton som använts för FTP-sessioner – SYS19

ASI0930	NILSSON PER
ASI0936	STÅHL PER
AVIY356	RIKSDAGSF-ODIN
AVIY357	KONSUM-MALMFÄLTEN
BSN0058	SUNDELIUS JEN
NUS	SPARDRIFT
SPRBI01	SALES PARTNER PGM T
SPRBI08	SALES PARTNER PGM P
SPRBI45	SALES PARTNER PGM HE
WAHS006	WADSTED MONIQUE

Huvudsakliga användarkonton som använts för TSO-sessioner – SYS19

WAHS006	WADSTED MONIQUE
DAF1017	KARLSSON ROSITA

Logica har analyserat körda batchar och valt ut dem som har körts av misstänkta användare utan att hitta några uppenbara tecken på att angriparen framgångsrikt kört batchjobb. För att med säkerhet avgöra om en angripare kört ett framgångsrikt batchjobb behöver loggar från ca 6 500 jobb gås igenom.

Misslyckade jobb har identifierats (ingen diskaccess och ingen tapeaccess). Angriparen har i dessa fall gjort mycket enkla fel.

1.5SYS3

De första inloggningarna mot SYS3 sker 10/3.

Under perioden 10/3 15:10 – 21/3 hämtar angriparen via användaren NUS ett antal filer. Användarnamn och lösenord har hämtats från SYS19.

20/3, ca 9:15 placerar angriparen en bakdörr i SYS3, som varit tillgänglig fram till att whitelistningen införts 24/3. Genom bakdörren har angriparen kunnat etablera ett sk reverse-shell som gett höga behörigheter i SYS3 USS-del.

21/3 08:20 identifieras inloggningar i SYS 3 av Logica. 08:42 droppas en session och användaren NUS revokeras. Blacklistning av SYS3 påbörjas. 14:30 identifierar Logica att filer med känslig information tillhörande SKV har hämtats och informerar Applicate om att intrånget ökat i omfattning. Säkerhetschef på SKV och KFM informeras. 16:38 gör användaren NUS ett misslyckat påloggningsförsök och 20:00 identifieras intrångsförsök från nya source-adresser.

23/3 hämtar användaren DAF5648 ZOS-filer från SYS3. Strax därefter utökas blacklistningen av SYS3.

24/3 införs whitelistning av SYS3 efter ytterligare filhämtningar av DAF5648.

Huvudsakliga användarkonton som använts för FTP-sessioner – SYS3

NUS	SPARDRIFT
DAF5648	STÅLSTIERNA CARINA

Huvudsakliga användarkonton som använts för TSO-sessioner – SYS3

DAF5648	STÅLSTIERNA CARINA

1.6Information om de IP-adresser som använts vid intrånget

Information har transporterats till VPS (Virtual private server) providers i bl a Tyskland (t ex 178.18.243.27) men företrädesvis har IP-adresser i Kambodja (Pnomh Pen) använts. Bland annat har man använt ett superuser-konto (högsta behörighet på systemen) från

27.109.118.33 och 123.108.250.50 samt ett reguljärt systemkonto från 203.176.141.205 (alla adresser finns i Kambodja). Enligt uppgift ska en stor del av denna aktivitet pågått runt perioden 10-15 mars 2012. Det finns även informationstransaktioner mot den svenska ISPn Bahnhof.

IP-adresser som accessat och överfört information:
46.50.183.5 (JSC "Zap-Sib TransTeleCom", Novosibirsk, Ryssland)
203.176.141.205 (MEKONGNET INTERNET SERVICE PROVIDER, Kambodja)
27.109.118.33 (DTV-STar Co.,Ltd, Kambodja)
123.108.250.50 (Neocomisp, Kambodja)
178.18.243.27 (QQ-Nova, Tyskland)
46.59.51.181 - h-51-181.a328.priv.bahnhof.se (Bahnhof, Sverige)
85.228.54.229 (Bredbandsbolaget)
178.174.180.144 (Tyfon Svenska AB)
202.120.189.223 (Tongji University, Shanghai)
93.186.170.54 (Inline Internet Online Dienste GmbH, Tyskland)

Ytterligare IP-adresser, oklart accessmöjligheter (loggats i brandvägg):
124.248.174.161 (Cogitel, Kambodja)
124.248.187.100 (Cogitel, Kambodja)

Reflektion:
Även om det gjorts ett större antal på loggningar på storsystemen från exempelvis Tyska ip-adresser så är Riksdagen, Kambodja och Bahnhof mer intressant än något annat och bör prioriteras i den mån det går. Övriga IP-adresser i Ryssland och Tyskland tillhör troligtvis server-/vps-provider.

2 Effekt/påverkan

Intrången i SYS3 och SYS19 har i huvudsak fått som konsekvens att applikationsdata har kopierats ut från systemen, dessa data har bland annat omfattat vissa känsliga personuppgifter.

Utöver applikationsdata har även viss programvarukod kopierats ut tillsammans med systemprogramvara och systemkonfigurationer.

Av angriparens arbetssätt har Logica konstaterat att det primära målet förefaller vara att samla in så mycket information som möjligt. Detta har inneburit att systemfiler, systemkonfigurationer, applikationsfiler och applikationsdata kopierats ut ur systemen. Bortsett från de bakdörrar som angriparen placerat i systemen bedömer dock Logica att sannolikheten är låg för att data och system har förändrats av angriparen.

2.1Påverkan på applikationsdata

Beskrivning av innehåll i de applikationsfiler som kopierats ut ur respektive system.

SYS19
Följande information har av Applicate identifierats som känslig:

- InfoTorg faktureringsinformation – Fakturering antal transaktioner per kund.
- PI (påloggning InfoTorg) – Filer som skickas in till LIME (CRM system). All information om kunder i InfoTorg och dess behörigheter.
- Infodata (Posten) – Adressmatchingar
- InfoTorg(PWC) – Spec på projektmärkning för vidarefakturering
- Applicate (Radiotjänst) – Faktureringsinformation
- InfoTorg/Infodata/Polisen – Faktureringsinformation, transaktionstyp och antal.
- Polisen – Transaktionsstatistik från 2006
- Infodata – tre(3) dataset där filnamnet innehåller texten "skyddade". Dataseten är från år 2007. 10 793 personnummer total i filerna, en kopia och två original har hämtats ut. D v s tre dataset.
- Applicate (blandade kunder) – Faktureringsstatistik

- Infodata – dataset innehållande personnummer i relation till varandra
- InfoTorg – BASUN (företagsinformation från SCB). Grundinfo, namn, juridisk form, storlek på företag etc.

SYS3

- FLISTEST – Handelsbankens fakturor till sina kunder 2006 och 2007 (test mtrl.)
- Enligt Kronofogdemyndigheten har ca 40 klartextfiler innehållande kunder och gäldenärer som normalt skickas till UNIX-systemen kopierats ut från SYS3. Filerna innehåller personnummer, namn, adress, skuld, vem som personen är skyldig. Filerna innehåller även uppgifter som gäldenärer med skyddade identiteter.
- Vidare har betalningsfiler till Swedbank samt sigill för signering av utbetalningsfiler kopierats ut ur SYS3, sigillet är dock utbytt.
- I SYS3 USS-del har ett stort antal filer packats i ett mindre antal arkivfiler vilka kopierats ut från SYS3 via FTP. En analys av arkivfilerna har gjorts och Logica kan inte se att dessa innehållit filer/information kopplad till Polisen eller Skatteverket/Kronofogdemyndigheten.

Logica gör bedömningen att sannolikheten för att något applikationsdata manipulerats av inkräktaren är liten. Detta underbyggs av bland annat FTP-loggar där de uppladdningar av filer som skett i huvudsak utgjorts av angriparens egen kod och bakdörrar.

2.2Påverkan på applikationskod

Från SYS19 har Cobolkoden till programmet Navet har kopierats ut tillsammans med KFM:s Navet-certifikat. Koden kan användas av inkräktaren för hitta svagheter och sårbarheter i applikationen Navet. Applikationen är dock endast tillgänglig från SKV nät och är inte publikt tillgänglig. Utöver detta krävs ett giltigt certifikat för att kunna upprätta en kommunikation med applikationen. Baserat på ovanstående beömer Logica att den risk detta medför är liten.

2.3Påverkan på system

SYS19
Ett förhållandevis stort antal systemfiler har kopierats ut ur systemen, de ur ett säkerhetsperspektiv mest intressanta filerna utgörs av en textfil med användarnamn tillhörande gruppen RYÅSY samt RACF-databasen.

Textfilen innehåller vissa användarnamn och grupptillhörigheter har skapats av angriparen och kopierats ut ur systemet, denna kan användas som utgångspunkt för en lösenordsgissarattack.

I stordatorsystemen ligger lösenord lagrade, krypterat, i RACF-databasen vilken utgörs av en stor binärfil. Under undersökningen av systemet kan Logica konstatera att en komprimerad fil med ett namn liknande binärfilens har kopierats ut från systemet. Den komprimerade filen har sedan raderats. Logica har inte kunnat återfinna den komprimerade filen på backuper etc men gör bedömningen att det är sannolikt att lösenordsfilen i komprimerad form kopierats ut ur systemet.

Angriparen har gjort vissa förändringar i RACF i form av ändrade behörigheter, alla sådana förändringar har återställts.

SYS3
I SYS3 har angriparen haft höga behörigheter i USS-delen och även placerat en bakdörr i systemet. Bakdörrar och annan misstänkt skadlig kod har tagits bort eller oskadliggjorts. Logica gör bedömningen att systemet SYS3 inte påverkats ytterligare av angriparen.

2.4Manipulation av data (dataintegritet)

Generellt gör Logica bedömningen att sannolikheten för att angriparen manipiulerat applikationsdata är liten.

SYS19
Angriparen har under en period haft tillräcklig behörighet att i SYS19 manipulera all data både avseende system och applikationer. Men IBM:s bedömning är dock att angriparna saknat adekvata kunskaper inom zOS för att genomföra förändringar detta baseras bland annat på de enkla fel angriparen begått och som fångats i loggar. Det finns idag inte tillräckligt med loggar för att gå tillbaka i tid för att säkerställa att man inte manipulerat system etc.

Det har konstaterats att angriparna haft tillräcklig kunskap för att elevera kontons behörigheter.

Manipulation av data kan dels ha skett via FTP,via de TSO-sessioner som angriparen upprättat. FTP-sessionerna är loggade och i dessa kan, tillsammans med berörda verksamheter, konstateras att applikationsdata och program inte förändrats. I TSO-sessionerna skedde vid tillfället för intrånget inte loggning av åtgärder varför Logica inte med säkerhet kan avgöra om förändringar skedde i dessa sessioner.

De filer som kopierats ut ur systemet via FTP har listats och skickats till Applicate och myndigheterna för bedömning av känslighet.

Angriparen hade TSO-sessioner upprättade mellan 10/3 17:00 och den 16/3 07:30 med ett användarkonto som enbart hade tillgång till USS-filsystemet men med höga behörigheter. Det finns för närvarande inga tecken på att angriparen har valt att förändra några filer i systemet utan snarare fokuserat på att komma över så stora datamängder som möjligt.

USS-delarna av SYS19 används för filöverföring via bland annat sftp.

Alla delar i USS-operativsystemet som innehåller binärer är monterade read-only och kan därför inte lätt ändras. Inga användar-kataloger (hemkataloger) är normalt synliga eftersom dessa monteras upp vid försök till åtkomst, för att få tillgång till användarkataloger behöver angriparen först veta vilka dessa är.

Angriparen har kopierat delar av användardatabasen till en textfil och därmed fått tillgång till vissa användarkonton vilka kunnat användas till att leta igenom dessa användares användarkataloger efter intressant information.

Angriparen hade via TSO tillgång till zOS mellan 15/3 19.00 och 16/3 10.00 med användarkontona WMROCAR, DAF1017, WAHS006. Via dessa användarkontona har angriparen tillskansat sig mycket höga behörigheter (operation och system special) i SYS19 vilka ger tillgång till behörighetsadministration och dataåtkomst för större delen av SYS19. Det finns inga tecken som idag tyder på att angriparen använt dessa behörigheter för att förändra data.

SYS3
Angriparen har under en del av perioden haft höga behörigheter i SYS3 USS-del. Logicas bedömning är dock att angriparen i första

hand har samtlat in information och inte påverkat system, program eller data.

Angriparen hade TSO-sessioner upprättade mellan 04:12 och 05:40 den 23/3 med användarkontot DAF5648, under perioden hade användarkontot tillgång till:

Dataset	Volume	Behörighet	Senaste Ref
D904.SONG.TEXT	MIGRAT2	READ	2009/05/26
E484.DAF1460.ISPCLIB	STN185	ALTER	2012/03/27
E484.DAF1460.TSOINIT.CLIST	STN207	ALTER	2012/03/27
E484.DAF1489.TPXLOAD	STN190	ALTER	2009/02/05
E484.DRK.JLIB.BKP.D111101	SYS304	ALTER	2012/03/24
E484.DSS.DCOLLECT	??????	ALTER	
E484.DSS.DCOLLECT.E769	STN904	ALTER	2012/03/23
E484.DSS.DCOLLECT.G0230V00	MIGRAT2	ALTER	2012/03/19
E484.DSS.DCOLLECT.G0231V00	STN204	ALTER	2012/03/26
E487.DAF1490.INFOAVT1.READREAD	MIGRAT2	UPDATE	2012/03/10
E487.DAF1492.ADMGDF	MIGRAT2	UPDATE	2011/04/18
E487.DAF1492.ISPF.PLUSOPT	MIGRAT2	UPDATE	2007/12/06
E487.DAF1492.SAS9.DSSKEYS	MIGRAT2	UPDATE	2007/12/06
E487.DAF1492.SAS9.SASUSER	MIGRAT2	UPDATE	2008/01/03
E487.DAF1492.SRCHFOR.LIST	MIGRAT2	UPDATE	2011/04/19
E487.DAF1492.SRCHFOR.LIST.SASJOBB	MIGRAT2	UPDATE	2009/02/11
E487.DAF1492.TSOINIT.CLIST	MIGRAT2	UPDATE	2011/04/19
E487.DAF1572.ADMGDF	STN204	UPDATE	2012/03/26
E487.DAF1572.CNTL	STN214	UPDATE	2012/03/14
E487.DAF1572.CNTL.X19	MIGRAT2	UPDATE	2010/11/03
E487.DAF1572.CNTL.Y19	MIGRAT2	UPDATE	2010/11/03
E487.DAF1572.DOK	MIGRAT2	UPDATE	2011/07/07
E487.DAF1572.ISPF.PLUSOPT	MIGRAT2	UPDATE	2008/02/07
E487.DAF1572.JCL	MIGRAT2	UPDATE	2012/02/21
E487.DAF1572.JCL.S19.F084	MIGRAT2	UPDATE	2012/02/21
E487.DAF1572.JCLSVDC	MIGRAT2	UPDATE	2009/10/01
E487.DAF1572.JCLS19	MIGRAT2	UPDATE	2012/02/20
E487.DAF1572.JUL.DOK	MIGRAT2	UPDATE	2009/10/01
E487.DAF1572.JUL.PGM	MIGRAT2	UPDATE	2009/10/01
E487.DAF1572.JULJCL	MIGRAT2	UPDATE	2009/10/01
E487.DAF1572.KYRKAN.CNTL	MIGRAT2	UPDATE	2008/02/07
E487.DAF1572.PROGRAM	MIGRAT2	UPDATE	2011/04/06
E487.DAF1572.SAS.CNTL.SYS12	MIGRAT2	UPDATE	2008/02/07

E487.DAF1572.SAS.DRK.JLIB	MIGRAT2	UPDATE	2011/11/15
E487.DAF1572.SAS.E897JCL	MIGRAT2	UPDATE	2011/11/15
E487.DAF1572.SOURCLIB.MODLIB	MIGRAT2	UPDATE	2008/02/07
E487.DAF1572.SPFLOG5.LIST	STN903	UPDATE	2012/03/27
E487.DAF1572.SRCHFOR.LIST	STN178	UPDATE	2012/03/27
E487.DAF1572.SRCHFOR.LISTX	MIGRAT2	UPDATE	2006/11/27
E487.DAF1572.S19.D120221	MIGRAT2	UPDATE	2012/02/22
E487.DSS.DOC	MIGRAT2	UPDATE	2011/04/06
E487.DSS.DOK	MIGRAT2	UPDATE	2011/04/06
E487.DSS.DOKUMENT	MIGRAT2	UPDATE	2011/04/06
E487.FAKTPER	MIGRAT2	UPDATE	2008/01/03
E487.LOG.MISC	MIGRAT1	UPDATE	2012/03/20
E487.PRODTRAN.BATTSOPR	??????	UPDATE	
E487.PRODTRAN.BATTSOPR.G0061V00	MIGRAT2	UPDATE	2005/12/19
E487.PRODTRAN.BATTSOPR.G0062V00	MIGRAT2	UPDATE	2006/01/23
E487.PRODTRAN.BATTSOPR.G0063V00	MIGRAT2	UPDATE	2006/02/20
E487.PRODTRAN.BATTSOPR.G0064V00	MIGRAT2	UPDATE	2006/03/20
E487.PRODTRAN.BATTSOPR.G0065V00	MIGRAT2	UPDATE	2006/04/21
E487.PRODTRAN.BATTSOPR.G0066V00	MIGRAT2	UPDATE	2006/05/22
E487.PRODTRAN.BATTSOPR.G0067V00	MIGRAT2	UPDATE	2006/06/19
E487.PRODTRAN.BATTSOPR.G0068V00	MIGRAT2	UPDATE	2006/07/24
E487.PRODTRAN.BATTSOPR.G0069V00	MIGRAT2	UPDATE	2006/08/21
E487.PRODTRAN.BATTSOPR.G0070V00	MIGRAT2	UPDATE	2006/09/22
E487.PRODTRAN.BATTSOPR.G0071V00	MIGRAT2	UPDATE	2006/10/23
E487.PRODTRAN.BATTSOPR.G0072V00	MIGRAT2	UPDATE	2006/11/20
E487.PRODTRAN.DEB420	??????	UPDATE	
E487.PRODTRAN.FAKTURA.DB	MIGRAT2	UPDATE	2006/11/20
E487.PRODTRAN.INFODATA	??????	UPDATE	
E487.PRODTRAN.PROGRAM	MIGRAT2	UPDATE	2011/04/06
E487.QZ3.PGM	MIGRAT2	UPDATE	2010/08/30

3 Sårbarheter/brister

3.1Nät

Brandväggsfiltreringen var vid tillfället för angreppet inte tillräckligt restriktiv då vem som helst tilläts köra både FTP, Teinet och ett antal andra protokoll mot både SYS3 och SYS 19.

3.2Applikationer

I InfoTorgs webbapplikation fanns vid tiden för angreppet en funktion för utbyte av lösenord som förhållandevis enkelt kunde manipuleras för att skicka lösenordet till godtycklig mottagare via e-post.

3.3RACF

I RACF och andra delar av stordatorns operativsystem saknades vid tiden för angreppet ett antal säkerhetskonfigurationer, dessa och de av IBM föreslagna åtgärderna finns beskrivs närmare i dokumentet Mainframe PM 22 Mars 2012.

4 Åtgärder

En av anledningarna till att intrånget upptäcktes var en oväntat hög belastning av systemet. Eftersom hög belastning även konstaterats vid tidigare tillfällen har en analys av dessa tillfällen gjorts för att avgöra om det finns en koppling till intrånget. Enligt den genomgång som gjorts har dessa tillfällen med hög belastning kunnat förklaras med andra händelser.

2011
Den 23/11 började MIPS uttaget i SYS19 att öka. Detta kunde kopplas till en uppgradering av CA- Platinum produkten.

2012
Den 8/2 beställde Applicate en 10 MIPS utökning i SYS19 för att klara av den trafik som börjat belasta maskinen efter en produktionssättning som gjordes 19/1. Efter närmare undersökning konstaterades att InfoTorg hade släppt en App som blivit väldigt populär hos bilhandlare och genererade den ökade belastningen.

Den 12/2 lades MIPS på i samband med uppgradering av Z/OS och Logicafiering av SYS19.

Den 27/2 indkerar Applicate hög belastning i SYS19, efter undersökning visade det sig vara ettt batchjobb, I001M006, som av misstag kördes på dagtid.

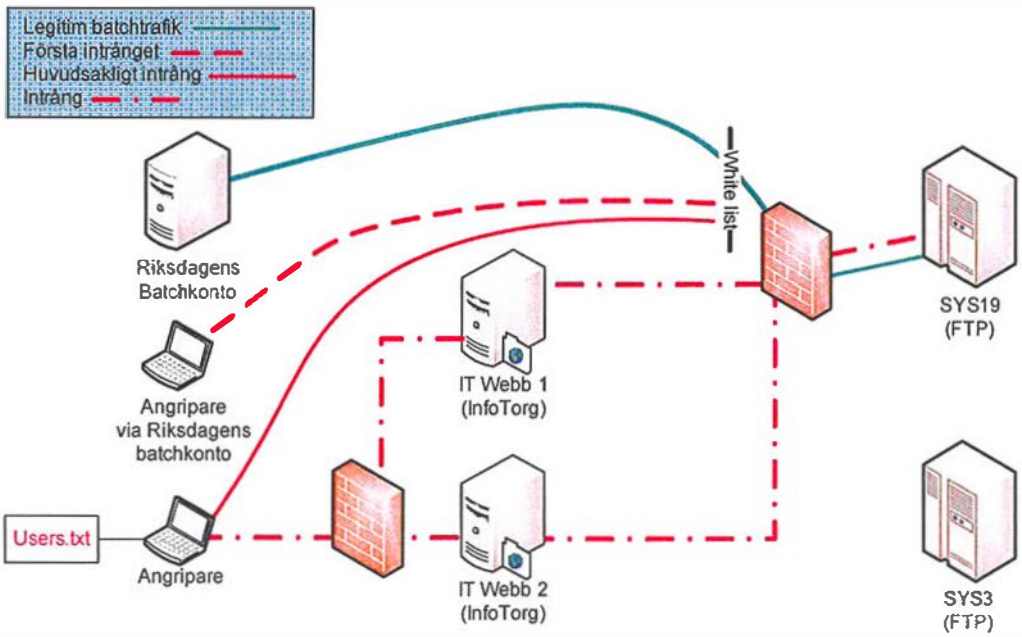
Utöver kontroll av CPU-belastningar har kontroller av rapporterad hög nätverkstrafik mellan Logica och Skatteverket genomförts, dessa har inte kunnat knytas till angreppet.

4.1På kort sikt

Nätverk & kommunikation
Den 9/3 upprättades blacklistning av IP-adresser til SYS19, blacklistning innebär att trafik från de IP-adresser som angriparen kommer ifrån filtreras bort i brandväggen.

För att begränsa attackytan mot SYS 19 infördes den 11/3 så kallad whitelistning av IP-adresser vilket innebär att endast IP-adresser som är konstaterat godkända släpps igenom brandväggen till systemet.

Den 21/3 etablerades blacklistning av trafik även till SYS3 för att den 24/3 göras om till whitelistning.



Bilden ovan visar effekten av whitelistningen av SYS19 och SYS3.

Under perioden har löpande scanningar genomförts från Internet för att avgöra hur stor attackytan har varit och för att successivt minska denna.

Sårbarhetsscanning av de 166 servrar som finns i mainframesystemens omedelbara närhet har genomförts. Insamlat data har analyserats, inga tecken på intrång har identifierats.

Konton
För att hantera risken att alla lösenord i stordatorsystemet knäcks har Logica bytt lösenord på alla konton som Logica ansvarar för. Kontinuerlig övervakning av systemadministratörers inloggningar sker där larm går direkt till Logicas övervakning, övervakning består i av misslyckade inloggningar (6 fel inom 30 sekunder).

Utöver detta har Applicate revokerat (stängt av) alla konton som inte har använts under de senaste 6 månaderna.

Arbete med att ändra lösenord på polisens egna 25 000 konton pågår hos Applicate tillsammans med bland annat byten av lösenord med låg kvalitet.

För att minska risken att funktionen för att byta lösenord i InfoTorg används av en angripare pågår ett arbete hos Applicate med att bygga om funktionen.

För att verifiera att inga webbanvändares RACF-konton eleverats har en matchning av dessa gjorts. Efter matchningen har Applicate kunnat verifera att behörigheterna i RACF inte har förändrats av angriparen, genomgången pekar på att alla webbanvändare har rätt behörigheter i RACF.

Dataintegritet
Ett stort antal misstänkta batchjobb har gåtts igenom för att avgöra om inkräktaren genom detta kan ha påverkat dataintegritet eller systemintegritet. Logica inte kunnat identifiera tecken på otillåtna förändringar som utförts via batchjobb.

Systemintegritet
En genomgång av SYS19 och SYS3 har gjorts med verktygen T01 IBM Security zSecure Admin och IBM Security zSecure Audit for RACF. Resultatet av genomgången av SYS19 har analyserats av specialist från IBM som har sammanställt en lista över rekommenderade åtgärder (se dokumentet Mainframe PM 22 Mars 2012). En genomgång har även gjorts av SYS3 tillsammans med en kortare analys av resultatet. Analysen pekar på att likheterna mellan SYS3 och SYS19 är stora men att vissa skillnader finns. En rapport motsvarande den för SYS19 kommer att tas fram under början av vecka 14.

En översiktlig genomgång av andra partitioner i samma miljö (PRD01, DBR1, DCP, TEK12 och VS22) har gjorts för att identifiera eventuella tecken på intrång. Vid genomgången kunde inte tecken på intrång i dessa konstateras.

Åtgärder har vidtagits på SYS19 och SYS3 för att höja säkerhetsnivån i RACF, sammanfattande beskrivning av dessa återfinns i dokumentet *Logica 2012-03-29-V2,0- Handlingsplan Verifieringsåtgärder säkerställa systemets riktighet.*

De bakdörrar och annan misstänkt skadlig kod som angriparen lämnat efter sig har tagits bort från systemen.

I TSO görs följande loggning:
- SYSLOG, på/av loggning, utförda kommandon (begränsad)
- SMF, Förbrukning, tider etc.
- RACF, På/Av loggning, Loggning mot data set med AUDIT påslagen
- OPS/MVS, jobbinformation, påloggningar larm m m.

4.2På lång sikt

Det finns ett antal tänkbara förslag till långsiktiga säkerhetshöjande åtgärder, bland dessa kan nämnas översyn av systemdesign, kommunikationsinfrastruktur, applikationsutformning.

5 Övrigt

5.1.1 Beskrivning av likheter med 2010-incidenten

I incidenten 2010 användes två demoanvändarkonton från InfoTorg. Det ena kontots lösenord återfanns i ett forum på Internet, det andra fick angriparen lösenord genom att manipulera funktionen för NYTTPW i webben.

Angriparen använder dessa konton för att köra ett antal webb-transaktioner. Samma användarkonto används även för att via FTP hämta viss information ur SYS3. Vid tiden för incidenten görs av Applicate bedömningen att känslig information inte kopierats ut ur systemet.

På grund av ett misstag hos dåvarande driftsleverantör, VolvoIT, fanns en möjlighet för angriparen att även logga in via TPX. Vid tiden för angreppet gjordes bedömningen att inkräktaren via TPX inte gjort några ändringar av data eller kopierat ut ytterligare data. Angriparen gjorde vissa förändringar i RACF vilka backades tillbaka.

I efterarbetet runt incidenten togs ett antal förslag till säkerhets-höjande åtgärder fram och presenterades för Applicate och VolvoIT. Merparten av förändringarna genomförs.

Under 2010-incidenten kommer angriparen huvudsakligen från följande IP-adresser:

130.240.204.195	crap.campus.luth.se.	Placerad i Lueå, på campus för Lueå Tekniska Universitet
202.84.75.138		Placerad I Kambodja, troligen proxunätverk
213.21.78.250	213-21-78-250.bon.t3.se.	Placerad I Sverige, Umeå, bredbandskund,
88.80.6.23	eduardo.prq.se.	Placerad i Sverige, Sthlm, Solna
194.71.126.18	flatline.pteah.estoykh.com.	Placerad I Kambodja
83.183.82.6	d83-183-82-6.cust.tele2.se.	Placerad I Sverige, Tele2 ADSL kund
85.17.146.78	hosted-by.leaseweb.com.	Placerad I Holland, Amsterdam, colo/hosting center,
88.80.28.72	host-72.prq.se.	Placerad I Sverige, Sthlm, Solna
88.80.20.41	thefinn.knark.net.	Placerad I Sverige, Sthlm, Solna
88.80.5.155	pluto.qualitum-net.	Placerad I Sverige, Sthlm, Solna
88.80.13.103	host-13-103-cust.prq.se.	Placerad I Sverige, Sthlm, Solna

5.1.2 Slagningarna i Dalarna

I den inledande fasen av intrånget har konstaterats att angriparen genomfört ett antal slagningar på personer i Dalarna. Detaljerad rapport har tagits fram av Applicate och levererats till Polisen separat.