Institutionen för Programvaruteknik och Datavetenskap
Department of Software Engineering and Computer Science

IT-säkerhetspolicy – efterlevs den av anställda?

Daniel Carlson
Henrik Pedersen

2003-06-03

BLEKINGE
TEKNISKA HÖGSKOLA

Blekinge Tekniska Högskola
Institutionen för Programvaruteknik och Datavetenskap
Box 520
SE-372 25 RONNEBY

Handledare:
Hans Kyhlbäck

Sammanfattning

IT-säkerhetspolicys är huvudsakligen till för att skydda företag mot intrång och oönskad spridning av information. Statistik visar att den IT-relaterade brottsligheten ökar och då är det viktigt att företagen är väl förberedda mot dessa. IT-säkerhetspolicyn utgör en viktig del i denna förberedelse.

Statistik visar på att de IT-relaterade brotten ökar och då är det viktigt att företagen är väl förberedda mot dessa. IT-säkerhetspolicyn utgör en viktig del i denna förberedelse.

Många av de IT-brott som begås kan härledas indirekt till anställda vid de företag där brotten sker. Genom att skapa en bättre förståelse för säkerhetsmässiga risker och hot hos den anställde kan man skydda företaget mot denna indirekta medverkan till brottslighet.

Detta kandidatarbete undersöker huruvida personalen vid Blekinge Flygflottilj (F 17) efterlever sin gällande IT-säkerhetspolicy. Detta görs i form av en omfattande enkätundersökning. Syftet med arbetet är att se hur en förankrad IT-säkerhetspolicy efterlevs av anställda vid F 17.

Resultatet av undersökningen visar att de anställda i viss mån bryter mot F 17:s IT-säkerhetspolicy. Beroende på vilken grad av IT-säkerhetsutbildning och på vilket sätt den anställde tagit del av policyn, visar det sig vara skillnader i hur de efterlever denna. De som inte alls tagit del av policyn var de som bryter mest mot denna.

Abstract

The main purpose of IT security policies is to protect companies against intrusion and unwanted spread of information. Statistics show that IT related crimes tend to increase and because of that it is important, from the company's side of view, to be well prepared. The IT security policy is an important part of that preparation.

A lot of the crimes related to IT can be deduced indirectly to employees at the companies where the crime takes place. By creating a better understanding of the security aspects and threats, the employee can help to protect the company from this indirect criminal activity.

This Bachelor thesis examines whether the personnel at Blekinge Wing (F 17) are complying their current IT security policy. This is done in form of an extensive questionnaire. The purpose of this thesis is to examine if the employees at F 17 are complying an already sanctioned IT security policy.

The result of our examination shows that the employees at F 17 in some ways don't comply with their IT security policy. There are differences in how the employees comply with the policy depending on their educational level of IT security and in what way they have been informed about the policy. The ones that hadn't taken part of the policy at all are the ones that tend to break the most against the policy.

Förord

Vi vill tacka de människor som hjälpt oss att färdigställa vår kandidatuppsats.

Först av allt vill vi visa vår uppskattning till IT-säkerhetschefen Major Tomas Rönnholm vid Blekinge Flygflottilj för att han givit oss sitt godkännande att genomföra vår kartläggning av F 17:s anställda. Utan Tomas hjälp hade vi inte haft möjlighet att kunna genomföra en så omfattande och ingående undersökning som vi gjort.

Vi vill också tacka vår handledare Hans Kyhlbäck, Blekinge Tekniska Högskola, som under 20 veckor lagt ner stor möda på att ge oss återkoppling och goda råd för vår uppsats. Med hans hjälp har vi fått ytterligare ett viktigt perspektiv till vårt arbete.

En person som vi också haft stor nytta av är IT-chefen vid Blekinge Flygflottilj, Kenneth Carlson. Från honom, har vi både fått ovärderlig information om F 17 och dess verksamhet samt praktisk hjälp med enkätundersökningen.

Slutligen vill vi passa på att tacka vår opponent vid Blekinge Tekniska Högskola för hans utmärkta återkoppling på vårt arbete, Oskar Ivinger.

Daniel Carlson
Henrik Pedersen

Ronneby, 13 maj 2003

Innehållsförteckning

1 Inledning

IT-säkerhetspolicys är något som de allra flesta organisationer och företag använder sig av. Denna policy är till för att skydda företaget från intrång och oönskad spridning av känslig information. När nya datorsystem och nätverk implementeras framtages samtidigt nya policys som ska införas i organisationen. För den anställde innebär detta kanske att denne måste vidta nya arbetsrutiner för att efterleva denna policy. För ledningens del ska det avsättas tid för utarbetning av denna policy, samt förankring av densamma bland de anställda.

Om anställda inte följer de regler och rutiner som organisationens ledning har tagit fram, spelar det ingen roll hur bra och genomarbetade dessa är. Vi tror att anställda inte alltid tar säkerhetsriskerna på det allvar som ledningen skulle vilja. Vi tror samtidigt att detta beror på att den anställde inte är införstådd med de risker som finns vid brytande mot IT-säkerhetspolicyn.

”Think your organization is immune from e-risk? Think again. Misuse and abuse of corporate e-mail, Internet, and software assets can trigger costly litigation and protracted electronic nightmares that few employers are prepared to handle”
- Nancy Flynn -

För att undersöka hur IT-säkerhetspolicys följs av anställda vid en organisation har vi valt att genomföra en undersökning vid Blekinge Flygflottilj (F 17), Kallinge. F 17 har i sin helhet drygt 1000 anställda.

1.2 Problembakgrund

Det finns många hot och risker som kan orsaka stor skada i organisationers datorsystem, vilket i sin tur kan resultera i att företag går miste om ovärderlig information. Peltier (2002, s. 8) skriver att det största hotet mot informationsskyddet idag är försummelser åstadkomna av anställda. Enligt en undersökning som Peltier (2002, s. 8) tagit del av så går det att relatera 65 procent av alla IT-incidenter till anställda. Det är alltså främst anställda som direkt eller indirekt medverkar till att IT-relaterade incidenter sker.

Sedan år 1995/ 1996 har de IT-relaterade brotten och incidenterna ökat med 55 procent i företag, myndigheter, kommuner och landsting med fler än 50 anställda. Vad gäller dataintrång är hotet från anställda betydligt större än hotet från utomstående personer. (BRÅ 2000, s. 7)

Även om avsiktliga brottshandlingar såsom piratkopiering, nedladdning av illegala programfiler, spridning av virus och barnpornografi, begås vid datorerna på arbetsplatser, är det oftast inte dessa avsiktliga brott som är vanligast förekommande eller som skapar mest problem för arbetsgivaren. Enligt säkerhetskonsulten på Symantec, Joakim von Braun, är bristande säkerhet vid företag och organisationer ofta orsakad av slarv och bristande förståelse av de anställda. (Dagens IT 2000)

Enligt en artikel i Computer Sweden (2002) är svenska företag säkra i teorin, men inte i praktiken. Nio av tio företag har en IT-säkerhetspolicy, men bara vart femte företag lever som det lär, enligt en undersökning från säkerhetsföretaget Dimension.

Undersökningen som Dimension gjorde baserades på frågor till 60 IT-chefer. 40 procent av IT-cheferna ansåg att de anställda, på grund av bristande kunskaper eller slarv, utgjorde det största hotet mot företagens datorsystem. En bidragande orsak till att personalen är oaktsam är att många företag inte arbetar för att hålla sina säkerhetsrutiner vid liv enligt Dimension.

I en artikel i tidskriften Network Security (Höne & Eloff 2002, ss. 14-16) skrivs det om att IT-säkerhetspolicyn inte efterlevs av den anställde. I samma artikel anges att de anställdas okunnighet om policyn beror på följande faktorer:

- De förstår inte policydokumentet fullt ut
- Policyn är för lång eller teknisk
- De ser inte sambandet mellan policyn och deras arbetssituation.
- De upplever policyn som besvärande.

Att de anställda uppfattar policyn på detta sätt beror troligtvis på att ledningen inte lyckats förankra IT-säkerhetspolicyn på tänkt sätt.

1.3 Problemformulering

Företags IT-sektioner eller avdelningars möjlighet att få respons på hur deras IT-säkerhetspolicys följs och efterlevs är begränsad. Övervakning av personalens efterlevnad av en policy är ett komplicerat problem (Maiwald & Sieglein 2002, s. 147). I allmänhet är det svårt och tidskrävande att övervaka de anställdas efterlevnad av en policy. Det finns inga bra automatiserade metoder att åstadkomma detta, och därför tvingas man att ta till manuella metoder. Enligt Maiwald och Sieglein (2002, s. 147) är manuellt arbete sällan kostandseffektivt inom IT-säkerhet och prioriteras därför ofta bort. Det är först efter att olyckan varit framme som man vet vad som behöver förändras i IT-säkerhetspolicyn och vilka andra säkerhetsrutiner som måste vidtagas. Det är därför angeläget att policyn är väl förankrad i organisationen och att denna efterlevs av de anställda.

Inom ramen för vårt kandidatarbete undersöker vi om F 17:s IT-säkerhetspolicy efterlevs av de anställda på föreskrivet sätt. På så sätt får F 17:s ledning en god indikation på hur väl förankrad policyn är och var det finns eventuella brister i deras IT-system.

1.4 Avgränsning

Vi undersöker hur anställda efterlever F 17:s IT-säkerhetspolicy och i vilken grad olika kategorier av anställda bryter mot policyn. Undersökningen gäller anställda vid F 17 som har sin arbetsplats i Kallinge, inom flottiljområdet. Det finns delar av F 17 som inte är lokaliserade i Kallinge. Anledningen till att vi inte tar med dessa i undersökningen är dels att flertalet är nytillkomna i organisationen från och med den 1 januari 2003 och inte har haft rimlig tid på sig att ta del av IT-säkerhetspolicyn, dels av praktiska skäl i samband enkätundersökningen.

Vi fokuserar på hur den enskilde anställde i sitt dagliga arbete handskas och arbetar med IT-utrustning. Vi undersöker inte sådana aspekter som rör endast ett fåtal av de anställda.

1.5 Syfte

Syftet med undersökningen är att se hur en redan förankrad IT-säkerhetspolicy efterlevs av anställda vid F 17. Vidare syftar undersökningen till att ge svar på om IT-säkerhetsutbildning gör att den anställde bryter i mindre grad mot IT-säkerhetspolicyn.

Indirekt kan arbetet vara till stöd för framtida framtagande och implementering av IT-säkerhetspolicys.

1.6 Hypotes/frågeställningar

Litteraturen om IT-säkerhetspolicy återkommer ständigt till vikten av att utforma en policy rätt för att de anställda ska efterfölja den på bästa sätt. Något som däremot inte nämns lika frekvent är i vilken utsträckning IT-säkerhetspolicys efterföljs. De undersökningar vi lyckats finna utdrag från visar bara i vilken utsträckning de IT-relaterade brotten kan härledas till anställda. Någon specifik utredning som tar upp i vilken utsträckning anställda verkligen bryter mot företagets policy har vi inte funnit. Vår hypotes lyder därför enligt följande:

”IT-säkerheten vid Blekinge
Flygflottilj är allvarligt hotad eftersom IT-säkerhetspolicyn har en
alltför låg grad av efterföljande”

Följande frågor har använts i arbetet med avsikt att understödja hypotesprövningen:

- Är anställda som inte tagit del av IT-säkerhetspolicyn mer benägna att bryta mot denna än de som har tagit del av policyn?
- Spelar sättet de anställda tagit del av IT-säkerhetspolicyn på någon roll för hur de efterlever den?
- Har graden av IT-säkerhetsutbildning hos den anställde någon betydelse för hur denne efterlever IT-säkerhetspolicyn?
- Är det någon skillnad i efterlevelse av IT-säkerhetspolicyn beroende på vilken enhet den anställde tillhör?

1.7 Målgrupp

IT-säkerhetschefer och motsvarande vid företag och organisationer kan genom att ta del av denna undersökning se vilka punkter i IT-säkerhetspolicys som efterlevs minst av de anställda.

2 Metod

För att kunna utröna huruvida anställda vid organisationer följer gällande IT-säkerhetsbestämmelser har vi studerat litteratur inom ämnet. Dels litteratur som behandlar framtagning av IT-säkerhetspolicys, dels litteratur som handlar om hur policys implementeras och förankras.

Inför undersökningen studerade vi F 17:s IT-säkerhetspolicy noggrant. Vi fick den hemskickad med e-post av F 17:s IT-säkerhetschef, Tomas Rönnholm. Initialt läste vi igenom den var för sig för att sedan träffas och diskutera innehållet. De saker som på något sätt var oklara eller som vi inte riktigt förstod i policyn frågade vi Tomas om vid vårt första möte med honom. Därefter började vi tillsammans med Tomas att titta på vad det var vi skulle fråga efter i undersökningen. Vi kom överens om att fråga om sådant som togs upp i policyn som den anställde ofta kommer i kontakt med.

Vår undersökningsmetod är en slags kartläggning (survey), vilket innebär att undersökningen görs på en större avgränsad grupp individer och använder sig av frågeinstrument, såsom intervjuer och enkäter (Patel Runa & Davidson Bo. 2003). I vårt fall är undersökningen kvalitativ och görs med hjälp av en enkät. Svaren ger oss data på nominal nivå. Då vi inte har möjlighet att undersöka hela den population vi är intresserade av, har ett slumpmässigt urval ur populationen gjorts.

2.2 Enkät

Frågorna som vi använder oss av i enkäten är av kvalitativt slag. Med kvalitativt menas att svaren är icke-numeriska och innebär en klassificering. Idéer till utformning av frågor hämtades bland annat från Nancy Flynns The Epolicy Handbook (2001, kap. 2). De allra flesta av frågorna är av sluten karaktär (givna svarsalternativ) och ger svar på nominal nivå. Svar på nominal nivå ger endast en ren klassificering, det vill säga att de svarande inte kan rangordnas på något sätt. (Ejlertsson, G. 1996, s. 96-97).

Många av frågorna saknar alternativ som ”vet ej”, ”kanske” och liknande. Detta är ett medvetet val vi gjort för att de svarande ska behöva ta ställning och tänka till. De flesta av frågorna i enkäten går att härleda till brott mot F 17:s IT-säkerhetspolicy. Övriga frågors svar ger information som behövs för att vi ska få en bild över den anställdes arbetssituation och för att vi ska kunna dela in de anställda i kategorier.

2.2.1 Motivering

En av anledningarna till att vi har valt att arbeta med en enkätundersökning i detta arbete är att det ger den som svarar en möjlighet att vara anonym. Då frågorna i enkäten kan upplevas vara av känslig karaktär, kan möjligheten att vara anonym vara av avgörande betydelse för att de som svarar ska vara uppriktiga. Den som besvarar enkäten kan också i lugn och ro fundera kring frågorna som ställs. Vidare ställs frågorna på samma sätt till alla som ska besvara enkäten. Ytterligare en anledning till valet av en enkätundersökning är att nå ut till många anställda vid organisationen. (Ejlertsson, G. 1996, s. 10-11)

2.2.2 Genomförande

Vi beslutade tillsammans med F 17:s IT-säkerhetschef att vi skulle skicka vår enkät till hälften av de anställda vid F 17 i Kallinge. Vi gick tillsammans igenom personallistorna och tog bort de namn från listorna som inte var tillgängliga för vår undersökning. Denna otillgänglighet berodde bland annat på tjänstledighet, utbildning och sjukskrivning. När detta arbete var gjort återstod 440 namn från åtta enheter som vi kunde nå ut till. Från varje enhet valdes slumpmässigt hälften av namnen ut och därmed blev det 219 stycken anställda som vi skulle skicka enkäter till. Innan vi skickade ut enkäterna testade vi den på tio anställda för att kontrollera att det inte var något som var svårbegripligt eller oklart på något sätt. Det var ingen av dessa tio som hade några invändningar mot enkäten. Vi var medvetna om att frågorna skulle uppfattas vara lite anklagande i sin ton, men det var det ingen som tyckte att det utgjorde något problem. Testpersonerna verkade tycka att undersökningen tog upp ett intressant ämne. Av deras reaktioner att döma förstod vi att de var klart intresserade av att se resultatet av undersökningen. Testpersonerna drog sig inte för att svara uppriktigt på frågor av känslig karaktär. Denna ärlighet som visades upp redan på detta stadiet gav oss förhoppningar om att svaren skulle vara av hög validitet.

Enkätutskicket gjordes med hjälp av Budcentralen, F 17:s interna postförmedling, den 12 mars 2003. Svarstiden bestämdes till två veckor.

2.2.3 Svarsbearbetning

Enkätsvarens data matades manuellt in i statistikprogrammet SPSS (v11.0.0). Med SPSS kunde vi sedan göra statistiska beräkningar för att få fram den information vi önskade. De grafiska diagrammen valde vi däremot att göra i MS Excel, främst av praktiska och estetiska skäl.

De punkter vi valt att ta upp i resultatet är tagna från enskilda frågor i enkäten men vi har också valt att göra jämföranden som grundas på flera frågekategorier. Exempel på sådana är när vi tar fram antalet punkter som de anställda bryter mot enligt IT-säkerhetspolicyn och som därefter jämförs med hur mycket IT-säkerhetsutbildning den anställde har.

2.3 Personlig kontakt

Vid genomförandet av detta arbete har vi vid ett flertal tillfällen varit i kontakt med F 17:s IT-säkerhetschef, Tomas Rönnholm. I övrigt har vi varit på besök på F 17 och bekantat oss med arbetsplatsen. I samband med att enkäten skulle skickas ut till de anställda var vi också i kontakt med de som arbetar på Budcentralen för att de skulle få en uppfattning om vilka vi är. Vårt enkätutskick innebar visst merjobb för dem, så därför kändes det bra för oss att träffa dem i samband med utskicket.

2.4 Val av organisation

När vi skulle välja ut en organisation att arbeta med för vår undersökning hade vi några kriterier som vi ville skulle vara uppfyllda av organisationen.

- Vi ville att det skulle vara en stor (>100 anställda) organisation för att få ett stort underlag för vår undersökning.
- Organisationen skulle ha en IT-säkerhetspolicy som inte var mer än fem år gammal.

Den första organisationen vi kontaktade var F 17 och vi fick direkt kontakt med dess IT-säkerhetschef, Tomas Rönnholm. Det visade sig att Tomas själv varit delaktig i framtagandet av den IT-säkerhetspolicy som F 17 använder sig av och att denna policy togs i bruk den 1 december 2000. Det har nu gått drygt två år sedan dess och därmed borde policyn vid det här laget vara väl förankrad i organisationen, samtidigt som den inte är för gammal och omodern.

3 Bakgrund

3.2 IT-säkerhetspolicy

Uttrycket säkerhetspolicy i informationssäkerhetssammanhang kan ha flera betydelser. Säkerhetspolicy är å ena sidan ledningens direktiv för att skapa en hög informationssäkerhetsnivå, å andra sidan kan det också vara de speciella säkerhetsregler som finns för ett enskilt datorsystem. Den kallas då normalt för systemsäkerhetspolicy (SSR97ETT 1997, s. 5). När vi i vårt arbete använder ordet IT-säkerhetspolicy eller policy är det den förstnämnda som vi relaterar till.

Det är i policyn organisationen förmedlar de viktigaste principerna och rutinerna som har med skyddet av information att göra. Det är den gemensamma referensen dit alla i organisationen kan ta sig för att ta reda på vad som är tillåtet och vad som inte är det (Maiwald E, Sieglein W. 2002, s. 62).

IT-säkerhetspolicys skiljer sig inte nämnvärt från andra typer av policys. De började tas fram i takt med att IT utvecklades och började användas mer frekvent på arbetsplatser och inom organisationer. Denna ökade användning av IT ledde till att organisationerna behövde riktlinjer och styrmedel för hur och i vilka sammanhang IT skulle användas.

Syftet med en IT-säkerhetspolicy är att skydda värdefull information, mjukvara och hårdvara i organisationen. En väl förankrad policy skyddar organisationens fysiska och finansiella tillgångar, anseende och de anställdas personuppgifter.

3.3 Blekinge Flygflottilj (F 17)

3.3.1 Historia[1]

F 17 är en av Försvarsmaktens fyra kvarvarande flygflottiljer i Sverige. F 17 grundades den första juli 1944. Inledningsvis var flottiljen ett förband för marin samverkan, en så kallad torpedflygflottilj. Detta visade sig dock inte vara helt lyckat och redan på våren 1947 gjordes F 17 om till en bombflygflottilj. 1973 påbörjades arbetet med att göra F 17 till en jaktflottilj. Mellan 1976 - 78 var F 17 en renodlad jaktflygflottilj med två jaktdivisioner (J 35 F Draken). 1978 lades en av divisionerna ned och ersattes med en modern spaningsdivision (S 37 SH/ SF Viggen). F 17 blev därmed en blandflottilj med jakt och spaning. 1993 flyttar spaningsdivisionen till F 10 och ersätts med en jaktdivision från nedlagda F 13. F 17 blev nu återigen en renodlad jaktflottilj med två divisioner. Under 2002 ombeväpnades flottiljen med två divisioner av den nya flygplanstypen JAS 39A Gripen.

1967 började arbetet med att etablera en helikopterdivision på F 17 för att förbättra flygräddningen. Detta gjorde att även sjöräddningstjänsten utvecklades. Sedan 1983 har även en marin helikopterdivision (13:e) varit lokaliserad på F 17. Helikopterdivisionen organiserades ur marinens helikopterdivision på Berga i Stockholms skärgård. Deras huvuduppgift var och är U-båtsjakt. Sedan 1998 är alla försvarets helikoptrar samlade i en organisation, Försvarsmaktens Helikopterflottilj. Delar av denna finns stationerad i Kallinge.

[1] Informationen är hämtad från F 17:s webbplats och felaktiga fakta har korrigerats av F 17:s IT-chef.

F 17 är idag den enda flygflottiljen vid Östersjön. Det geografiska läget har bland annat medfört att utbildningen av Flygvapnets piloter i fallskärmshoppning bedrivs här.

3.3.2 Uppgift

Just nu upplevs ett krigshot som avlägset, jämfört med läget under det kalla kriget. Ändå är det varje stats skyldighet mot sina medborgare att upprätthålla ett visst skydd, även mot ett oväntat angrepp. Om Sverige drogs in i ett krig, skulle huvuduppgiften för F 17 vara luftförsvar av Sverige. F 17 skulle då bekämpa eller uppehålla fientligt flyg. I första hand skulle fientliga attack-, luftlandsättnings- och bombföretag bekämpas. Nya uppgifter som tillkommit i och med att F 17 blivit bestyckat med JAS39 Gripen är attack- och spaningsuppdrag.

3.3.2.1 Internationell verksamhet

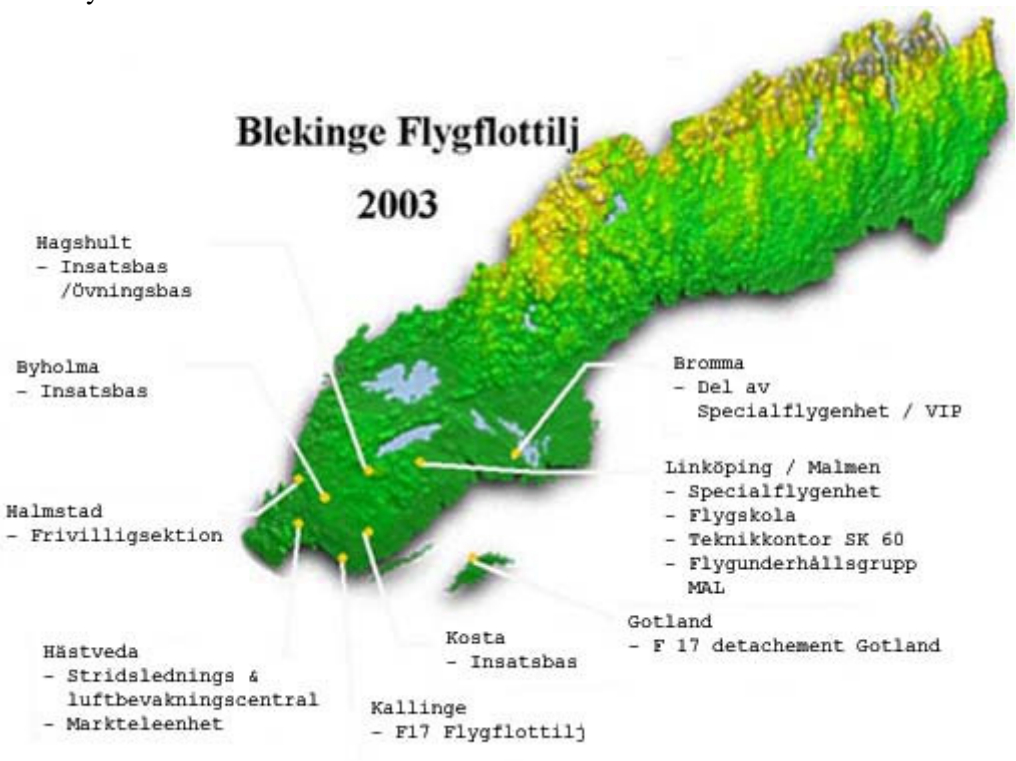
Idag är internationella uppgifter en verklighet även för svenska flygstridskrafter. Därför går mycket av F 17:s tid till utbildning och övning, inför t.ex. fredsbevarande uppdrag under FN-flagg.

3.3.2.2 Incidentberedskap

Incidentberedskapen består av en startklar rote (två flygplan), som står beredd att identifiera och vid behov avvisa främmande flygplan som kränker vårt territorium. Varje vecka identifierar F 17 utländska flygplan i närheten, men antalet rena kränkningar har minskat betydligt sedan 80-talet.

3.3.3 Organisation

F 17:s olika organisatoriska delar är idag stationerade på ett antal platser i södra Sverige. Till stor del beror detta på att flottiljen har tagit över verksamhet från andra flottiljer/ förband som lagts ned. Vissa delar tillkom så sent som den 1 januari 2003.
Den största delen av F 17:s verksamhet är dock förlagd till Kallinge. Ronneby Garnison är ett samlingsnamn för all verksamhet som finns innanför flottiljområdet i Kallinge. Ronneby Garnison innehåller delar som inte tillhör F 17.



Figur 1 F 17:s geografiska utbredning

Då vårt kandidatarbete inriktas på att undersöka hur personalen på flygflottiljen i Kallinge följer organisationens IT-säkerhetspolicy, ges här en kort beskrivning av vad respektive enhet i Kallinge har för uppgift.

3.3.3.1 Flottiljstaben (FLJ-STAB)

Flottiljstabens uppgifter är att bereda ärenden så att beslut kan fattas samt att stödja övriga flottiljen i deras produktion. Flottiljstaben består av fyra sektioner som arbetar brett igenom alla tjänstegrenar.

3.3.3.2 Flygenheten (FLYGE)

Flygenheten utgör kärnan i F 17:s verksamhet. Det finns ungefär 35 aktiva stridspiloter på F 17. I en flygdivision finns, förutom piloterna, även stödfunktioner för flygverksamheten. Underrättelsebefälen stödjer divisionen med underrättelser och analyser då taktiken planeras.

3.3.3.3 Flygplatsenheten (FLYGPLE)

Flygplatsenheten har till uppgift att sköta fälthållning och flygplatsräddningstjänst på Blekinge Flygflottilj och Ronneby flygplats. Flygplatsenheten ansvarar även för bevakning inom F 17, samt kontroll av anläggningar och förråd i södra Sverige.

Enheten funktionsleder även en utlokaliserad bevakningsavdelning som har till uppgift att bevaka en av F 17:s yttre anläggningar.

3.3.3.4 Flygunderhållsenheten (FU E)
Flygunderhållsenhetens huvuduppgifter är produktion av flygtid, upprätthållande av beredskap samt utbildning av värnpliktiga för krigsplacering inom Flygbasbataljon 04. Vid Flygunderhållsenheten genomförs förebyggande samt avhjälpande underhåll av flygplan och tillhörande kringutrustning.

3.3.3.5 Sambands- och informationssystemenheten (SIS E)
Sambands- och informationssystemenheten är ansvarig för sambands- och informationssystemtjänst på F 17. Enheten har ett antal underavdelningar som till exempel arbetar med:

- Uppdatering av samband vid egna flygbaser
- Övningar vid egen flygbas
- Utbildning av övrig personal och värnpliktiga i sambandstjänst
- Drift och underhåll av marktelemateriel (telekommunikations-, väder-, landnings- och navigeringssystem) för flottilj och basbataljoner
- Ansvar för drift, underhåll och förvaltning av F 17:s olika informationssystem och nätverk

3.3.3.6 Strilenheten (STRIL E)
Strilenheten tillhör F 17, men rent geografiskt finns den utspridd på ett antal arbetsplatser på och utanför flottiljen i Ronneby. Strilenhetens främsta uppgifter i fred är att ansvara för stora delar av svensk incidentberedskap i luften över och runt vårt land. Enheten leder och genomför stridsledning av flygvapnets flygförband i södra och mellersta Sverige

3.3.3.7 Utbildningsenheten (UTB E)
Utbildningsenheten utbildar officerare, värnpliktiga, frivilliga och civila till att ingå i flygvapnets insatsförband. Exempel på uppgifter för utbildningsenheten är:

- Sjukvårdsutbildning
- Motorutbildning
- Utbildning av hundar och hundförare
- Utbildning av Radarkompani och Radiopluton
- Betjäning av flygförband på flygbas

3.3.3.8 Hälso – och sjukvårdsenheten (HS E)
Har som uppgift att ansvara för sjukvård och förebyggande friskvård för anställda och värnpliktiga.

3.3.4 F 17:s IT-säkerhetspolicy[2]

F 17:s IT-säkerhetspolicy består av ett huvuddokument (IT-säkerhetsbestämmelser) och är daterat den 1 december 2000. Huvuddokumentet är uppdelat i tre delar: Grundläggande bestämmelser, Policy IT-säkerhet och Inriktning IT-säkerhet. Till huvuddokumentet har efterhand (2001-09-24) ytterligare två policydokumentet tillkommit avseende Internet och E-post. Sammanräknat består F 17:s IT-säkerhets-policy av totalt 28 sidor och ansvarig för dokumentet är IT-säkerhetschefen, Tomas Rönnholm.

3.3.4.1 Förmedling

F 17:s IT-säkerhetspolicy förmedlas muntligt till de anställda vid F 17 i samband med att de går Grundkursen i IT-säkerhet. Denna kurs ligger till grund för att de anställda ska få tillgång till det lokala nätverket och de resterande systemen som återfinns inom flottiljen. IT-säkerhetspolicyn finns också tillgänglig för de anställda på F 17:s intranät, Wingnet.

3.3.4.2 Uppföljning

F 17 har inte tidigare gjort någon uppföljning huruvida F 17:s IT-säkerhetspolicy följs och fungerar. Försvarsmakten har inte heller från centralt håll genomfört någon sådan kontroll.

3.3.4.3 Tillstånd

För att föra in privat datamedia till F 17 krävs tillstånd. Detta tillstånd ska vara godkänt av IT-säkerhetschefen och Informationssystemsektionen. Något sådant tillstånd har inte utfärdats.

3.3.5 Internetdatorer

F 17:s lokala nätverk ska inte vara kopplat mot Internet på något sätt. För Internetåtkomst för de anställda finns det istället ett antal så kallade internetdatorer utplacerade på flottiljområdet. Dessa är till för informationsinsamling som rör tjänsten. Av säkerhetsskäl finns det ingen diskettstation på dessa datorer. För tillfället är internetdatorerna cirka 60 stycken till antalet, vilket motsvarar ungefär en per byggnad.

3.3.6 Lösenord

Den anställde konstruerar själv de lösenord som krävs för åtkomst till F 17:s nätverk. Lösenordet måste uppfylla kraven på att det innehåller åtta tecken, varav det måste ingå gemener, versaler, siffror och specialtecken. Om inte dessa krav är uppfyllda accepterar inte systemet lösenordet. Lösenordet måste bytas ut var tredje månad och systemet som hanterar lösenorden kommer automatiskt ihåg de sex senaste lösenorden en anställd tidigare använt sig av.

3.3.7 Försvarsmaktens e-postsystem

Inom F 17 används Försvarsmaktens e-postsystem, TODAPOST. I korthet innebär detta att när den anställde skickar eller tar emot e-post, går meddelandet via en central SMTP- eller POP3-server. Detta system filtrerar bort eventuella exekverbara filer och macros som finns bifogade med e-postmeddelanden. Vidare körs en viruskontroll på alla e-postmeddelanden på dessa centralt belägna servrar. Detta utgör ett relativt gott

[2] Informationen i detta rubrikavsnitt är hämtad från F 17:s IT-chef och IT-säkerhetschef.

skydd för F 17 vad gäller säkerhetsrisker med e-posthantering av anställda och utomstående.

3.3.8 Backup

På F 17 genomförs varje dygn backuper enligt särskilt schema.

4 Resultat

Antalet enkätsvar som vi fick tillbaka var 154 av 219 utskickade (70 %). Fördelningen över vid vilken enhet de svarande arbetar vid är enligt tabell 1. En person valde att inte svara på vid vilken enhet denne arbetar vid.

Enhet	Antal utskick	Antal svar	Bortfall
FLJ-STAB	24	24	0
FLYG E	31	22	9
FLYGPL E	34	22	12
FU E	68	43	25
SIS E	15	10	5
STRIL E	6	5	1
UTB E	37	23	14
HS E	4	4	0
TOTAL	219	153	66

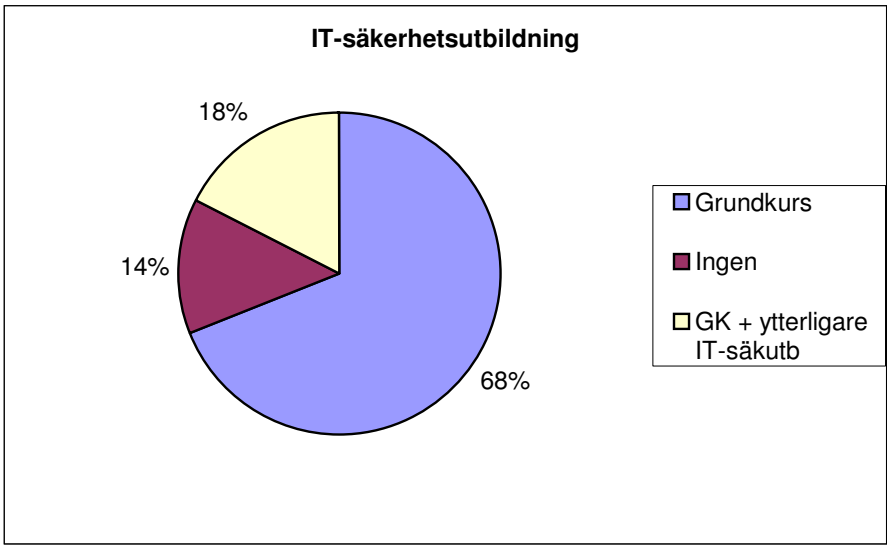
Tabell 1 Fördelning av svar och bortfall

Bortfallen beror till viss del att personal vid vissa enheter inte alltid befinner sig på flottiljen. Anledningar till detta är att personal är på utbildning eller övningar på annan ort.

4.2 Utbildning

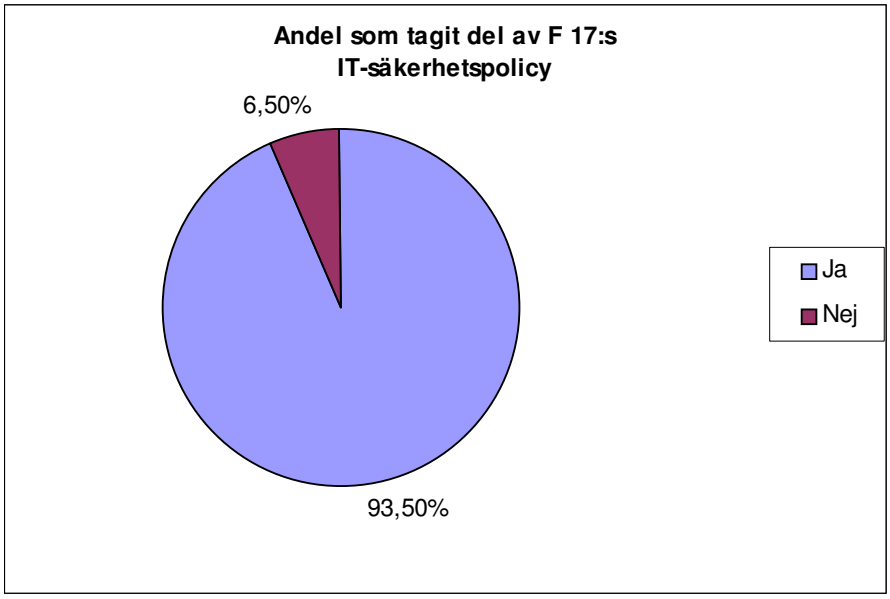
Det pågår ständigt utbildning inom IT-säkerhet vid F 17. Anledningen till detta är att F 17 vill att deras personal ska ha en hög grad av riskmedvetande. Muntlig delgivning av IT-säkerhetspolicyn ges vid en Grundkurs som alla anställda ska genomföra.

Enligt vår undersökning visar det sig att 68,8 % av de svarande genomgått denna Grundkurs. Av de som genomfört Grundkursen har 25,5 % också haft ytterligare IT-säkerhetsutbildning. 31,2 % har svarat att de inte genom gått någon IT-säkerhets-utbildning alls. (se figur 2)



Figur 2 IT-säkerhetsutbildning

De flesta (93,5 %) av de svarande har på något sätt tagit del av F 17:s IT-säkerhetspolicy (se figur 3). Det finns tre olika sätt att ta del av policyn: muntligen, skriftligen och bådadera. Det var 77,1 % som tagit del av policyn muntligen och 68,1 % som tagit del genom att läsa policyn. Det är 45 % som tagit del av policyn både muntligt och skriftligt.

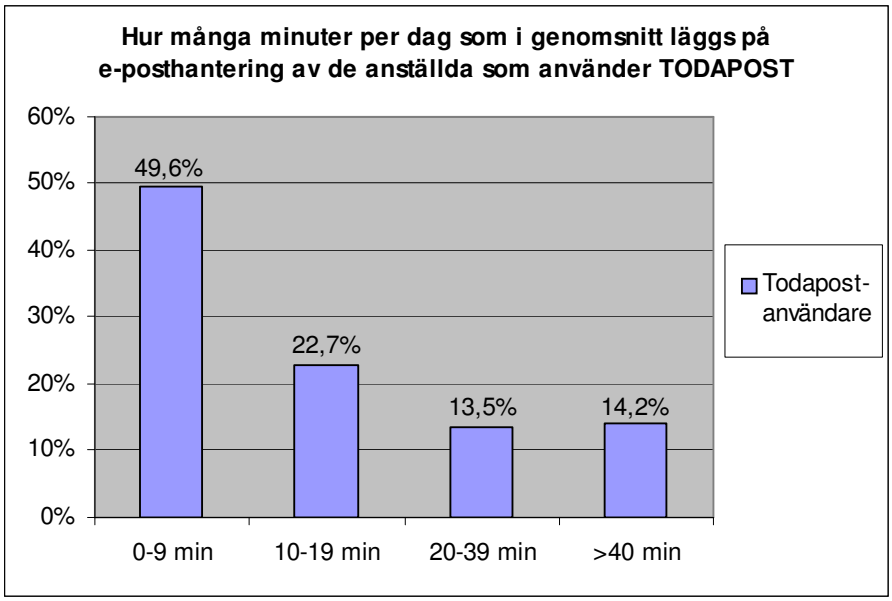


Figur 3 Andel som tagit del av IT-säkerhetspolicyn

4.1 E-post

Av de svarande på enkäten använder 91,6 % Försvarsmaktens e-postsystem (TODAPOST). För att undersöka de anställdas e-postvanor, frågade vi hur mycket tid som lades ned på e-posthantering. Enligt policyn ska användningen av TODAPOST vara rimlig och inte ta omotiverad tid i anspråk, vilket lämnar det öppet för subjektiv tolkning för vad som är tillåtet. Vi kan således inte avgöra om de anställda bryter mot policyn i detta fall.

I figur 4 nedan visas hur mycket tid per dag som i genomsnitt läggs på e-posthantering av de anställda.



Figur 4 E-posthantering

Av de svarande som använder TODAPOST ägnar 49,6 % mindre än tio minuter om dagen till e-posthantering. Det är 14,2 % som ägnar mer än 40 minuter per dag till e-posthantering. Resterande (36,2 %) spenderar 10 till 39 minuter om dagen till att läsa och skriva e-post.

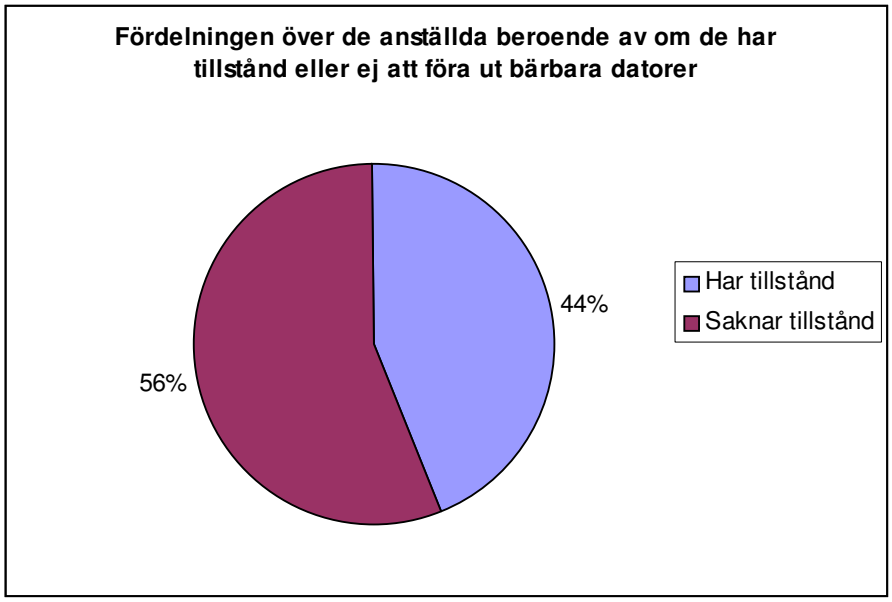
Enligt F 17:s IT-säkerhetspolicy får privat användning av TODAPOST ske ”under förutsättning att den inte tar omotiverad tid i anspråk och/ eller skadar Försvarsmaktens anseende”. Under dessa förutsättningar står det i och för sig också att e-post är avsett för kommunikation i tjänsten, men det är troligtvis en felskrivning. Detta gör att vi inte kan avgöra huruvida de anställda bryter mot policyn i det här avseendet. Det visade sig att 70,1 % av de svarande använder TODAPOST för privat bruk. I *ett* fall visar det sig att en anställd ägnar i genomsnitt mer än 20 minuter per dag till e-posthantering och samtidigt hanterar en andel privata e-postmeddelanden som överstiger en fjärdedel av den totala e-postskörden.

Enligt policyn får man inte skicka eller vidarebefordra virusvarningar. Bland de som använder TODAPOST är det 26,2 % som någon gång fått en virusvarning i ett e-postmeddelande. Den största delen av dessa har vidtagit åtgärder som enligt policyn som är acceptabla. Andelen som vidarebefordrat en virusvarning, och därigenom bryter mot policyn på denna punkt, är 10,8 %.

4.2 Bärbara datorer

På F 17 används bärbara datorer i flera olika sammanhang. De tillfällen som de används vid varierar allt ifrån konferenser till militära övningar. Detta innebär att känslig information och data vid vissa tillfällen befinner sig utanför flottiljområdet, vilket i sin tur innebär en säkerhetsrisk. Därför krävs det från ledningens sida ett skriftligt godkännande för utförsel av datorer och datormedia med sekretessbelagt innehåll.

Bärbara datorer används i tjänsten av 20,1 % av de svarande. Av de som tagit med en bärbar dator utanför flottiljområdet är det mer än hälften (56 %) som inte har tillåtelse till detta. Således bryter alltså merparten av de som använder bärbara datorer mot F 17:s IT-säkerhetspolicy. (se figur 5)

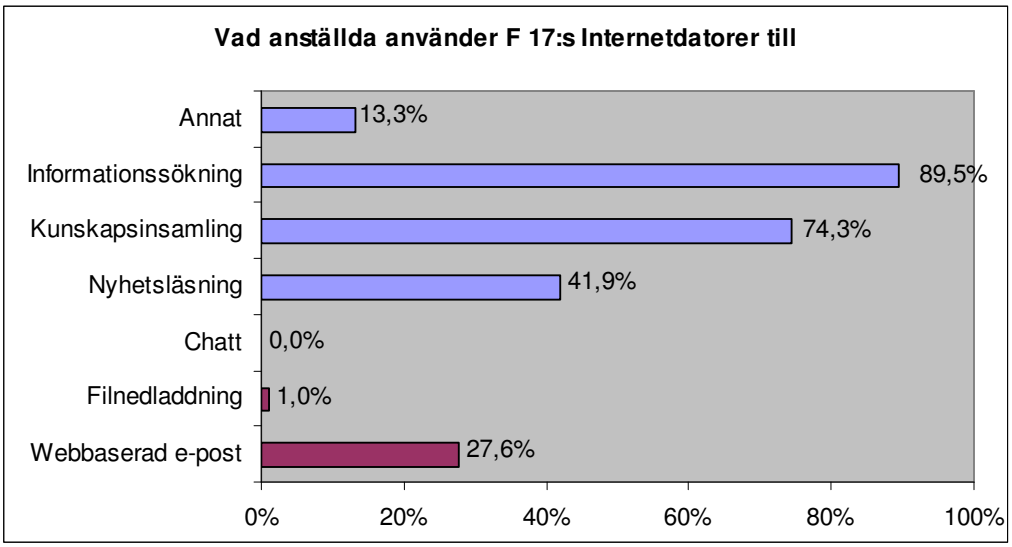


Figur 5 Bärbara datorer

4.3 Internet

För att de anställda ska kunna nå informationskanaler som inte finns inom flottiljområdet har F 17 placerat ut internetdatorer i flottiljens byggnader. Dessa kan bland annat utnyttjas för att erhålla information som rör utbildningar och andra förband. Det framgår i policyn att: ”Användningen av Internet är avsett för informations- och kunskapsinsamling i tjänsten.”. Policyn tar inte upp distinktionen mellan dessa båda begrepp, men det framgår tydligt att internetdatorerna ska användas till sådant som rör tjänsten. Det är enligt policyn inte tillåtet att nyttja internetdatorerna till webbaserad e-post eller nedladdning av program-, musik-, eller videofiler.

Enligt vår undersökning har 68,2 % av de svarande använt F 17:s internetdatorer. Av de som använder internetdatorerna bryter 27,6 % mot IT-säkerhetspolicyn vad gäller regeln om användandet av webbaserad e-post. En procent bryter mot regeln om nedladdning av filer. (se figur 6)



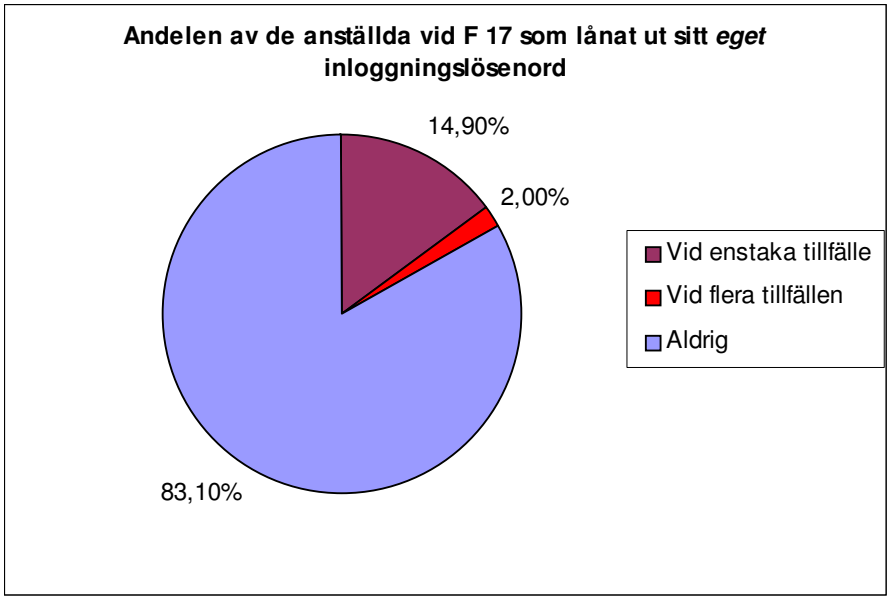
Figur 6 Internetdatorernas användningsområden

Det är enligt IT-säkerhetspolicyn inte heller tillåtet att inneha film- och musikfiler, eller pornografiska bilder på datorerna. Enligt policyn är den anställde skyldig att rapportera till Garnisonschefen om han/ hon har upptäckt något sådant hos annan anställd. Det visade sig vara 11 % av de svarande som kände till att någon annan har sådant material i sin dator. Ingen av dessa har rapporterat detta på ett, enligt policyn, korrekt sätt. De flesta ignorerade problemet, medan andra påtalade olämpligheten direkt till innehavaren.

4.4 Lösenord

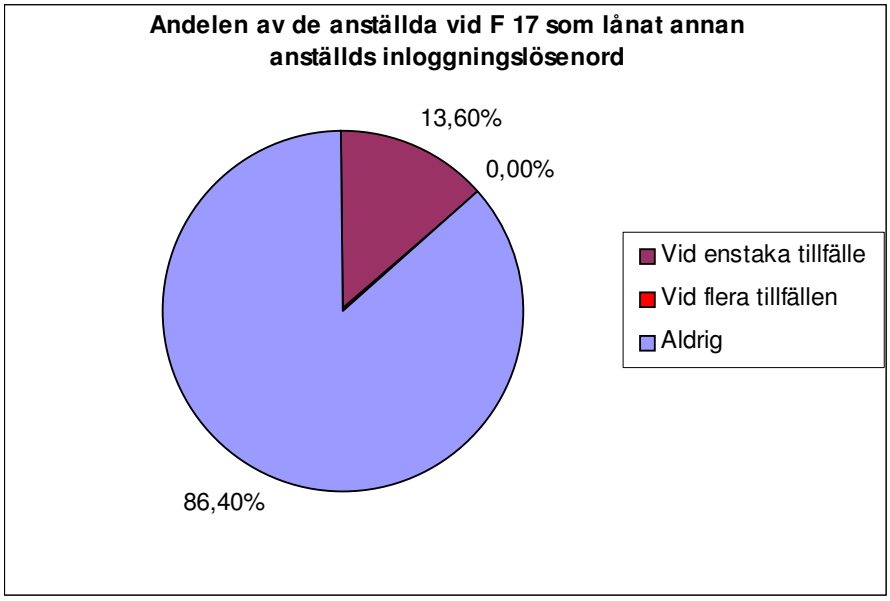
På F 17 behandlas både känslig och sekretessbelagd information som rör rikets säkerhet vilket gör det viktigt att obehöriga inte tar del av material som de inte är berättigade till. För att säkerställa att obehöriga inte får tillgång till sådant material används personliga lösenord vid inloggning till datorsystemen. Om anställda lånar eller lånar ut personliga lösenord kan bland annat ovanstående problem uppstå. Vidare mister ledningen kontrollen över vem som verkligen gör vad i systemen. I förlängningen kan detta innebära att fel person hålls ansvarig för begångna handlingar.

Lösenord är personligt och får inte överlåtas till annan anställd enligt policyn. Det visade sig att det är 14,9 % som lånat ut sitt *eget* lösenord vid enstaka tillfälle och 2 % som har gjort detta vid upprepade tillfällen. Detta går helt stick i stäv med vad policyn uttrycker. (se figur 7)



Figur 7 Utlån av eget lösenord

Samtidigt är det 13,6 % som lånat *någon annans* lösenord vid något enstaka tillfälle. Ingen har lånat annans lösenord vid upprepade tillfällen (se figur 8). Totalt är det 28,6 % som antigen lånat eller lånat ut lösenord vid något tillfälle. Vid en kontroll om det är samma personer som har lånat respektive lånat ut lösenord visade det sig att det är 25 % av de som antingen lånat eller lånat ut lösenord som gjort bådadera. Detta innebär att 7,1 % av de svarande både lånar och lånar ut lösenord.



Figur 8 Lån av annans lösenord

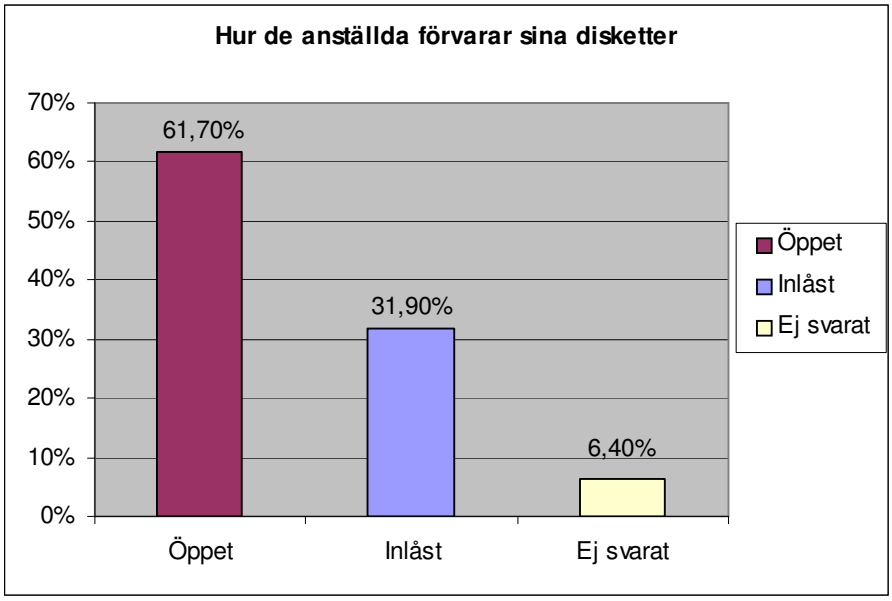
Vi undersökte också om det är någon skillnad i lösenordshantering mellan de som använder egen dator och de som delar dator med andra. Av de svarande som arbetar vid egen dator är det 13,3 % som lånat *någon annans* lösenord vid något tillfälle och 18,7 % som lånat ut sitt *eget* lösenord vid något tillfälle. Av de som delar dator med andra har 13,9 % lånat *någon annans* lösenord, samtidigt som 15,2 % har lånat ut sitt *eget* lösenord.

Det visade sig inte vara någon större skillnad i hanteringen av lösenord mellan de som använder egen dator och de som delar dator med andra.

4.5 Datamedia

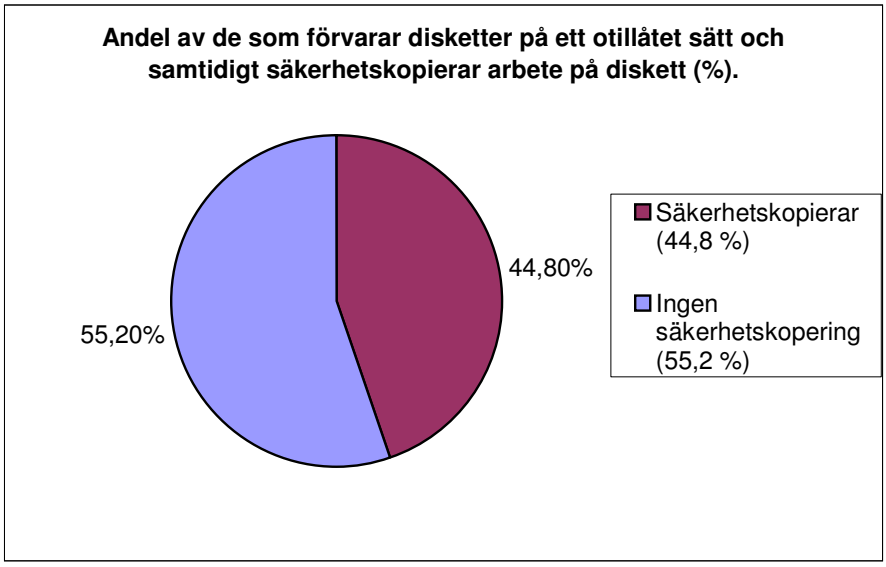
Slarv och försummelser med portabel datamedia, t.ex. disketter och CD-rom, kan innebära att obehöriga får tillgång till information som är säkerhetsklassad. Ett säkerhetskopierat dokument på en diskett som förvaras öppet möjliggör att någon oberättigad kan få tillgång till dokumentet utan att behöva logga in på en dator eller nätverket. Om ett datamedia används i både hemmet och på arbetsplatsen ökar också risken för att virus sprids.

På F 17 är det 61,5 % av de svarande som använder sig av disketter i tjänsten. Enligt IT-säkerhetspolicyn ska disketter förvaras inlåsta. Endast när den svarande uttryckligen svarat inlåst eller säkerhetsskåp på frågan hur de förvarar sina disketter, har vi tolkat det som att de följer policyn. Av de som använder disketter i tjänsten var det 31,9 % som förvarade dessa på ett korrekt sätt. Resterande 61,7 % förvarade sina disketter i eller på skrivbordet, diskettbox, arbetsväska eller helt öppet. 6,4 % av de svarande valde att inte ange hur de förvarar sina disketter (se figur 9). Den största delen av de som använder disketter i tjänsten bryter alltså mot policyn vad gäller hanteringen av disketter.



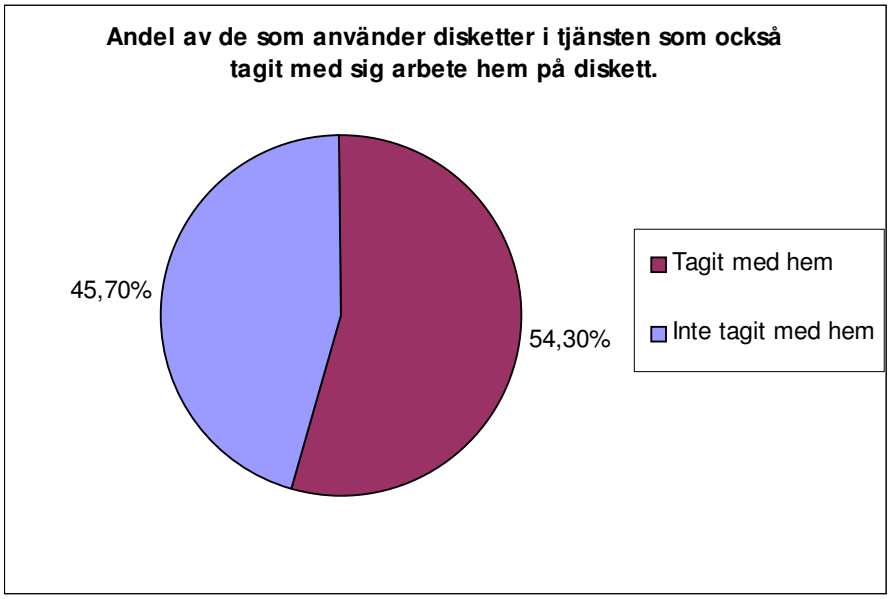
Figur 9 Diskettförvaring

Av de svarande som förvarar sina disketter på otillåtet sätt enligt policyn, säkerhetskopierar 44,8 % sina dokument på diskett. (se figur 10)



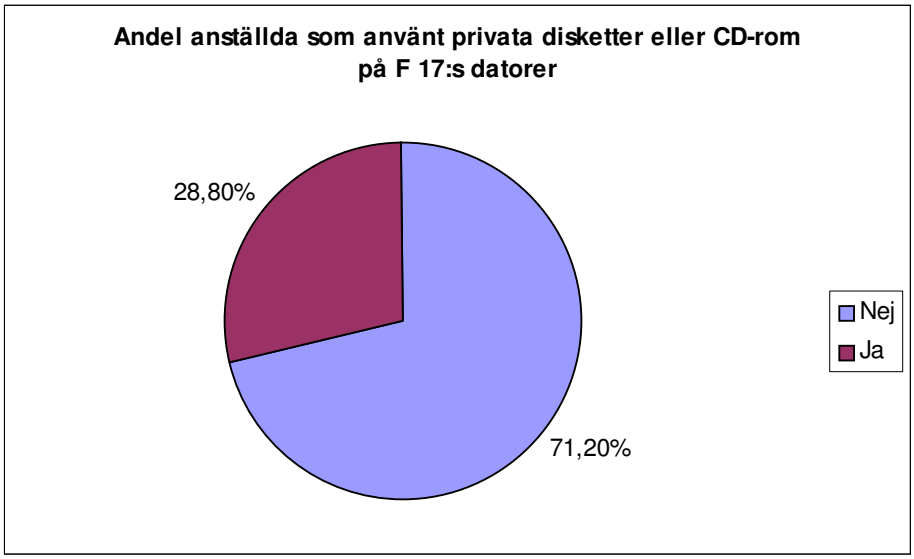
Figur 10 Otillåten förvaring av diskett samt säkerhetskopiering

Av de som använder disketter i tjänsten har 54,3 % också tagit med sig arbete hem på diskett. (se figur 11)



Figur 11 Disketter i hemmet

På frågan om de anställda använt privata disketter eller CD-rom på F 17:s datorer svarade 28,8 % ja (se figur 12). Detta är enligt IT-säkerhetspolicyn endast tillåtet om den anställde har tillstånd.



Figur 12 Privat datamedia på F 17:s datorer

I jämförelsen om det var någon skillnad i hur disketter förvaras mellan anställda som använder sig av en egen dator och de som delar dator med andra blev resultatet enligt Tabell 2.

	Egen dator	Delad dator
Öppet	65,4 %	66,6 %
Inlåst	34,6 %	33,3 %

Tabell 2 Hur anställda förvarar disketter beroende på om de delar dator eller ej

Det visade sig inte vara någon större skillnad i hur disketter förvaras mellan dessa två grupper.

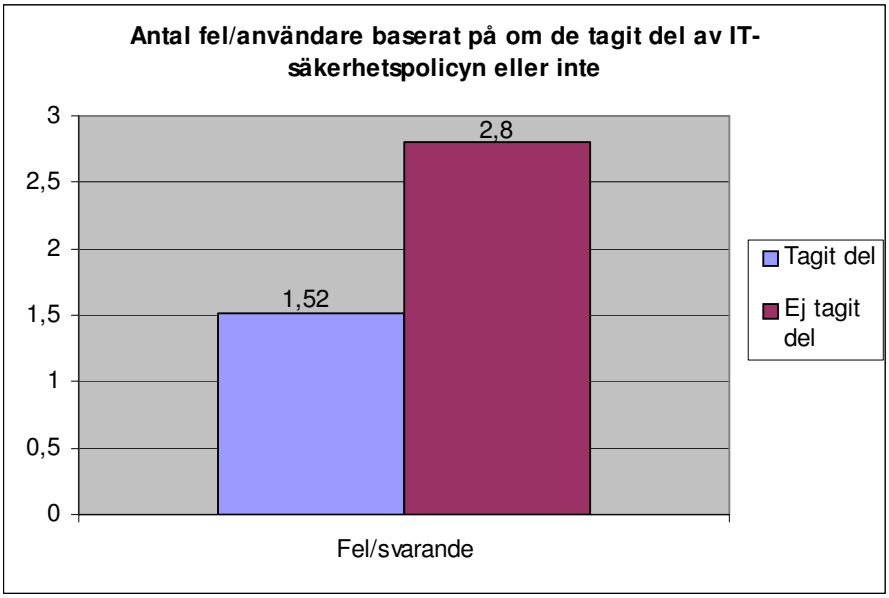
4.6 Överträdelse

För att undersöka hur olika kategorier av de svarande efterlever IT-säkerhetspolicyn, valdes nio punkter ut från denna (se nedan). Med kategori menar vi här en grupp som konstruerats baserat på att de svarat likadant på en eller flera frågor i enkät-undersökningen. De nio punkterna kan direkt härledas till IT-säkerhetspolicyn och betraktas som överträdelser mot denna. En svarande kan således bryta mot totalt nio punkter. När vi nedan använder ordet ”fel” syftar det på brott mot punkterna. För varje jämförelse vi gör mellan olika kategorier, beräknas ett medelvärde över antal fel per svarande inom respektive kategori.

- Använt webbaserad e-post
- Laddat ner filer
- Lånat ut eget lösenord
- Lånat annans lösenord
- Förvarat disketter på otillåtet sätt
- Tagit med arbete hem på diskett
- Använt privata disketter/ CD-rom på F 17:s datorer
- Vidarebefordrat virusvarningar
- Att utan tillåtelse fört ut bärbar dator

I genomsnitt bryter de svarande mot 1,6 punkter i IT-säkerhetspolicyn. Detta tal kan fungera som referens när vi jämför olika kategorier av anställda.

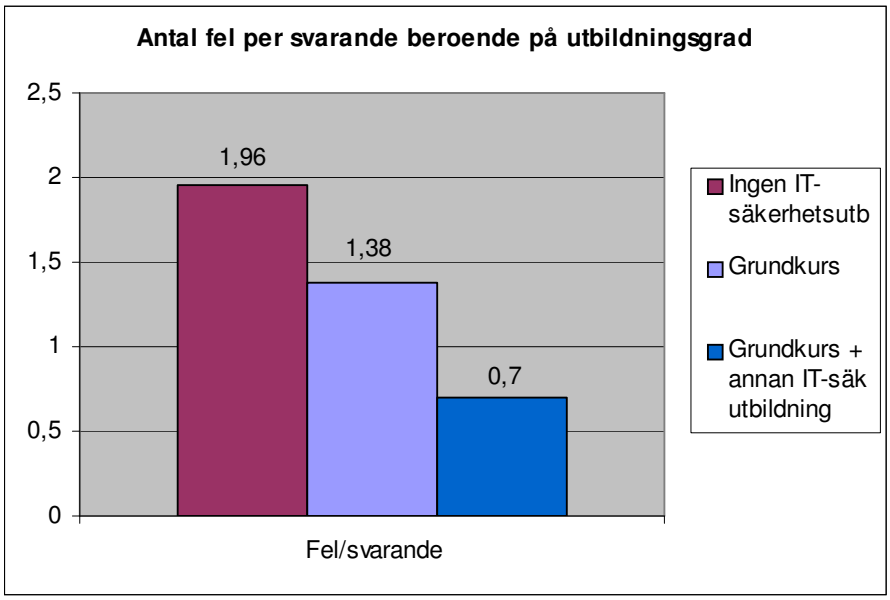
De första kategorierna vi jämförde var de som tagit del av policyn och de som inte tagit del av denna. Det visade sig att de svarande som *inte* tagit del av IT-säkerhetspolicyn bryter mot i genomsnitt 2,8 punkter. De som tagit del av policyn bryter mot 1,52 punkter per svarande. (se figur 13)



Figur 13 Fel per svarande, IT-säkerhetspolicy

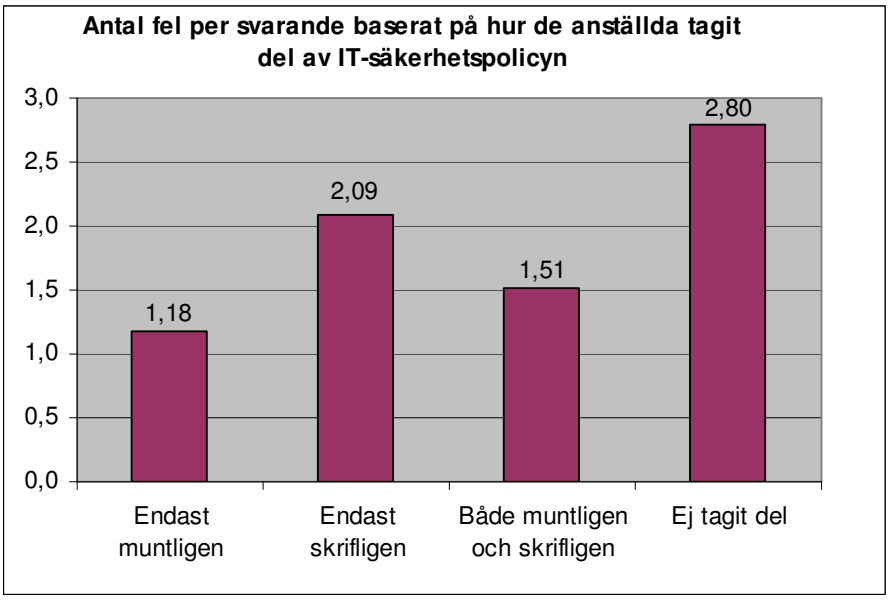
Nästa tre kategorier vi jämförde baserades på vilken utbildningsgrad inom IT-säkerhet de svarande har: ingen IT-säkerhetsutbildning, enbart Grundkurs och Grundkurs samt annan IT-säkerhetsutbildning.

De svarande som *inte* genomfört någon IT-säkerhetsutbildning bryter mot i genomsnitt 1,96 punkter. Något mindre punkter bryter de som genomfört Grundkursen mot. De uppvisade 1,38 fel per svarande. De med genomförd Grundkurs och ytterligare IT-säkerhetsutbildning visade upp 0,7 fel i genomsnitt. (se figur 14)



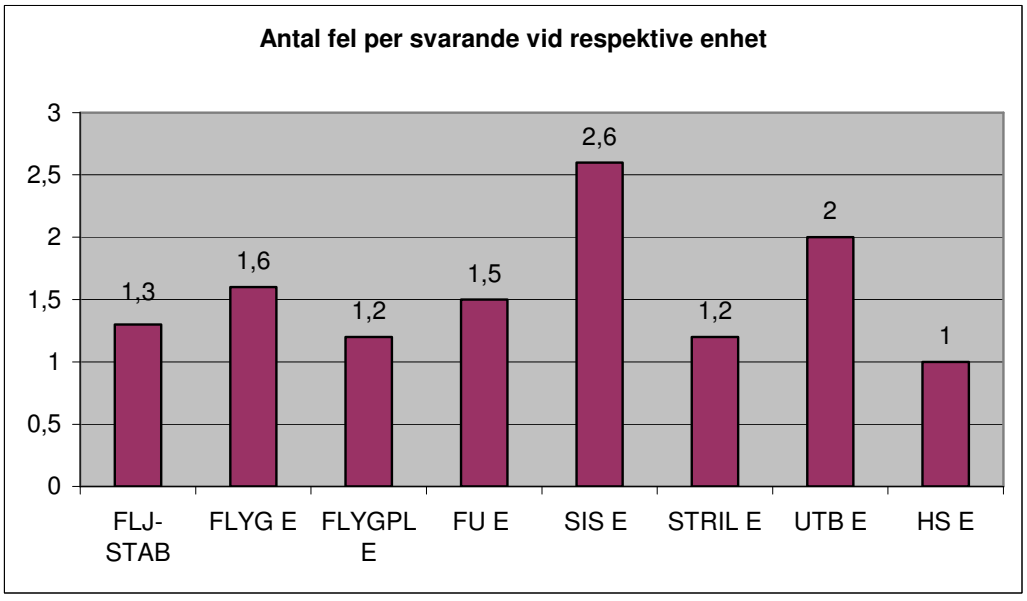
Figur 14 Fel per svarande, utbildningsgrad

Det finns skillnader i antalet fel per anställd beroende på hur de tagit del av IT-säkerhetspolicyn. Det visade sig att de som endast fått muntlig information var de som uppvisade minst antal fel (1,18). De som endast skriftligen tagit del av policyn hade 2,09 fel per svarande och de som både tagit del av policyn muntligen och skriftligen hade något mindre antal fel (1,51). De som inte alls tagit del av policyn uppvisade det högsta antalet fel per svarande (2,8). (se figur 15)



Figur 15 Fel per svarande, hur de anställda tagit del av IT-säkerhetspolicyn

Slutligen undersökte vi om det finns några skillnader i hur de anställda vid de olika enheterna ”sköter sig”. Sambands- och informationssystemenheten (SIS E) var den enhet som uppvisade flest antal fel per svarande. (se figur 16)



Figur 16 Fel per svarande, enhet

5 Slutsatser/diskussion

5.1 Slutsatser

Efter att ha genomfört en enkätundersökning vid F 17 har vi fått en någorlunda klar bild över hur de anställda följer flottiljens IT-säkerhetspolicy. Så mycket som 93,5 % av de anställda har uppgivit att de tagit del av F 17:s IT-säkerhetspolicy. Många har dessutom erhållit både muntlig och skriftlig delgivning av policyn. Detta borde därför innebära att F 17:s anställda har ett relativt högt IT-säkerhetsmedvetande, vilket i sin tur skulle innebära att flottiljen som helhet har goda förutsättningar att hålla en hög IT-säkerhetsnivå.

5.1.1 E-post

F 17:s IT-säkerhetspolicy är tämligen vagt formulerad gällande hur mycket tid som får tagas i anspråk till e-posthantering. Enligt policyn får den anställde lägga ned ”rimlig” tid på e-posthantering. Därför kan vi inte avgöra om de anställda bryter mot IT-säkerhetspolicyn ur denna aspekt. Beroende hur man tolkar policyn är det antigen tillåtet eller icke tillåtet med privat e-posthantering. Den största delen av de svarande utnyttjar TODAPOST även för privat bruk.

Drygt en fjärdedel av TODAPOST-användarna har erhållit någon virusvarning och bara ett fåtal av dessa har vidarebefordrat denna. Att det är få som bryter mot denna punkt i policyn är bra, då virusvarningar ofta innehåller just virus. Frågan är dock om det kommer in virussmittad e-post till F 17 via TODAPOST, då denna är virus-kontrollerad centralt.

5.1.2 Bärbara datorer

Enligt policyn kan enskild öppen data/ information sammanställd i datorn bli klassificerad som sekretessbelagd. Vi utgår därför ifrån att det vid flera tillfällen rör sig om sekretessbelagt material som lämnar flottiljområdet när en anställd för ut en bärbar dator. Mer än hälften av de som använder sig av bärbara datorer i tjänsten har då, enligt oss, olovligen tagit dessa utanför flottiljområdet. Denna punkt visar, enligt oss, att de anställda inte efterlever IT-säkerhetspolicyn på ett godtagbart sätt. Bärbara datorer är i allmänhet stöldbegärliga och det utgör en klar säkerhetsrisk för F 17 att det finns datorer och information utanför flottiljen utan ledningens vetskap. Vi har inte kommit fram till någon bra lösning på detta problem men vi antar att ett större riskmedvetande, genom utbildning till de som brukar bärbara datorer, skulle kunna minska säkerhets-riskerna.

5.1.3 Internet

När det gäller användningen av internetdatorerna, visar de anställda vid F 17 att de i stort sätt använder dessa till det de är ämnade för d.v.s. ”informations- och kunskapsinsamling i tjänsten”. Dock var det så mycket som 27,6 % av de som använder internetdatorerna som använder dessa till webbaserad e-post, vilket enligt policyn är förbjudet. Vi är inte förvånade över detta då Internet till stor del används till e-post. Finns möjligheten att snabbt och gratis kunna läsa sin privata e-post på arbetet är det inte konstigt att de anställda gör det. F 17:s internetdatorer är ej sammankopplade med F 17:s övriga nätverk, vilket gör att riskerna med otillåten hantering av dessa enligt oss inte är speciellt stora. Då det inte heller finns diskettstationer på internetdatorerna minimeras riskerna med att de anställda kan ta med nedladdat material från dessa till

sina tjänstedatorer. Den risk som ändå föreligger är att anställda kan skicka över filer via sitt webbaserade e-postprogram till sin militära e-postadress.

De anställda får inte ha filmer, musik eller pornografisk material på internetdatorerna. I arbetet har vi utgått från att sådant material inte heller får finnas på tjänstedatorerna. Ingen av de som känner till att någon annan anställd innehar denna typ av material har rapporterat detta på ett korrekt sätt. Vi tycker inte att detta är anmärkningsvärt då man inte gärna angiver sina arbetskollegor.

5.1.4 Lösenord

Undersökningen visar att det slarvas en hel del med lösenordshanteringen på flottiljen. Att så många som 14,9 % lånat ut sitt personliga lösenord är definitivt inte bra och det strider också mot IT-säkerhetspolicyn. Det är ungefär lika många som lånat någon annans lösenord. De som bryter mest mot policyn i fråga om lösenordshantering är de 7,1 % som både lånar och lånar ut lösenord. Anledningarna till att lösenords-hanteringen inte fungerar på tänkt sätt kan vara flera. En av dessa kan vara att en anställd behöver komma åt material på någon kollegas konto och därför ”tillfälligt” lånar dennes lösenord. Det kan också vara så att tillfälligt anställda eller praoelever får låna lösenord från fast personal av praktiska skäl, då dessa inte har egna konton.

F 17:s ledning har till viss del försökt att eliminera problemet med lösenordsspridning genom att datorsystemet tvingar den anställde att byta sitt lösenord var tredje månad. Detta gör att om någon på otillåtet sätt har tillgång till nätverket har denna det i max tre månader. För att helt få bukt på denna problematik måste F 17 skärpa sina säkerhetsrutiner ytterligare. En tänkbar lösning skulle kunna vara att införa biometriska inloggningsinstrument, exempelvis irisskanner eller fingeravtrycksläsare.

5.1.5 Datamedia

Den allra största delen av de anställda använder sig av disketter, som de också förvarar öppet. Att förvara sina disketter öppet innebär att dokument, som normalt sätt är utom åtkomst för obehöriga på nätverket, finns enkelt tillgängliga för desamma inom flottiljområdet. Störst säkerhetsrisk utgör den grupp svarande som säkerhetskopierar sina dokument på diskett och förvarar dessa öppet. Att förvara sina disketter på detta vis innebär att avsikten med personligt inloggningslösenord försvagas avsevärt. Enligt IT-säkerhetspolicyn ska disketter förvaras inlåsta, vi måste därför utgå från att alla har möjlighet att låsa in sina disketter och att de som inte gör detta bryter mot IT-säkerhetspolicyn.

Mer än hälften av de som använder disketter i tjänsten har tagit dessa med sig hem. Som vi nämnde i föregående stycke så ska disketter förvaras inlåsta. Dessutom får man inte normalt sätt föra datamedia utanför flottiljområdet. Vi kan naturligtvis inte veta om dessa disketter förvaras på ett säkert sätt i hemmen, men troligtvis är säkerheten där lägre än på flottiljen. Om disketter förs utanför flottiljen innebär detta också att dessa kan utsättas för stöldrisk, virusangrepp och kopiering. Därför anser vi detta kan vara ett brott mot IT-säkerhetspolicyn i dubbel bemärkelse.

Många använder sig dessutom av privata disketter och CD-roms på F 17:s datorer vilket utan tillstånd är förbjudet. Några sådana tillstånd har från det att IT-säkerhetspolicyn implementerades inte utfärdats. Sålunda bryter de 28,8 % av de svarande som använder privat datamedia på F 17:s datorer mot policyn. Detta är allvarligt då det största virushotet mot Försvarsmaktens nätverk är användningen av

disketter och CD-skivor som inte kontrollerats. Enligt Militära Underrättelse- och Säkerhetstjänstens (MUST) årsrapport (2002) har de virus som kommit in i Försvarsmaktens nätverk i de flesta fall förts in via smittade disketter eller CD-skivor och inte via e-post. Antalet utgående virus eller skadlig kod under 2002 var 486 stycken. Det mest allvarliga i detta är att virusen är av sådan typ att Försvarsmakten kan anta att mer än 60 % sänts med avsikt. Ytterligare en aspekt på användandet av privat datamedia är att det blir svårt att ha kontroll på vad som finns i datorsystemet.

5.1.6 Delad tjänstedator

På F 17 är det inte alla som har tillgång till en egen tjänstedator. De som delar dator med annan anställd hanterar inte lösenord sämre än de som arbetar vid egen dator. De uppvisar heller inte att de skulle vara slarvigare med förvaringen av disketter än övriga anställda. När denna kategori av anställda förvarar sina disketter öppet är det enligt oss värre än när övriga gör det. Denna slutsats grundar vi på att det blir svårare att ha uppsikt över sina disketter. Risken att obehöriga tar del av innehållet på disketten, eller stjäl den, ökar också jämfört med om den anställde har en egen tjänstedator. Disketter kan också lättare av misstag förväxlas när kollegor delar dator. På så sätt kan känslig information komma i fel händer. Därför är det kanske viktigare att poängtera vikten av en säker diskettförvaring till denna kategori anställda än till övrig personal.

5.1.7 Överträdelse

I vår resultatdel görs en sammanslagning av nio stycken punkter som direkt kan härledas som brott mot IT-säkerhetspolicyn.

Enligt vår undersökning, går det att se en distinktion mellan de som tagit del av F 17:s IT-säkerhetspolicy och de som ej tagit del, i fråga om i vilken grad de bryter mot de nio punkterna. De som inte tagit del bryter mot fler punkter än övriga. Noteras bör att det var knappt sju procent som inte tagit del av policyn. Att viss personal ej tagit del av IT-säkerhetspolicyn kan tänkas ha flera olika anledningar. Det kan röra sig om nyanställd personal som ännu ej fått information eller förhinder vid utbildningstillfällen. Troligtvis är anledningen till att dessa bryter mer mot policyn att de är mindre medvetna om vad som inte är tillåtet.

Sättet de anställda blivit informerade om policyn har inverkan i fråga om hur de efterlever den. Den kategori som blivit muntligt informerad om policyn följer den i större utsträckning än t.ex. den kategori som enbart läst den. Detta tror vi beror på att muntlig delgivning har flera fördelar jämfört med skriftlig. Fördelarna är som vi ser det att man vid ett muntligt informationstillfälle från ledningens håll kan förklara varför bestämmelserna finns och varför de bör följas. Om den anställde får denna insikt har en god grund lagts för att han eller hon får ett säkerhetsmässigt tänkande i sitt dagliga arbete. Ytterligare en fördel med muntlig information är att det i samband med den går att uttrycka frågor och funderingar kring policydokumentet.

När vi i undersökningen kontrollerar om graden av utbildning hos den anställde spelar någon roll för i vilken grad denne bryter mot punkterna, visar det sig att så är fallet. De utan IT-säkerhetsutbildning bryter mer mot punkterna än de som fått grundläggande IT-säkerhetsutbildning (grundkurs). Jämför vi sedan de utan utbildning med de som gått både grundkurs och ytterligare säkerhetsutbildning blir skillnaden än större. Vi tycker oss se ett klart samband mellan hur den anställde efterlever F 17:s IT-säkerhetspolicy och den anställdes utbildningsgrad. Men det går kanske inte

kategoriskt att se på saken på detta sätt då det kan vara stora skillnader i hur de anställda kommer i kontakt med och hanterar IT-utrustning i tjänsten.

När vi nedan skriver om de olika enheternas grad av användning av IT-utrustning, gör vi antaganden som bygger på kapitel 3.3.3 (Organisation). Vid en granskning över hur de olika enheternas personal förhåller sig till de nio punkterna kan vi dra slutsatsen att SIS E bryter mest mot dessa. Personalen vid SIS E hanterar IT-utrustning i stor omfattning, och borde vara väl medvetna om gällande bestämmelser. Att dessa är de som ändå bryter mest mot punkterna kan bero på just det faktum att de ofta hanterar IT-utrustning och därmed utsätts för många ”risker att göra fel” i sin arbetssituation. Men det mönster vi kan se mellan de olika enheterna är också tvetydigt. UTB E som vi antar hanterar förhållandevis lite IT-utrustning, visar upp den näst högsta förbrytelsen mot punkterna. Samtidigt visar FLYGPL E, som också antas hantera lite IT-utrustning, upp den näst lägsta förbrytelsen mot dessa punkter. Vi tycker oss därför inte se något *egentligt* samband beroende på hur mycket de anställda hanterar IT-utrustning vid de olika enheterna.

5.2 Hypotesprövning

Vår hypotes lyder enligt följande:

”IT-säkerheten vid Blekinge Flygflottilj är allvarligt hotad eftersom IT-säkerhetspolicyn har en alltför låg grad av efterföljande”

Vår undersökning vid Blekinge Flygflottilj har visat att de anställda bryter mot gällande IT-säkerhetspolicy. Graden av brytandet mot denna gör att vi kan konstatera vår hypotes som accepterad.

5.2.1 Besvarande av frågeställningar

Är anställda som inte tagit del av IT-säkerhetspolicyn mer benägna att bryta mot denna än de som har tagit del av policyn?

Ja, enligt vår undersökning visar det sig att de anställda som inte tagit del av IT-säkerhetspolicyn följer denna sämre än övriga anställda.

Spelar sättet de anställda tagit del av IT-säkerhetspolicyn på någon roll för hur de efterlever den?

Ja, det sätt som de anställda tagit del av IT-säkerhetspolicyn på inverkar på hur de efterlever denna. Enligt undersökningen var de som endast muntligen tagit del av policyn *minst* benägna att bryta mot denna.

Har graden av IT-säkerhetsutbildning hos den anställde någon betydelse för hur denne efterlever IT-säkerhetspolicyn?

Ja, graden av IT-säkerhetsutbildning visar sig även den ha betydelse för hur den anställde efterlever IT-säkerhetspolicyn. De med högre grad av IT-säkerhetsutbildning uppvisade en större efterlevnad.

Är det någon skillnad i efterlevelse av IT-säkerhetspolicyn beroende på vilken enhet den anställde tillhör?

Ja, men vi kan inte se något mönster som visar på vad skillnaden beror på.

5.3 Diskussion

Blekinge Flygflottiljs anställda har i hög grad tagit del av IT-säkerhetspolicyn. Hur kan det då komma sig att det ändå bryts mot denna? Vi tror inte anställda vid F 17 medvetet vill bryta mot regler och bestämmelser och vi tror inte heller att de gör detta i större utsträckning än vid andra företag. Att de anställda ändå inte efterlever policyn kan bero på olika inverkande faktorer. Till viss del kan det bero på att F 17 är en stor arbetsplats. Detta tillsammans med att den också är statlig kan göra att en anställd känner lite mindre personligt ansvar gentemot arbetsgivaren än om den anställde arbetat vid ett mindre och/ eller privat företag. Till viss del kan överträdelser mot policyn troligtvis bero på att den anställde inte är medveten om att han eller hon gör fel. Vår undersökning har visat på att mer utbildning till de anställda som resultat ger en mindre benägenhet att bryta mot policyn, d.v.s. ett högre riskmedvetande.

Det man i övrigt som arbetsgivare, förutom att utbilda sina medarbetare, kan göra för att öka IT-säkerheten är att försöka helt eliminera de största hoten. F 17 har vidtagit en del sådana tekniska åtgärder. Till exempel använder flottiljen sig av Försvarsmaktens e-postsystem som bl.a. viruskontrollerar alla e-postmeddelanden. Vidare har F 17 ett säkert system för hindra den anställde från att konstruera enkla lösenord, som också måste bytas ut ofta. Flottiljens internetdatorer är separerade från det övriga nätverket, vilket gör att överträdelser mot IT-säkerhetspolicyn i samband med användandet av internetdatorerna blir mindre allvarliga. Ett exempel på detta är när de anställda utnyttjar internetdatorerna till webbaserad e-post. Detta är förvisso ett brott mot policyn men risken att det ställer till allvarlig skada för F 17 är minimal.

Vad skulle F 17 kunna göra för att ytterligare öka säkerhetsmedvetandet bland sina anställda? Till att börja med är det viktigt att fånga upp de som ännu inte genomfört någon utbildning inom IT-säkerhet. Genom att ge muntlig information till de anställda har man en god möjlighet att ge kunskap *om*, och förståelse *för* policyns innebörd. Vår undersökning visade också på att de som fått muntlig information om IT-säkerhetspolicyn efterlevde den bäst. Även kontinuerlig repetition om vikten av ett säkert användande av IT-utrustning skulle troligtvis ha en positiv inverkan på den anställdes säkerhetsmedvetande.

5.3.1 Självkritisk betraktelse

Vår undersökning behandlar ett område som kan upplevas som känsligt för de svarande. Vi kan därför inte vara helt säkra på graden av enkätsvarens validitet. Utformningen och valet av vissa av enkätfrågorna kunde ha gjorts bättre. I efterhand har vi kunnat konstatera att några av enkätfrågorna kunde ha varit mer precist utformade, någon till och med uteslutas. Dessa misstag hade kunnat reduceras om vi varit mer noggranna vid enkätfrågornas utformning.

Om vi hade haft mer tid och större tillträde till F 17 hade vi helst sett att vi kunnat genomföra någon form av etnografiska studier och intervjuer på flottiljen. Detta hade gett oss en bättre inblick i hur de anställda handskas med IT-utrustning.

Vi har inte undersökt om det finns skillnader mellan manlig och kvinnlig efterlevelse av IT-säkerhetspolicyn. Anledningen till detta är att F 17:s anställda till allra största del består av män. Detta hade annars varit en intressant aspekt att undersöka. Vi har valt att begränsa vårt arbete till att endast behandla de delar ur F 17:s IT-säkerhetspolicy som tar upp den anställdes vardagliga kontakt med och hantering av IT-utrustning. Specialfall och ansvarsförhållanden som endast rör ett fåtal anställda har lämnats åt sidan. Vår undersökning ger därmed inte en heltäckande bild över hur de anställda vid F 17 efterlever policyn.

5.3.2 Framtida forskning

Då vårt arbete inriktas på hur anställda efterlever sin IT-säkerhetspolicy, vore det av intresse att det framarbetades en förankrings- och uppföljningsmodell för IT-säkerhetspolicys inom Försvarsmakten. Vidare hade det varit lämpligt att genomföra studier av liknande karaktär, på dels andra militära förband, dels på privata företag, för att kunna dra ytterligare slutsatser och jämförelser.

Källförteckning

Ejlertsson, Göran (1996). *Enkäten i praktiken – En handbok i enkätmetodik*. Lund: Studentlitteratur.

Flynn, Nancy (2001). *The Epolicy Handbook*. New York, NY, USA: Amacom.

Höne, Karin, Eloff, J.H.P. (2002). *What makes an Effective information Security Policy?* Network Security, Vol. 2002 (6).

Maiwald, Eric, Sieglein, William (2002) *Datasäkerhet I Praktiken*. Stockholm: Pagina förlags AB.

Patel, Runa, Davidson, Bo (2003) *Forskningsmetodikens grunder*. Lund: Studentlitteratur.

Peltier. Tomas R. (2002). *Information Security Policies, Procedures, and Standards – Guidelines for Effective Information Security Management*. Wyandotte, Mi, USA: Auerbach Publications.

SSR97ETT (1997). *Riktlinjer för god informationssäkerhet*. Lund: Studentlitteratur.

Elektroniska källor

BRÅ (Brottsförebyggande rådet) (2002). *IT-relaterad brottslighet BRÅ -rapport 2002:2*, Tillgänglig:
<http:/ / www.bra.se/ dynamaster/ publication/ pdf_archive/ 00020922854.pdf> [2003-05-12]

Computer Sweden webbplats (2002-10-09). Tillgänglig:
<http:/ / computersweden.idg.se/ ArticlePages/ 200210/ 08/ 20021008173533_CS255/ 20021008173533_CS255.dbp.asp>. [2003-04-28].

Dagens IT (2000-04-05). Tillgänglig:
<http:/ / skolan.presstext.prb.se/ bin/ neta2gate?f=doc&state=jrh60u.4.6>. [2003-04-14].

F 17:s webbplats (senast uppdaterad 2003-04-16). Tillgänglig:
<http:/ / www.f17.mil.se/ >. [2003-04-28].

MUST (Militära Underrättelse- och Säkerhetstjänsten) (2003). *Årsrapport Säkerhetstjänst 02,* Tillgänglig:
<http:/ / www.hkv.mil.se/ attachments/ sak_ar02_s5_sv.pdf> [2003-05-09]

Bilaga A: F 17:s IT-säkerhetspolicy (förkortad)

Med anledning av att F 17:s IT-säkerhetspolicy omfattning är bred (24 sidor) och tar upp delar som vi valt att inte undersöka har vi på eget initiativ förkortat ner policydokumentet till att endast omfatta bara de rubriker som enkätfrågorna är grundade på.

Inriktning IT-säkerhet

Sekretess

Sekretessbedömning görs med hjälp av H SÄK Sekrbed, 1999 (Handbok för Försvarsmaktens säkerhetsskyddstjänst sekretessbedömning).
”Den som upprättar en handling har ansvaret för att en korrekt sekretessbedömning av uppgifterna görs. Då det kan vara svårt att bedöma om en uppgift omfattas av sekretess enligt sekretesslagen (1980:100), har handboken med riktlinjer för sekretessbedömning tagits fram. Riktlinjerna syftar till att tjäna som stöd vid bedömningen.”
”Med stöd av handboken skall värdering av om en uppgift omfattas av sekretess göras mot bakgrund av om uppgiften har betydelse för rikets säkerhet och om ett röjande av informationen kan leda till men (skada) för rikets säkerhet. Sekretessbedömning inom Försvarsmakten utförs i regel mot 2 kapitlet 2 § sekretesslagen, den sk försvarssekretessen.”

Om en datamängd (fil, post, dataelement m m) som finns i en dator eller lagras på sekundärminne och innehåller uppgifter som omfattas av sekretess blir hela datasystemet sekretessbelagt.

Vaksamhet skall iakttas när stora datamängder bearbetas. Observera att enskild öppen information kan sammanställd i datorn bli sekretessbelagd. Vid varje förändring av informationsstrukturen i ett IT-system, skall förnyad sekretessbedömning göras.

Flottiljchefen har alltid det direkta ansvaret för skyddet av den information som behandlas vid och avsänds vid flottiljen.

Lösenord

Lösenord konstrueras på ett sådant sätt att det försvårar för obehörig att komma åt systemen. Lösenord är personligt och får inte överlåtas till annan användare.
Följande regler gäller för hur lösenorden skall konstrueras och hanteras:
Första gången användare loggar in skall tvingande lösenordsbyte ske.
Lösenord skall bytas regelbundet enligt ackrediteringsbeslut för aktuellt system. Om inget annat anges sker tvingande byte var tredje (3) månad.
Efter fem (5) misslyckade inloggningar låses systemet för användaren. Upplåsning sker av Helpdesk.

Lösenordet skall bestå av minst sju (7) tecken.
Blanda gemener, versaler, siffror och specialtecken.
Lösenordet konstrueras efter principen – lätt memorerbar mening, tex ”Sommaren –98 badade Jag endast 2 Gånger” detta ger lösenordet ”S98bJe2G” (detta lösenord får ej användas)

Förvaring

Samma bestämmelser, som gäller för förvaring av sekretessbelagda pappersdokument, gäller för datamedia som innehåller/ har innehållit sekretessbelagd information. Säkerhetskopior bör förvaras i brandskyddat säkerhetsskåp enl VDMA 24991 testnorm (+55 grader och 80 % luftfuktighet) eller på förvaringsplats som är brandskyddsmässigt skild från datorns förvaringsplats och uppfyller enligt H SÄK. Vaksamhet bör iakttas då flera säkerhetskopior från sekretessbelagda system förvaras i samma säkerhetsskåp. Den sammanställda informationen kan uppnå kvalificerat hemlig nivå. Säkerhetskopior från olika IT-system skiljs med låsbara utrymmen i säkerhetsskåpet, så att enbart behöriga

har tillgång till respektive kopia. Datamedia kan om det ligger framme, kopieras eller förstöras inom några sekunder/ minuter av obehörig. Förvara därför alltid även öppen datamedia inlåst.

Transport

Datamedia och datorer får normalt ej föras utanför flottiljen (anläggning). Vid transport av sekretessbelagda uppgifter skall den vara skriftligt godkänd av enhetschef (motsv) i samråd med IT-säkerhetschefen.
Transport klassad som KH skall godkännas av flottiljchefen.

Kopiering av datamedia

Kopiering av hemligt datamedia eller delar därav, utförs genom registratorns försorg av IS-sektionen. Anteckning om kopiering (antal exemplar, ev begränsat avsnitt m m) skall göras i kvittenslista hos registratorn och i förteckning hos användaren.
Kopiering skall ske med stor restriktivitet.

Införsel av IT-utrustning

Datorer får ej införas och driftsättas vid F 17 (avser även externa skyddsobjekt) utan att IS-sektionen och IT-säkerhetschefen godkänt datorn och mjukvaran. **Privata datorer får ej medföras till F 17 utan tillstånd**.

Virus

Antivirusprogrammet F-Secure Anti-Virus Windows NT skall användas som antivirusskydd.
Stor vaksamhet skall iakttas mot overifierade datamedia. Datamedia och disketter som varit i okänd/ overifierad datormiljö skall viruskontrolleras innan de får driftsättas. Samråd bör ske med IS-sektionen och IT-säkerhetschefen.

OBS! Antivirus-program upptäcker inte alla virus.

Privata datamedia/ program får ej medföras till F17 utan tillstånd.

Åtgärder vid överträdelser

Rapportera enligt rapporteringsvägar direkt till IT-säkerhetschef eller Säkerhetschef. Vid konstaterad överträdelse som inte är att hänföra till misstag, skall anmälan ske till flottiljchefen för beslut om eventuell disciplinåtgärd. C Undsäk handlägger, på flottiljchefens uppdrag, utredningens utfall och ansvarsfråga.

Vid konstaterat brott skall polisanmälan göras.
En rapporterad överträdelse skall utredas och beslut dokumenteras. Beslutet skall fastställa huruvida:

- misstanke kvarstår
- ytterligare utredning erfordras
- anmälan för disciplinåtgärd skall göras
- polisanmälan skall göras

Utbildning

Samtliga användare av IT-system med sekretessbelagd information, skall genomgå IT-säkerhetsutbildning innan de bereds tillgång till systemet. Ansvaret för denna utbildning åligger respektive enhetschef (motsv). IT-säkerhetschefen stödjer/ genomför utbildning efter direkt överenskommelse. Särskild uppmärksamhet skall ägnas IT-säkerhetsutbildning för personalen vid IS-sektionen.
Utbildningsplan

A. ***Grundkurs*** 4 timmar (PC och terminalanvändare m fl)

B. ***SÄK DATA kurs*** 2 timmar (sekretessbelagda system)

C. ***RÖS kurs*** 2 timmar (sekretessbelagda system)

D. ***Systemspecifik IT-säkerhetsutbildning*** skall genomföras genom respektive systemägares försorg enl LI FV styrdokument.

Rapportering

Grundläggande bestämmelser för säkerhetsrapportering framgår av bl a TF F17 kap 9 säkerhetstjänst. Det är av stor vikt att rapporteringen sker snabbt för att kunna möta och skydda IT-systemen mot exempelvis driftstörningar, virusangrepp, dataintrång eller andra hot och brister. Rapport görs snarast tjänstevägen. Händelser som inträffat under icke tjänstetid skall anmälas senast påföljande tjänstgöringsdag till IT-säkerhetschef, Säkerhetschef och C IS-sektionen.

Virusangrepp/ logiska hot
Misstänkta virusangrepp eller andra logiska hot skall snarast rapporteras till ADB-chef och ADB-säkerhetschef.

1. Policy avseende INTERNET för Ronneby Garnison

1.1 Inledning

Syftet med policyn är ett försök att beskriva gränser för hur Försvarsmaktens datorer och elektroniska adresser (…@…mil.se) får utnyttjas för e-post och Internet. Policyn för Internet och e-post bygger på Försvarsmaktens etiska policy för e-post och Internetanvändning.

Policy gäller samtliga användare inom Ronneby Garnison.

Nedanstående bestämmelser skall anslås vid varje Internetdator.

1.2 Huvudinriktning

Alla inom Ronneby Garnison som använder Försvarsmaktens datorer eller elektroniska adresser (…@…mil.se) måste alltid ta hänsyn till följande:

- Användningen får inte stå i strid mot bestämmelser i lag eller någon annan författning (föreskrift).
- Användningen skall vara rimlig. Det innebär till exempel att utnyttjandet inte får ta omotiverad tid i anspråk eller på annat sätt orsaka myndigheten särskilda kostnader.
- Användningen får inte medföra risk för att Försvarsmaktens anseende skadas.

1.3 Internet

1.3.1 Allmänt

Internetanvändningen är avsett för informations- och kunskapsinsamling i tjänsten. Användningen skall vara rimlig. Varje användning av Internet måste vara kostnads-effektiv. Användning av Internet för annat än tjänsteändamål får inte gå ut över det ordinarie arbetet.

Endast utrustning, programvaror och övriga tillbehör beslutade av C IS-sektionen får installeras och användas på internetdatorerna. Behov av lagring av information skall ske på avsedd server varvid flyttning av material från server till lokalt nät utförs av Helpdesk, IS-sektionen.

Uppmärksamhet mot försök till intrång eller manipulation skall iakttagas och vid minsta antydan anmälas till IT-säk.

Observera att loggning sker av all surfning både på F 17 och på de servrar användaren besöker.

1.3.2 Regler

Följande regler gäller för användandet av Internet:
Internet skall användas för tjänstebruk.
Det är ej tillåtet att ha koppling mellan internetdatorerna och något Förbands-LAN
Personligt login skall användas.
Användare får inte ändra inställningar eller dylikt.
Användare får inte ta bort systemfiler (motsv).

Användare får inte hämta, söka eller sprida information som kan uppfattas som stötande, såsom hets mot folkgrupp, våld och pornografi.
Användare får inte bearbeta sekretessbelagd eller annan känslig information. Känslig information kan t ex vara ekonomisk information, organisationsplaner, utdrag ur databaser, personallistor, teknisk information, lösenord eller avtal.
Nedladdning av program-, musik- eller videofiler mm är ej tillåtet.
Respektera alla former av upphovsrätt.
Tänk på att Du som användare lämnar spår efter Dig. Risker med Internet se underbilaga 1.
E-post får ej nyttjas på internetdatorerna. E-post skall ske via TODAPOST.

Tänk på att Du vid Internetanvändande representerar F 17 och Försvarsmakten.

1.4 Privat användning av Internet

Privat användning av Ronneby Garnisons Internetanslutning får utnyttjas för egen kompetensutveckling, dock skall punkt 1.2 och 1.3 åtföljas.

1.5 Överträdelser

Vid missbruk av denna policy kommer användare att stängas av från Internet.

Vid konstaterad grövre överträdelse (enligt punkt 1.2 och 1.3.1) som inte är att hänföra till misstag, skall anmälan ske till Garnisonschefen för beslut om eventuell disciplinåtgärd.

2. Policy avseende E-POST för Ronneby Garnison

2.1 Inledning

Syftet med policyn är ett försök att beskriva gränser för hur Försvarsmaktens datorer och elektroniska adresser (…@…mil.se) får utnyttjas för e-post. Policyn för e-post bygger på Försvarsmaktens etiska policy för e-post och Internetanvändning. Policy gäller samtliga användare inom Ronneby Garnison.

2.2 Huvudinriktning

Alla inom Ronneby Garnison som använder Försvarsmaktens datorer eller elektroniska adresser (…@…mil.se) måste alltid ta hänsyn till följande:
Användningen får inte stå i strid mot bestämmelser i lag eller någon annan författning (föreskrift).
Användningen skall vara rimlig. Det innebär till exempel att utnyttjandet inte får ta omotiverad tid i anspråk eller på annat sätt orsaka myndigheten särskilda kostnader.
Användningen får inte medföra risk för att Försvarsmaktens anseende skadas.

2.3 E-post

2.3.1 Allmänt

E-post är avsett för kommunikation i tjänsten. Utgående e-post från Försvarsmaktens elektroniska adresser (…@…mil.se) uppfattas som Försvarsmaktens eftersom Försvarsmakten står som avsändare. Endast godkänd e-posthanterare får användas (f n Netscape).

All e-post trafik loggas.

2.3.2 Regler

Följande regler gäller för användandet av e-post:
E-post är avsett för kommunikation i tjänsten.
All e-post skall skickas via TODAPOST.
Skicka/ vidarefodra inga virusvarningar, "skojiga" filer eller kedjebrev via e-post. Oftast är virusvarningar och "skojiga" filer smittade av virus. Kedjebreven är oftast oönskade av mottagaren.
Mottagare av inkommen allmän handling, till personlig adress, skall tillse att handlingen registreras vid centralexpedition vid respektive förband.
Utgående allmän handling, via e-post, skall gå via centralexpedition vid respektive förband.
Undvik att skicka e-post med stora sändlistor om inte alla i sändlistan oundgängligen behöver informationen.
Undvik att skicka stora bifogade filer detta särskilt om stora sändlistor används.
Enskild användare får inte läsa någon annans e-post utan dennes medgivande.
Automatisk vidarebefordra av e-post skall ske restriktivt och beslutas av förbandschef. Vidarbefordran av e-post får ske till endast av HKV godkänd adress, vanligen nn.nn@postbox.mil.se. Vid vidarebefordran skall den enskilde säkerställa att myndighetspost hanteras korrekt.

2.4 Privat användning

Privat användning av e-post må utnyttjas under förutsättning att punkt 2.2 och 2.3 åtföljs.

2.5 Överträdelser

Vid konstaterad överträdelse som inte är att hänföra till misstag, skall anmälan ske till Garnisonschefen för beslut om eventuell disciplinåtgärd.

Bilaga B: Enkät

Enkät om IT-säkerhetspolicy vid F17

Kandidatuppsats vid Blekinge Tekniska Högskola våren 2003

Vi är två studenter som läser programmet Informationssystem 120 poäng vid Blekinge Tekniska Högskola. Vi har som examensarbete valt att undersöka datoranvändande vid organisationer.

Avsikten med undersökningen är att dina svar tillsammans med andra ska ligga till grund för en kartläggning av vilka risker användandet av informationsteknologi medför för en organisation.

50 procent av de anställda vid F17 har slumpmässigt valts ut för att besvara ett sådant här frågeformulär. Vi ber dig att svara på frågorna och returnera formuläret i bifogat svarskuvert. Svarskuvertet skickar du med den interna postgången. Blekinge Tekniska Högskola har tillfälligt lånat ett postfack på BudC där kuverten kommer att hamna.

Undersökningen görs helt anonymt. Ingen av oss som arbetar med undersökningen kommer att veta vem som svarat vad. När svaren kommit in sammanställs de i form av ett generellt resonemang och en enskilds svar kommer ej att kunna utläsas. Resultatet kommer att publiceras i vårt examensarbete.

Om du har några frågor om undersökningen så hör du av dig till Henrik Pedersen, telefon: 0706 - 89 21 29, e-post: is00hpe@student.bth.se

På förhand tack för din medverkan.

Ronneby i mars 2003

Svar önskas senast 26 mars med internpost.

1. Vilken enhet tillhör du?

- □ FLJ-STAB
- □ FLYG E
- □ FLYGPL E
- □ FU E
- □ SIS E
- □ STRIL E
- □ UTB E
- □ HS E
- □ Annan, vilken: _____

2. Har du någonsin använt F17:s e-postsystem (TODAPOST)? Ja □ Nej □

Om du svarat **Nej** på fråga **2** hoppa till fråga **7**

3. Har du någonsin använt F17:s e-postsystem för personligt bruk? Ja □ Nej □

4. Hur många minuter spenderar du i genomsnitt under en vanlig arbetsdag åt att läsa/ skriva e-postmeddelanden?

- □ 0 – 9 minuter
- □ 10 – 19 minuter
- □ 20 – 39 minuter
- □ 40 minuter eller mer

5. Ungefär hur många procent av e-postmeddelandena som du läser eller skriver är privata (d.v.s. icke arbetsrelaterade)?

- □ 0 %
- □ 10 % eller mindre
- □ 11 – 24 %
- □ 25 – 49 %
- □ 50 % eller mer

6. Har du någonsin mottagit någon virusvarning i ett e-postmeddelande? Ja □ Nej □

Om du svarat **Ja** på fråga **6:**
Vad gjorde du med detta meddelande?

- □ Ignorerade och raderade
- □ Vidarebefordrade till andra som du tycker behöver varnas
- □ Annat, vad i så fall?

_____

_____

7. Har du någonsin använt F17:s internetdatorer? Ja □ Nej □

Om du svarat **Ja** på fråga **7**:
I vilket syfte?

□ Webbaserad e-post (t.ex. Hotmail eller Yahoo)
□ Laddat ner filer (musik och filmer)
□ Läsa nyheter
□ Kunskapsinsamling
□ Chattat
□ Informationsinsamling
□ Annat

8. Har du vid något tillfälle lånat någon annans lösenord?

□ Ja, vid enstaka tillfälle
□ Ja, vid flera tillfällen
□ Nej

9. Har du vid något tillfälle lånat ut ditt eget lösenord?

□ Ja, vid enstaka tillfälle
□ Ja, vid flera tillfällen
□ Nej

10. Finns det diskettstation på den dator du vanligtvis använder? Ja □ Nej □

11. Använder du disketter i tjänsten? Ja □ Nej □

Om du svarat **Ja** på fråga **11**:
Hur förvarar du dina disketter?

_____

_____

12. Händer det att du säkerhetskopierar dina dokument på diskett? Ja □ Nej □

13. Har det hänt att du tagit med dig arbete hem på diskett? Ja □ Nej □

14. Har du någonsin använt privata disketter eller Cd-romskivor på F17:s datorer? Ja □ Nej □

15. Använder du en bärbar dator (Laptop) i tjänsten? Ja □ Nej □

Om du svarat **Ja** på fråga **15**:
Har det hänt att du tagit med den utanför flottiljområdet? Ja □ Nej □

Om du svarat **Ja** på föregående fråga:
Har du skriftligt godkännande av enhetschef (motsv.) till detta? Ja □ Nej □

16. Enligt F17:s IT-säkerhetspolicy är det inte tillåtet att ha filmer, musik eller pornografiskt material på sin tjänstedator. Känner du till någon som bryter mot det? Ja □ Nej □

Om du svarat **Ja** på fråga **16**:
Hur rapporteras detta?

_____

_____

17. Hur många personer använder den dator du normalt sätt brukar?

□ 1 st.
□ 2 st.
□ 3 st.
□ 4 st. eller fler

18. Har du tagit del av F17:s IT-säkerhetspolicy? Ja □ Nej □

Om du svarat **Ja** på fråga **18:**
På vilket sätt?

□ Muntlig information.
□ På egen hand (läst).
□ Båda ovanstående.

19. Vilka IT-säkerhetsutbildningar har du genomgått?

□ Grundkurs 4h (PC och terminalanvändande).
□ Systemspecifik IT-säkerhetsutbildning.
□ Inga ovanstående.
□ Annat, vad?

_____

_____