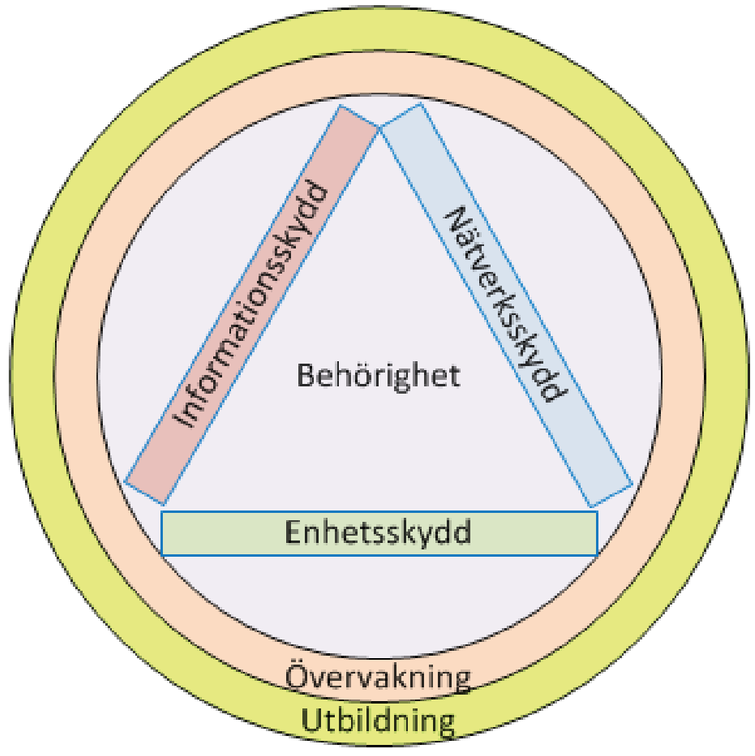
Säker internetåtkomst

Till Försvarsmaktens standardarbetsplatser

TOMMY GUSTAFSSON, LARS WESTERDAHL



FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
Informationssystem
Box 1165
581 11 Linköping

Tel: 013-37 80 00
Fax: 013-37 81 00

www.foi.se

FOI-R--3241--SE
ISSN 1650-1942

Teknisk rapport
Augusti 2011

Informationssystem

Tommy Gustafsson, Lars Westerdahl

Säker internetåtkomst

Till Försvarsmaktens standardarbetsplatser

Titel	Säker internetåtkomst
Title	Secure Internet Access
Rapportnr/Report no	FOI-R--3241--SE
Rapporttyp /Report Type	Technical report
Månad/Month	Augusti/August
Utgivningsår/Year	2011
Antal sidor/Pages	64 p
ISSN	ISSN 1650-1942
Kund/Customer	Försvarsmakten
Projektnr/Project no	E53298
Godkänd av/Approved by	Anders Törne

FOI, Totalförsvarets Forskningsinstitut
Avdelningen för Informationssystem
Box 1165
581 11 Linköping

FOI, Swedish Defence Research Agency
Information Systems
Box 1165
SE-581 11 Linköping

Sammanfattning

Försvarsmakten har en önskan att erbjuda en internetåtkomst med utökad funktionalitet jämfört med dagens lösning. Denna internetåtkomst skall vara tillgängligt för anställda via Försvarsmaktens standardarbetsplats. Den utökade funktionaliteten måste vägas mot Försvarsmaktens behov att skydda interna IT-system och informationstillgångar. Huvudfrågeställningen i denna rapport är således hurivida det är möjligt att bygga en internetåtkomst som uppfyller Försvarsmaktens önskemål på funktionalitet samtidigt som exponeringen av interna system och informationstillgångar hålls låg.

Arbetet har skett genom att identifiera och analysera den hotbild som en internet-anslutning medför. Därefter har Försvarsmaktens funktionella önskemål identifierats och arkitekturer som kan erbjuda efterfrågad funktionalitet beskrivits. Dessa arkitekturer har sedan värderats för att avgöra hur mycket av de interna systemen som exponeras av arkitekturen. Internetrelaterade sårbarheter har beskrivits med förslag på lämpliga skyddsåtgärder.

Resultatet av analysen är en arkitektur som erbjuder önskad funktionalitet med en låg exponering av Försvarsmaktens interna IT-system och informations-tillgångar. Arkitekturen innebär att standardarbetsplatsen ansluts indirekt till Internet. Användarnas internetåtkomst sker via en terminalserverarkitektur och applikationernas internetåtkomst sker via ombudsservrar.

Nyckelord: Internetåtkomst, Internet, IT-säkerhet, Informationssäkerhet

Summary

The Swedish Armed Forces wishes to supply Internet access with enhanced functionality compared to the current solution. The Internet access should be made available to employees through the standard workstation. The enhanced functionality must be weighed against the need to protect the internal IT-systems and information resources of the Swedish Armed Forces. The main question for this assignment has been if it is possible to build a solution for Internet access that corresponds with the needs and wishes of the Swedish Armed Forces, and at the same time minimizing the exposure of internal systems and assets.

The assignment has been carried out by identifying and analyzing the threat profile which is related to the existence of an Internet connection. Then, the sought after functionality has been identified along with architectures which can supply the functionality. The identified architectures were then compared to determine the resulting exposure of internal systems. Internet related vulnerabilities have been evaluated along with suitable security measures to counter these vulnerabilities.

The result of the analysis is a suggested architecture which combines the aspired functionality with a low exposure of the Swedish Armed Forces internal IT-systems and information resources. The architecture lets the workstations connect indirectly to the Internet. The users access the Internet through a terminal server architecture and the applications access the Internet through proxy-like architectures.

Keywords: Internet access, Internet, IT security, information security,

Innehåll

Bildförteckning

Tabellförteckning

1 Inledning

Åtkomsten till Internet kommer att vara möjlig från den SK-miljö[1] som är under uppbyggnad. I samband med denna byggnation finns en önskan om att även förbättra den internetåtkomst som sker via Försvarsmaktens standarddatorer (FM AP). Målbilden är att, jämfört med dagens lösning, förbättra användbarheten och utöka tillgängliga tjänster. Denna funktionalitet skall vara tillgänglig på FM AP, både i och utanför Försvarsmaktens lokaler utan att allvarligt exponera Försvarsmaktens IT-system och informationstillgångar.

1.1 Problemformulering

Internetåtkomst förutsätts ofta idag, både från system som vill kommunicera med sin leverantör eller som är sammankopplade med andra system, men även av den individuelle användaren. Denna åtkomst kan dock inte tas för given.

Ur ett säkerhetsperspektiv innebär en internetanslutning av Försvarsmaktens datanät en ökad exponering av dessa nät och därmed en utökad hotbild[2] mot Försvarsmaktens system. Mot den utökade hotbilden ställs den möjliga nyttan av att tillåta system kommunicera med andra system utanför Försvarsmaktens nät, samt användarens tillgång till Internet.

För användare skulle en internetåtkomst med utökad funktionalitet, jämfört med dagens Charon-lösning, ge en större förmåga till att utnyttja det informationsflöde som Internet innebär. Användare som är vana vid att använda tillgänglig teknik kan idag nyttja privata lösningar för kommunikation för att överbrygga de funktionella hinder som Försvarsmaktens system har. Säkerhetsmässigt är detta inte en god lösning. Det vore mer fördelaktigt med en Försvarsmaktslösning där god funktionalitet erbjuds i standardlösningen.

Åtkomstsbehovet sträcker sig även utanför Försvarsmaktens fasta nät. Personal som till exempel är på tjänsteresa kan ha behov av att kommunicera via sin dator, både med Försvarsmaktens system men även utåt.

Det blir vanligare med applikationer som vill kommunicera med sin tillverkare i syfte att hämta uppdateringar eller nyttja utökade bibliotek, till exempel Clipart för Microsoft Officeapplikationer. Avsaknad av internetkommunikation kan i vissa fall hämma funktionalitet i en applikation.

En moderniserad internetåtkomst måste kunna balansera de funktionella önskemål som användare och system ställer med den exponering och hotbild som

[1] SK syftar på det som kallas sekretessklassad uppgift, SK-miljön avser en gemensam infrastruktur som skall ersätta SWEDI och FM AP infrastruktur.

[2] Med hotbild avses en uppsättning hot som bedöms föreligga mot en viss verksamhet.(SIS HB 550)

åtkomsten medför. Lösningen bör kunna erbjuda säkerhetsmässigt likartade egenskaper både för arbetsplatser inom det fasta nätet, såväl som för arbetsplatser utanför.

1.2 Frågeställningar

Denna rapport behandlar följande frågor:

Huvudfråga:

- Är det möjligt att bygga en internetåtkomst med av Försvarsmakten önskad funktionalitet och med en låg exponering av Försvarsmaktens interna IT-system och informationstillgångar?

För att svara på huvudfrågan ställs även ett antal stödfrågor.

- Hur ser den aktuella hotbilden för internetanslutna datanät ut?
- Vilka arkitekturer kan erbjuda en internetåtkomst med den av Försvarsmakten önskade funktionaliteten?
- Hur påverkar dessa arkitekturer Försvarsmaktens exponering mot Internet?
- Vilka skyddsåtgärder kan användas för att hantera exponeringen?
- Hur kan dessa arkitekturer hantera internetåtkomst för Försvarsmaktens anställda utanför Försvarsmaktens lokaler?

1.3 Syfte

Resultatet i den här rapporten syftar till att vara ett diskussionsunderlag vid val av arkitektur för internetanslutning av Försvarsmaktens IT-system.

1.4 Avgränsningar

Denna rapport beskriver en konceptuell arkitektur och inte en slutgiltig teknisk design. Ekonomiska aspekter, såsom införande, vidmakthållande och utveckling av lösningsförslagen har inte varit en del av analysen. Däremot har helt parallella arkitekturer av ekonomiska och funktionsmässiga skäl uteslutits i samråd med uppdragsgivaren. Likaså har inte heller Försvarsmaktens befintliga lösning behandlats eller värderats.

De funktionella önskemål som tas upp i rapporten har tillhandahållits av Försvarsmakten. Verksamhetsnyttan med dessa önskemål har inte analyserats

gentemot den risk varje önskemål resulterar i. E-post hanteras i separata system och ingår därför inte i analysen.

Denna rapport beskriver endast hur en internetanslutning av datanät för hantering av SK-klassad information kan ske. Datanät som innehåller information av högre säkerhetsklass har ej hanterats.

2 Metod

I det här kapitlet presenteras den metodik som använts för att samla in och analysera data.

2.1 Datainsamling

Underlaget för denna rapport baseras på en dialog med Försvarsmakten, litteraturstudier, idékläckningssessioner[3], tidigare känd kunskap och begränsade empiriska studier. Dialogen med Försvarsmakten har skett löpande under rapportens författande och inkluderat önskad funktionalitet och lämpliga arkitekturer.

Litteraturstudierna har omfattat publikationer från Försvarsmakten, IT-säkerhetsorganisationer och systemleverantörer samt internetbaserade forum och bloggar. Informationen i Försvarsmaktens publikationer har använts för att få en ökad förståelse av Försvarsmaktens syn på aktuell hotbild, interna krav på IT-system och dess skydd, terminologi samt önskad funktionalitet. Studier av publikationer från ett antal IT-säkerhetsorganisationer har gett information om aktuella hot, skyddsåtgärder och trender. Publikationer från ett antal systemleverantörer, internetbaserade forum och bloggar har använts för att fördjupa kunskapen om hur vissa arkitekturer kan byggas samt hur väl de kan leverera efterfrågad funktionalitet. Vidare har sökmotorer använts för att hitta relevant kunskap om aktuella arkitekturer eller funktionaliteter.

Idékläckningssessioner har använts löpande under framtagandet av rapporten för att identifiera och värdera relevanta komponenter samt för att eliminera ej relevanta komponenter. Dessa komponenter inkluderar hot, arkitekturer, sårbarheter och skyddsåtgärder.

I vissa fall har begränsade empiriska studier använts för att undersöka hur en viss arkitektur kan tillhandahålla efterfrågad funktionalitet.

2.2 Analys

Analysen av insamlad data har skett genom diskussion, generalisering, eliminering och komparativa studier.

Diskussionen har använts för att värdera terminologi, påverkande faktorer, hotbild, sårbarheter, arkitekturer och skyddsåtgärder. I huvudsak har diskussionen skett mellan författarna men har vid behov även inkluderat personer utanför gruppen när det varit relevant.

[3] Eng. Brainstorming

Eliminering och generalisering av uppkomna hot och lösningar har använts löpande som verktyg för att fokusera arbetet och rapporten.

Komparativa studier har genomförts för att på ett tydligt sätt illustrera hur valet av arkitektur påverkar funktionalitet och säkerhet.

3 Bakgrund

I det här kapitlet presenteras nyckelbegrepp samt en övergripande bild av den bakgrund på vilken arbetet är baserat.

3.1 Begrepp

Nedan definieras ett antal begrepp som är centrala för rapporten.

Hot: Möjlig, oönskad händelse med negativa konsekvenser för verksamheten.[4]

Hotbild: Uppsättning hot som bedöms föreligga mot en viss [typ av] verksamhet.[5]

IT-system: System med teknik som hanterar och utbyter information med omgivningen.[6]

Sårbarhet: Brist i skyddet av en tillgång exponerad för hot.[7]

Skyddsåtgärd: Handling, rutin eller tekniskt arrangemang som, genom att minska sårbarheten möter ett identifierat hot.[8] I den här rapporten är skyddsåtgärd likställt med termen säkerhetsmekanism som används i H Säk IT (2006).

Skydd: Effekt av handlingar, rutiner och tekniska arrangemang som syftar till att minska sårbarheten.[9] Skyddet byggs upp av ett antal skyddsåtgärder. I den här rapporten är skydd likställt med termen säkerhetsfunktion som används i H Säk IT (2006).

Tillgång: Allt som är av värde för organisationen.[10] I denna rapport omfattar tillgångar Försvarsmaktens IT-system och information som är tillgänglig via dessa system.

Arkitektur: Med arkitektur avses sättet att organisera komponenterna i ett IT-system.

Exponering: De gränssnitt i form av tjänster, funktioner och resurser som är åtkomliga för en potentiell angripare.

[4] SIS HB 550, Utgåva 3, 2007
[5] SIS HB 550, Utgåva 3, 2007
[6] H Säk IT, 2006
[7] ISO/IEC 13335-1:2004
[8] SIS HB 550, Utgåva 3, 2007
[9] SIS HB 550, Utgåva 3, 2007
[10] SIS HB 550, Utgåva 3, 2007

Försvarsmakten beskriver i Handbok Säkerhetstjänst Informationsteknologi (H Säk IT, 2006) och Krav på säkerhetsfunktioner (KSF 2.0 Grunder) en indelning av säkerhetsfunktioner, säkerhetsmekanismer samt relevanta krav på dessa.

I denna rapport används termerna skydd och skyddsåtgärd istället för säkerhetsfunktion respektive säkerhetsmekanism. Bakgrunden är att de säkerhetsfunktioner som beskrivs av Försvarsmakten inte till fullo omfattar de hot som uppstår i och med en internetanslutning.

3.2 Nuläge

Åtkomst till Internet från FM AP kan delas in i två olika delar; användarorienterad och applikationsorienterad internetåtkomst. Användarorienterad internetåtkomst kan likställas med den trafik som sker via en webbläsare. Applikationsorienterad internetåtkomst avser den åtkomst som sker från andra applikationer, exempelvis Microsoft Office, för att hämta Clipart eller mallar, eller för anti-virusapplikationer som hämtar uppdaterade anti-virusdefinitioner.

I dag sker all användarorienterad internetåtkomst från FM AP via ett fjärrskrivbord[11], en lösning kallad Charon. Ingen direktanslutning mellan FM AP och Internet är möjlig. Dagens lösning upplevs begränsande, såväl i funktionalitet som i användbarhet. Användbarheten begränsas av inloggningsförfarandet på en fjärrdator samt av ett långsamt användargränssnitt.

Den applikationsorienterade internetåtkomsten från FM AP sker genom att applikationen kontaktar en server som i sin tur har åtkomst till Internet. Detta medför att varje applikation som behöver internetåtkomst kräver en skräddarsydd lösning.

[11] Eng. Remote Desktop

3.3 Sekretessindelning i Försvarsmakten

Försvarsmakten utgår från offentlighets- och sekretesslagen (2009:400), OSL, för att avgöra vilka uppgifter som omfattas av sekretess och vilka uppgifter som inte gör det. De uppgifter som omfattas av sekretess indelas i hemliga (H), utrikes-klassificerade (UK) samt sekretessklassificerade (SK) uppgifter. Hemliga och utrikesklassificerade uppgifter indelas vidare i en respektive fyra klasser i enlighet med bild 1.

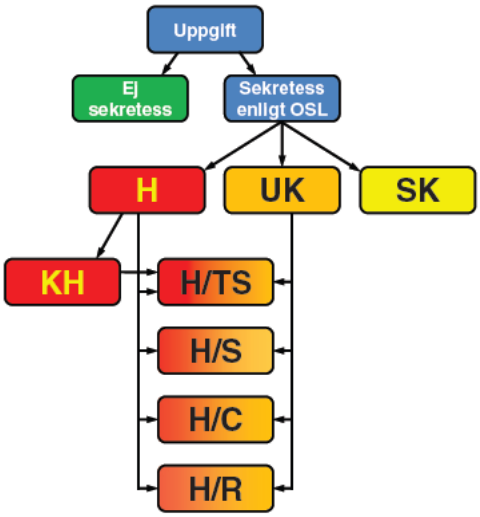


Bild 1, Sekretessindelning inom försvarsmakten[12]

För hemlig uppgift finns klassen kvalificerat hemlig och för utrikesklassificerad uppgift finns HEMLIG/RESTRICTED (H/R), HEMLIG/CONFIDENTIAL (H/C), HEMLIG/SECRET (H/S) och HEMLIG/TOP SECRET (H/TS).

Om flera uppgifter av en informationssäkerhetsklass återfinns i ett dokument eller IT-system, kan detta behöva en högre informationssäkerhetsklass än de enskilda uppgifterna. Denna princip kallas för aggregation[13]. En mängd H/R-klassificerade uppgifter kan således medföra att ett dokument eller IT-system som helhet ska klassificeras som H/C.

Denna utredning omfattar endast internetåtkomst från IT-system vilka högst hanterar uppgifter klassade som SK, men inte H eller UK.

[12] H Säk Sekrbed A (2011), sidan 12
[13] H Säk Sekrbed A (2011), sidan 45

3.4 Förändrad hotbild

Traditionella skyddsåtgärder har tidigare kunnat stoppa internetbaserade hot genom att analysera trafikegenskaper, såsom avsändare, mottagare och protokoll. Mer moderna attacker utnyttjar godkänd trafik men med skadligt innehåll. Därmed kan angreppet passera skyddsåtgärder som enbart analyserar mot trafikegenskaper. För att bemöta denna förändrade hotbild är det viktigt att skyddsåtgärderna har möjlighet att genomföra innehållsbaserade analyser.

Skiftet från trafikorienterade angrepp till innehållsorienterade angrepp innebär att hotbildens fokus skiftat från system till användare. Samtidigt har Internet utvecklats från ett forum med relativt kontrollerad publicering till ett forum med dynamiska tjänster där användarna kan bidra med material. Sociala media, forum och bloggar är exempel på dynamiska tjänster där en angripare kan plantera skadlig kod. Det är vanligt att utnyttja sociala knep[14] för att angriparen skall få åtkomst till IT-system genom att helt enkelt överlista användaren.

Dagens angrepp av denna typ har blivit så avancerade att det kan vara svårt att skydda sig, även för en säkerhetsmedveten person[15]. Kunskap är dock fortfarande användarens främsta verktyg och utgör en vital del av organisationens skyddsnivå[16].

[14] Eng. Social engineering
[15] Cisco 2010 Annual Security Report
[16] Websense 2010 Threat Report

4 Funktionsönskemål

Försvarsmaktens önskade funktionalitet för internetåtkomst kan delas in i två målgrupper, användare och applikationer. Skillnaden mellan målgrupperna är hur de kan interagera med andra IT-system för att åstadkomma internetåtkomst samt var den internetbaserade koden exekveras. Internetbaserad kod är all kod som hämtas från Internet, inte enbart exekverbara filer utan inkluderar även bilder och textdokument. Denna kod kan oavsett om den exekveras eller används som indata till en annan applikation utnyttja sårbarheter i en dator.

En användares upplevelse av en session styrs bland annat av tillgänglighet och svarstider. Det viktiga för en användare är att önskat resultat uppnås, till exempel att en video spelas upp med god kvalité och inom rimlig tid från det att den begärdes. Var i systemet som själva koden exekveras är dock sällan något användaren behöver fundera på vilket ger en utökad möjlighet avseende arkitektur. En användare kan interagera med IT-system för att åstadkomma en internetåtkomst, till exempel genom en inloggningsprocess med ett engångslösenord.

Applikationer kan anpassas för att hantera internetåtkomst, men erbjuder ingen eller begränsad interaktivitet med andra IT-system. Åtkomsten måste därför ske enligt i förväg fastställda processer. Applikationernas internetanvändning är generellt sett innehållsfokuserad och erbjuder bättre funktionalitet till användaren. Den internetbaserade koden exekveras då förr eller senare på samma dator som applikationen.

De funktionsönskemål som framkommit är:

RSS: Försvarsmaktens användare bör kunna följa RSS-flöden (Really Simple Syndication) från internetbaserade källor. På så sätt kan en användare till exempel följa ett nyhetsflöde i realtid genom att abonnera på flödet och få automatiska uppdateringar när en förändring skett. RSS-flödet är xml-filer[17], det vill säga text med viss formatering.

Ljud: Försvarsmaktens användare bör kunna höra ljud som sänds via Internet. Det kan exempelvis vara ljud som är en del av en sida eller en strömmande ljudsändning såsom webbradio.

Det finns även en form av ”internetmedia” som kallas podcasts. Det är en ljud eller videofil som användaren kan ladda ner och lyssna eller titta på. En podcast kan likställas med hämtade filer.

Video: Försvarsmaktens användare bör kunna se strömmande video som sänds via Internet, exempelvis webbaserade kurser eller tv-utsändningar.

[17] XML, Extensible Markup Language

Klientbaserad videokonferens: Försvarsmaktens användare bör ha tillgång till klientbaserad videokonferens. Den klientbaserade videokonferensen ställer krav på samverkan med kamera och mikrofon samt att ljud och bild skall kunna skickas i realtid från användarens klient.

Direktmeddelanden: Försvarsmaktens användare bör ha tillgång till system för direktmeddelanden[18]. Direktmeddelanden är en snabb kommunikations-metod som tillåter användaren att se och utbyta information med andra. Programmen för direktmeddelanden hanterar textmeddelanden, ljud, bild och filöverföring och kan också inkludera klientbaserad videokonferens.

Klipp och klistra: Försvarsmaktens användare bör ha möjlighet att klippa och klistra information mellan FM AP och Internet. Det kan till exempel röra sig om att kopiera textstycken eller länkar.

Länkar: Försvarsmaktens användare bör ha möjlighet att följa en länk, exempelvis på intranätet eller i e-posten genom att klicka på den.

Hämta och skicka filer: Försvarsmaktens användare bör ha möjlighet att hämta och skicka filer. Det kan till exempel röra sig om bilagor till e-post, nedladdade och uppladdade filer.

Favoriter: Försvarsmaktens användare bör ha möjlighet att lägga upp egna favoriter eller bokmärken i webbläsaren.

Applikationskommunikation: Utvalda applikationer på FM AP bör ha möjlighet att kommunicera med Internet. Ett exempel kan vara för applikationer som hämtar nytt material såsom Clipart eller mallar.

Insticksmoduler: FM AP bör ha stöd för så kallade insticksmoduler. En insticksmodul är ett program som helt eller delvis integreras med webbläsaren och kan användas för att ge användaren ett mervärde. Det finns ett antal allmänna insticksmoduler som bör vara allmänt tillgängliga. Det finns även en önskan att det skall vara möjligt att använda övriga, mindre spridda moduler.

Användbarhet: Internetåtkomsten från FM AP bör vara lättillgänglig för användaren.

Nivån på funktionsönskemålen är av varierar, från tekniska behov till ökad användbarhet. Försvarsmakten är också enligt egna direktiv positiv till användningen av sociala medier, både som myndighet och för dess personal. [19] Sociala medier kan enligt samma källa bland annat vara ett viktigt stöd för personal vid utlandstjänstgöring.

[18] Eng. Instant messaging
[19] Remiss till Direktiv om Försvarsmaktens hantering av sociala medier, 2011

5 Hotbild

Hotbilden är en sammanställning av tänkbara angripare (aktör), aktörens motiv, aktörens medel samt vilka metoder aktören kan tänkas använda i sitt angrepp. Följande hotbild uppstår om Försvarsmakten erbjuder internetåtkomst från SK-miljön.

5.1 Datanätverksoperationer

Datornätverksoperationer (CNO)[20] är en samlingsterm för avsiktliga handlingar i syfte att angripa eller försvara ett IT-system.[21] Operationerna indelas vidare i angrepp (CNA), försvar (CND) och utnyttjande (CNE)[22]. Ur ett hotbilds-perspektiv är endast attack och utnyttjande aktuellt. En datanätverksoperation initieras från utsidan men det är tänkbart att interna aktörer utnyttjas.

Datanätverksoperationer genomförs av en medveten och välfinansierad aktör och kan förväntas ske på ett metodiskt och organiserat sätt. Främmande makt, kriminella grupperingar eller icke-statliga organisationer är tänkbara aktörer. En operation har i detta fall affärsmässiga motiv, exempelvis att tillförskansa sig information och/eller störa Försvarsmaktens verksamhet i syfte att öka den egna operativa förmågan. Det kan också vara ekonomisk vinning, till exempel genom att sälja uppgifter eller att tillförskansa sig militär materiel.

Datanätverksoperationer utförda av främmande makt utgör enligt MUST det enskilt största hotet mot Försvarsmakten inom cyberområdet.[23]

Tabell 1, Sammanställning datanätverksoperationer

Sammanställning datanätverksoperationer	
Aktör:	Främmande makt, kriminella grupperingar eller icke-statliga organisationer.
Motiv:	Affärsmässigt eller politiskt, såsom egen eller angripen makts operativ förmåga. Ekonomisk vinning.
Medel:	Välfinansierade, hög kompetens och stark motivation.
Metoder:	Medveten handling med alla tänkbara metoder.

[20] Eng. Computer Network Operations
[21] Joint Publication 1-02 Dictionary of Military and Associated Terms. Department of Defence, 8 november 2010.
[22] Eng. Computer Network Attack, Computer Network Defence, Computer Network Exploit
[23] Årsrapport Säkerhetstjänst 2009, sid. 22

5.2 Asymmetriska datanätverksoperationer

En asymmetrisk datanätverksoperation genomförs av en enskild individ eller en mindre grupp. Angreppet är medvetet. Kompetensen hos aktören kan likställas med kompetensen hos datanätverksoperationsaktören men finansiella och organisatoriska medel är begränsade.

En betydande skillnad mot fullskalig datanätverksoperation är att motivet är personligt. En asymmetrisk datanätverksoperation kan initieras från både insidan och utsidan. Det kan handla om missnöjd personal som vill hämnas eller någon som vill utnyttja sina kunskaper för egen vinning. Detta innebär att befintliga skyddsåtgärder kan sättas ur spel eftersom aktören kan ha behörighet till de angripna systemen. Det kan också vara externa aktörer som vill uttrycka sin åsikt om Försvarsmakten och dess verksamhet. Denna typ av angrepp kan tänkas utnyttja alla tänkbara angreppsmetoder.

Tabell 2, Sammanställning Asymmetrisk datanätverksoperationer

Sammanställning asymmetriska datanätverksoperationer	
Aktör:	Individ eller mindre grupp.
Motiv:	Personligt, såsom egen vinning, hämnd eller känslomässiga motiv.
Medel:	Hög kompetens och stark motivation. Eventuellt behörighet.
Metoder:	Medveten handling med alla tänkbara metoder.

5.3 Spontana angrepp

Vid sidan av de mer organiserade angreppen finns det också ett utökat hot från spontana angrepp för en internetansluten organisation. Spontana angrepp kan vara medvetna eller omedvetna angrepp utförda av en extern aktör utan uttalat syfte eller mål. Ett exempel på ett medvetet angrepp kan vara en person eller en grupp som använder webbsidor med skadlig kod för att inleda ett angrepp. När någon besöker en sådan sida öppnas en potentiell väg in. Lite slarvigt kan det säga att tillfället gör tjuven och mål för angrepp blir helt enkelt den som besöker sidan. Om angreppet lyckas kan det sedan utvecklas eller avvecklas, beroende på vad aktören finner. Exempel på omedvetna angrepp kan vara utbrott av skadlig kod hos andra organisationer som i sin tur drabbar Försvarsmakten.

Tabell 3, Sammanställning spontana angrepp

Sammanställning spontana angrepp	
Aktör:	Individ eller mindre grupp.
Motiv:	Inget uttalat motiv mer än att möjligheten till angrepp finns.
Medel:	Hög kompetens.
Metoder:	Medveten eller omedveten handling med alla tänkbara metoder.

5.4 Oavsiktlig händelse

Oavsiktlig händelse är ett hot som uppstår som en konsekvens av en handling som utförs av en betrodd person. Det kan vara personal som medvetet eller omedvetet använder systemet på fel sätt. Det kan också vara rena handhavandefel som därmed utlöser en oönskad händelse. Gemensamt är att den betrodda personens behörighet kan kringgå normala skyddsåtgärder vilket kan få allvarliga konsekvenser.

Till skillnad mot övriga hot är angreppet oavsiktligt och det sker inte någon aktiv åtgärd för att fullfölja ett angrepp. En oavsiktlig händelse kan dock leda till att relevanta skyddsåtgärder sätts ur spel vilket kan utlösa andra angreppsformer.

Oavsiktliga händelser har sitt ursprung internt men kan i andra hand utnyttjas av extern angripare.

Tabell 4, Sammanställning oavsiktlig händelse

Sammanställning oavsiktlig händelse	
Aktör:	Betrodd person.
Motiv:	Angreppet är inte handlingens avsikt.
Medel:	Behörighet.
Metoder:	Oavsiktlig händelse med alla tänkbara metoder.

6 Sårbarheter

Det finns sårbarheter som uppstår när ett datanät ansluts till Internet. Dessa internetrelaterade sårbarheter exponerar Försvarsmaktens IT-system och informationstillgångar och kan utnyttjas för angrepp mot Försvarsmakten.

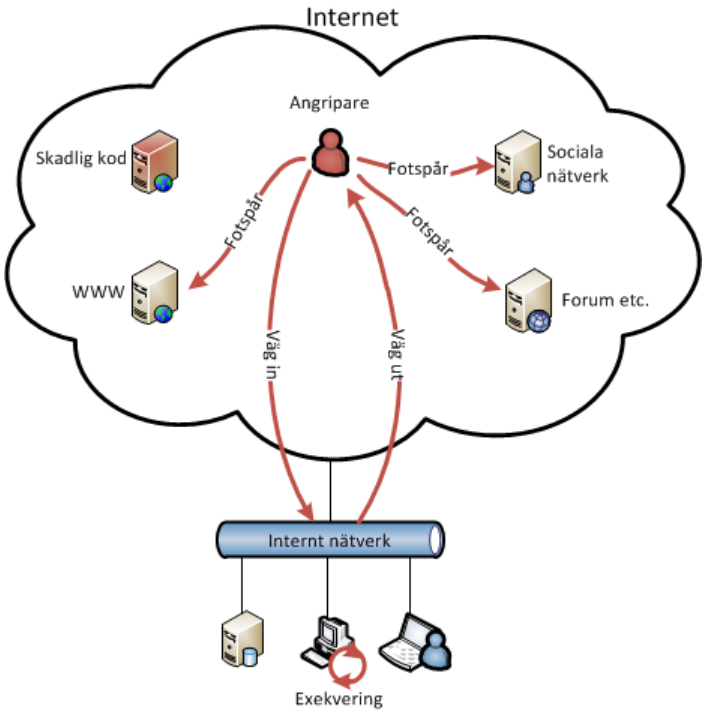


Bild 2, Internetrelaterade sårbarheter

Bild 2 ger en generaliserad bild över de sårbarheter ett system får då det ansluts mot Internet.

Det digitala fotspåret är det spår eller avtryck som en besökare lämnar på Internet. Det kan till exempel vara information om vilka webbsidor som har besökts, inlägg på forum eller uppgifter om sökmönster. Denna information är öppen och kan användas som informationskälla av en potentiell angripare.

En väg in behövs för att användaren skall kunna ta emot data från och interagera med IT-system på Internet. Vägen in är även det som gör det möjligt att initiera ett internetbaserat angrepp mot Försvarsmakten.

Exekvering av internetbaserad kod är i de flesta fall en förutsättning för att använda Internet. Det kan vara en webbsida som visas för användaren eller en

video som denne tittar på. Internetåtkomsten innebär att internetbaserad kod ges möjlighet att exekvera på de egna IT-systemen vilket möjliggör ett angrepp.

En väg ut behövs för att användaren skall kunna styra vilka data som hämtas från Internet samt för att kunna sända information. Vägen ut ger samtidigt en möjlighet för en angripare att kontrollera ett angrepp samt att läcka information.

Alla internetrelaterade angrepp utnyttjar en eller flera av dessa sårbarheter. Det är kanske framför allt den första fasen som varierar då ett angrepp kan, till exempel, initieras via ett USB-minne som fysiskt förs in till systemet. Detta kan ske med uppsåt, men kanske vanligast utan att budbäraren har något illasinnad avsikt. Den initiala vägen in i ett system för en angripare kan därmed variera men väl inne är angrepp likartade då de oftast kontrolleras utifrån. Därav kommer fall med en fysisk väg in i ett system, till exempel via ett USB-minne, inte att utredas vidare. Rapporten kommer enbart att fokuserar på de internetrelaterade sårbarheterna.

7 Arkitektur

Arkitektur avser sättet på vilket komponenter i ett IT-system organiseras. Dess primära funktion är att tillgodose den funktionalitet som Försvarsmakten efterfrågar. Dock kan arkitekturen även påverka till vilken grad Försvarsmaktens IT-system exponeras utåt genom att minska de sårbarheter som uppstår när ett datanät ansluts till Internet.

Arkitekturer kan med fördel användas som byggstenar och kan kombineras för att erhålla en internetåtkomst med önskad funktionalitet med en låg exponering.

7.1 Direktansluten

Med direktansluten arkitektur enligt bild 3 sker all internetåtkomst och den resulterande exekveringen av internetbaserad kod direkt från FM AP. Det är en flexibel arkitektur som uppfyller önskemålen av utökad funktionalitet för både användare och applikation. Den direktanslutna arkitekturen hanterar ingen av de internetrelaterade sårbarheterna vilket leder till den högsta exponering av Försvarsmaktens interna IT-system och informationstillgångar.

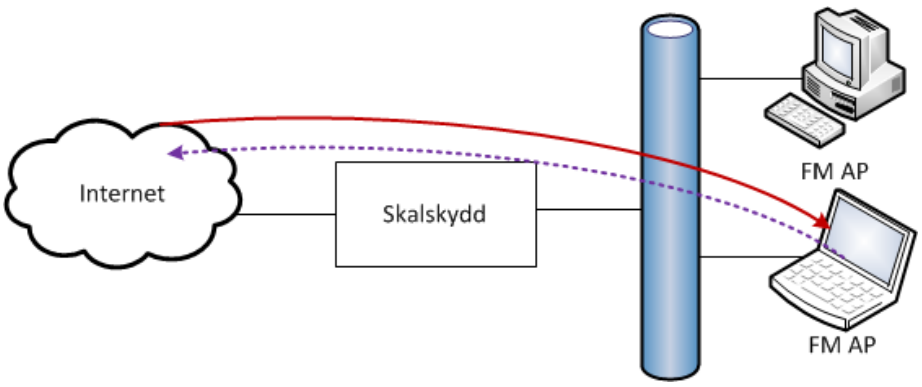


Bild 3, Direktansluten arkitektur

När det gäller distansarbete med direktanslutna FM AP är det möjligt att erbjuda samma funktionalitet både inom och utanför Försvarsmaktens lokaler. Vid distansarbete blir exponeringen av FM AP högre eftersom att den enskilda datorn kopplas mot Internet utan att passera de skyddsåtgärder som det lokala Försvarsmaktsnätverket har. Detta går att åtgärda genom att tunnla all trafik genom Försvarsmaktens skyddsåtgärder.

Fördelar med denna arkitektur är att:

- Arkitekturen erbjuder flexibilitet för både användare och applikationer.

- Detta är den arkitektur som merparten av alla programvaror utvecklats för vilket innebär att inga anpassningar behövs för att erhålla önskad funktionalitet.

Nackdelar med denna arkitektur är att:

- Arkitekturen hanterar inga av de internetrelaterade sårbarheterna.
- Skyddet av FM AP vid distansarbete försvåras.

7.2 Virtuell dator

En virtuell dator körs som en applikation på en klient eller en server enligt bild 4. Den virtuella datorn är logiskt åtskild från dess fysiska värd och har ett eget operativsystem och egna applikationer. Det sker ingen direkt kommunikation mellan värd och virtuell dator. De applikationer som behöver internetåtkomst kan därför exekveras i en logiskt isolerad miljö sett från FM AP vilket leder till en lägre exponering av Försvarsmaktens interna tillgångar. Om en applikation behöver åtkomst till både interna tillgångar och Internet förloras den logiska isoleringen och den virtuella datorn kan likställas med en direktansluten arkitektur.

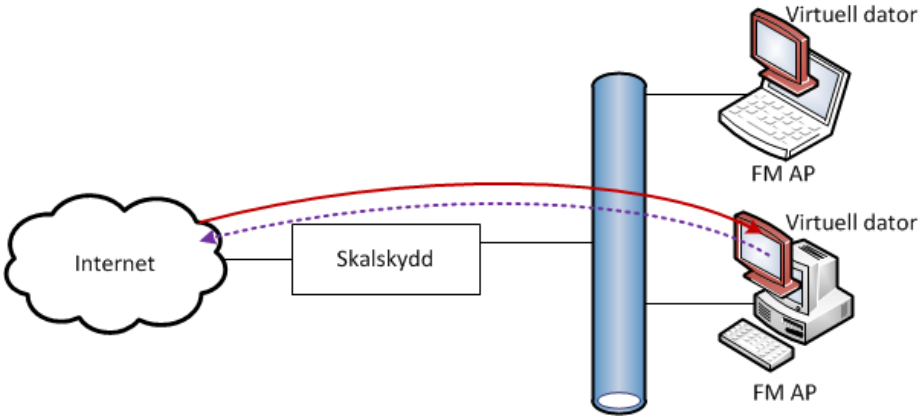


Bild 4, Virtuell dator, internetåtkomst från en logisk dator i FM AP

Det är möjligt att logiskt binda viss hårdvara till den virtuella datorn, till exempel ett nätverkskort. Genom att anpassa FM AP med dubbla nätverkskort kan en parallell klientstruktur skapas med samma fysiska FM AP som grund. Om inte någon parallell struktur byggs upp kommer Internet att vara tillgängligt på den fysiska värden och måste hanteras med enhetsbaserade skyddsåtgärder.

Möjligheten till distansarbete påverkas av hur den virtuella datorn hanterar sina nätverkskopplingar. Används samma nätverkskort för fysisk och virtuell dator

fungerar distansarbete på motsvarande sätt som anslutning i Försvarsmaktens lokaler. Används istället alternativet med en separata nätverkskort krävs det att användaren ansluter rätt nätverk till rätt nätverkskort.

För att erhålla samma skyddsnivå vid distansarbete måste trafiken passera genom Försvarsmaktens skyddsåtgärder.

Fördelar med denna arkitektur är att:

- Arkitekturen gör det möjligt att logiskt isolera Internet från Försvarsmaktens interna IT-system och informationstillgångar.

Nackdelar med denna arkitektur är att:

- Arkitekturen kan vara svår för användaren att hantera för distansarbete.
- Den logiska isoleringen bygger på att applikationen som exekverar den virtuella datorn inte innehåller några sårbarheter.
- Arkitekturen förutsätter att applikationer som exekverar internetbaserad kod ej kräver åtkomst till Försvarsmaktens tillgångar.

7.3 Sandlåda

Sandlådan[24] är en arkitektur som skapas med en sandlådeapplikation, vilken logiskt isolerar den applikation som körs i sandlådan. Målet är att minska den interna exponeringen i FM AP genom att neka tillträde till andra applikationer och systemresurser enligt bild 5. Sandlådearkitekturen motverkar också förändringar på de program som körs isolerat.

Skillnaden mot en virtuell dator är att sandlådearkitekturen saknar ett eget operativsystem och att den därmed inte kan hantera egen hårdvara. All kommunikation med omvärlden sker via FM AP. En konsekvens av detta blir att det går att åstadkomma viss kontrollerad samverkan mellan den isolerade applikationen och FM AP. En annan konsekvens blir att Internet även kommer att vara åtkomlig från FM AP och dess övriga applikationer vilket måste hanteras med enhetsbaserade skyddsåtgärder.

Med sandlådearkitekturen kan samma applikation köras isolerat för internetåtkomst eller oisolerat för intern åtkomst. På så sätt behövs inte dubbla licenser eller installationer.

[24] Eng. Sandbox

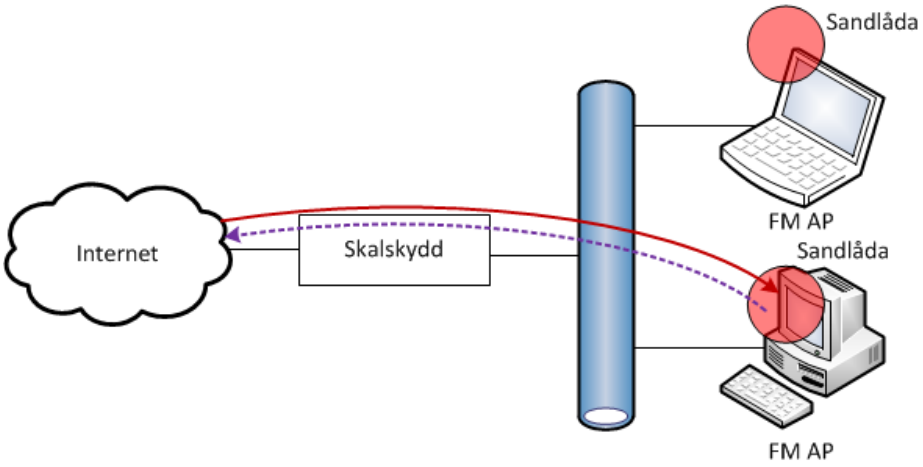


Bild 5, Sandlåda, internetåtkomst från en isolerad applikation på FM AP

Sandlådeapplikationen fungerar på samma sätt oavsett var datorn befinner sig och således påverkas inte möjligheten till distansarbete. För att erhålla samma skyddsnivå för FM AP vid distansarbete måste trafiken passera genom Försvarsmaktens skyddsåtgärder.

Fördelar med denna arkitektur är att:

- Arkitekturen medför att all exekvering av internetbaserad kod kan ske i en logiskt isolerad miljö.
- Det finns en möjlighet till kontrollerad samverkan med övriga applikationer på FM AP
- Det går att använda samma installation av en applikation både isolerat och oisolerat.

Nackdelar med denna arkitektur är att:

- Den logiska isoleringen bygger på att applikationen som exekverar sandlådan inte innehåller några sårbarheter.
- Internet kommer att vara tillgängligt på FM AP och måste begränsas med skyddsåtgärder.
- Användaren kan ha svårt att förstå när applikationer som har åtkomst till interna IT-system respektive Internet.

7.4 Terminalserver

Terminalserver är en arkitektur där exekvering sker på en annan dator än den egna enligt bild 6. Användaren ser egentligen bara själva resultatet av exekveringen. All kommunikation mellan FM AP och terminalservern sker med specifika terminalserverprotokoll och är relativt enkel att kontrollera. Försvarsmaktens interna IT-system och informationstillgångar kan då placeras i en annan säkerhetsdomän än servern som exekverar den internetbaserade koden. Arkitekturen möjliggör på detta sätt en separation mellan internetåtkomsten och SK-miljön. Om en angripare skulle tillförskansa sig kontrollen över en terminalserver så är angreppet isolerat till den aktuella säkerhetsdomänen.

För en användare upplevs inte nödvändigtvis någon skillnad mellan en applikation som exekverar lokalt och en som exekveras på en terminalserver. Det är resultatet av exekveringen som är intressant för användaren.

En applikation som ges åtkomst till Internet och interna resurser samtidigt, till exempel en ordbehandlare, medför en utökad kommunikation mellan terminalserver och SK-miljön. Därmed förloras separationen mellan exekveringen av internetbaserad kod och intern åtkomst. Ur ett applikationsperspektiv är därför den säkerhetsrelaterade nyttan med en terminal-serverarkitektur begränsad jämfört med en direktansluten arkitektur.

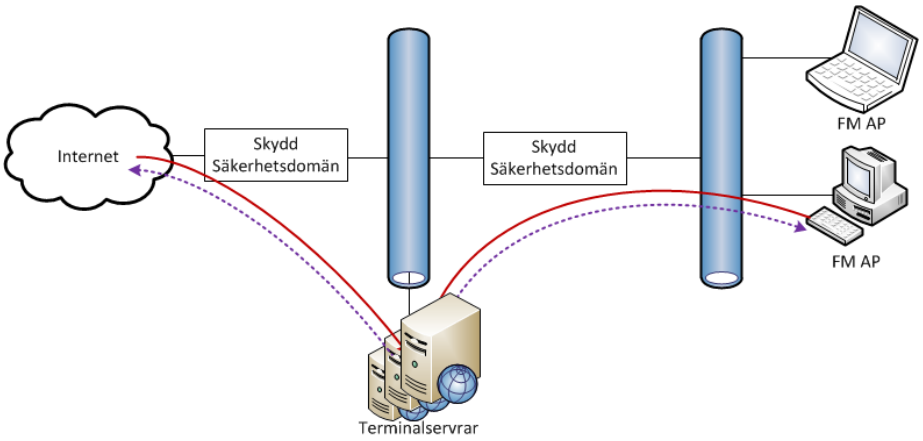


Bild 6, Terminalserverarkitektur

Det är möjligt att justera hur användaren upplever en terminalserverlösning genom att avgöra hur applikationerna visas för användaren. Följande alternativ finns:

Fjärrskrivbord: användaren ansluter och loggar in på en annan dator och startar därefter sin applikation.

Publicerad terminalserver: användaren startar ett program som i sin tur presenterar vilka applikationer som finns tillgängliga för användaren.

Publicerad applikation: en genväg publiceras direkt på användarens dator och applikationen startas på sedvanligt sätt.

Portal: användaren surfar till en portal och startar sin applikation från denna.

Det finns idag ett antal COTS[25]-alternativ som kan erbjuda de olika typerna av terminalserverlösningar som presenteras ovan.

Distansarbete via en terminalserverarkitektur kan ske genom att användaren ansluter till Försvarsmaktens IT-system via en krypterad tunnel. På så sätt har användaren samma skydd och samma funktionalitet oavsett var i världen denne befinner sig. Exponeringen av FM AP vid distansarbete måste hanteras av enhetsbaserade skyddsåtgärder.

Fördelar med denna arkitektur är att:

- Terminalserverarkitekturen gör det möjligt att åtskilja exekvering av internet-baserad kod från Försvarsmaktens IT-system och informationstillgångar.
- En användare behöver inte samma rättigheter på en server som på en klient vilket gör det möjligt att härda servern.

Nackdelar med denna arkitektur är att:

- De applikationer som behöver internetåtkomst kan ej ges åtkomst till Försvarsmaktens interna system utan att bryta isoleringen.
- Det kan vara svårt att hantera klientansluten hårdvara såsom kameror.

7.5 Ombudsarkitektur

En ombudsarkitektur innebär att FM AP ansluter till en server som i sin tur ansluter till Internet enligt bild 7. Därmed sker ingen direkt kommunikation från FM AP till Internet utan servern agerar ombud för klienten. Skillnaden mellan ombudsarkitekturen och terminalserverarkitekturen är att med ombuds-arkitekturen sker exekveringen av den internetbaserade koden till slut på FM AP. Ombudsarkitekturen är främst aktuell ur ett applikationsperspektiv eftersom den inte är tillräckligt flexibel för att interagera med användaren.

Eftersom olika applikationer har olika krav och möjligheter behöver denna arkitektur anpassas till varje applikation eller funktion den skall leverera. Det är tänkbart att flera parallella ombudsarkitekturer behöver utnyttjas för att erbjuda den funktion som efterfrågas. Nedan följer ett par tänkbara exempel.

[25] COTS – Commersial off the shelf, kommersiellt tillgänglig programvara.

Filsluss: En filsluss är ett system som mellanlagrar filer som hämtas och/eller lämnas på Internet. Användaren måste utöver själva överföringen göra en medveten handling för att filen skall nå sitt mål vilket försvårar angrepp. Ett exempel kan vara att använda nätverksmappar eller filöverföringsprotokoll för att hantera detta via nätverket, ett annat exempel kan vara att använda flyttbara media såsom USB-minnen. Den senare ger en lägre exponering men minskar användbarheten.

Innehållsserver: En innehållsserver är ett system som hämtar en viss typ av statisk data från Internet. Applikationen på FM AP ansluter sedan till innehållsservern istället för till den Internetbaserade källan. Denna lösning är lämplig för till exempel Clipart, mallar eller systemuppdateringar.

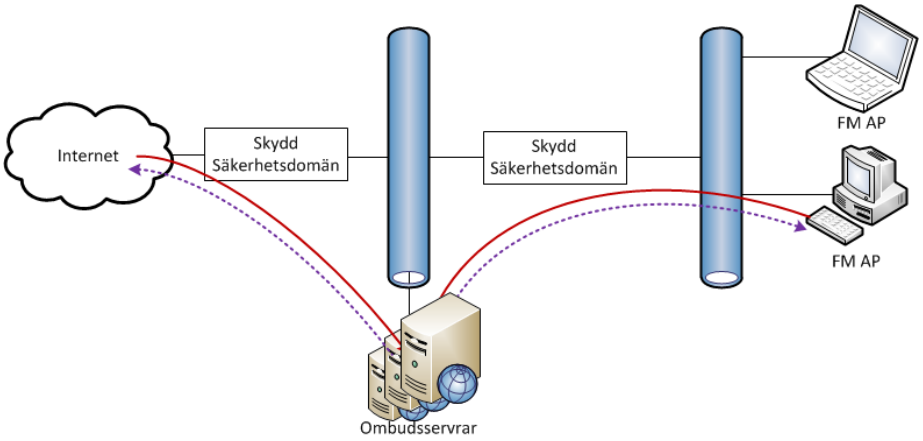


Bild 7, Ombudsarkitektur

Ombudsarkitekturen innebär att en anslutning mot Försvarsmaktens IT-system måste ske för att tjänsterna skall vara nåbara. Exponeringen av FM AP vid distansarbete måste hanteras av enhetsbaserade skyddsåtgärder.

Fördelar med denna arkitektur är att:

- Arkitekturen möjliggör att applikationer på FM AP kan kommunicera med Internet via indirekt anslutning.

Nackdelar med denna arkitektur är att:

- Det kan krävas specialanpassning av arkitekturen för att stödja en applikation.
- Det kan finnas applikationer som inte stödjer ombudsarkitekturen.

8 Hot

Hot är en möjlig, oönskad händelse som får negativa konsekvenser för verksamheten. Ett hot utnyttjar oftast sårbarheter i befintliga system, även om andra sårbarheter är tänkbara, och beskrivs här utifrån den internetrelaterade sårbarhet de primärt utnyttjar. I det här kapitlet beskrivs fyra generaliserade typer av hot; Digitalt fotspår, Väg in, Exekvering, samt Väg ut. Dessa hot uppkommer som en följd av att ett nät ansluts mot Internet.

8.1 Digitalt fotspår

En angripare kan samla in information om ett system både med offensiva metoder men även genom mer diskreta. Då en offensiv metod används utmanar angriparen det system som denne har som mål att angripa, i syfte att studera den trafik angreppet genererar. Vid mer passiva metoder utnyttjar angriparen den trafik som en användare normalt genererar samt den information som finns tillgänglig om systemet i fråga.

8.1.1 Sondering

Sonderingen är en aktivitet med syfte att åstadkomma och registrera svar från (mål)systemet som kan ge information om systemets konfiguration och uppbyggnad.[26] Det är en direkt förberedande aktivitet inför ett eventuellt angrepp. Avsikten är att kartlägga målet och hitta möjliga sårbarheter mot vilket angreppet kan riktas. Exempel på metoder för sondering är bannergrabbing, portavsökning och protokollspecifika meddelanden.

8.1.2 Avlyssning

Avlyssning innebär att en angripare följer ett pågående trafikflöde för att tillgodogöra sig informationen. Avlyssning förenklas av att viss trafik mellan användarens dator och Internet sker i klartext på gemensamma kanaler, såsom oskyddade trådlösa nätverk. I dessa fall kan en angripare se trafiken genom att vara ansluten till samma nätverk.

Denna form av avlyssning är framförallt ett hot vid distansarbete då användaren ansluter sig via publika nät.

[26] SIS HB 550, Utgåva 3, 2007

8.1.3 Öppen information

Den öppna informationen kan utnyttjas för spaning och som förberedelse till angrepp. Principen är enkel, genom att samla in, sammanställa och analysera allmänt tillgänglig information som användaren har lämnat på Internet skapas en bild av målet. Denna bild kan sedan utnyttjas för vidare angrepp, rekryteringsförsök eller som en informationskälla i sig.

Med en bättre internetåtkomst kan exponeringen genom öppen information öka på flera sätt. För det första blir en större mängd information från Försvarsmaktens personal troligen tillgänglig på Internet i och med utökad användning. För det andra är det lättare att binda informationen till Försvarsmaktens personal i och med att alla kommer från en gemensam känd adress.

8.2 Väg in

Det är ofta svårt för en angripare att direkt attackera ett system framgångsrikt och därmed kunna sprida sin skadliga kod inom det angripna systemet. I de fall detta sker har systemen ofta en svaghet i sin programkod eller installation som angriparen känner till. En kanske vanligare metod är att locka eller vilseleda en användare att själv öppna upp för ett angrepp.

Försvarsmakten var under 2009 utsatt för ett stort antal angrepp med skadlig kod och analysen visar att det främst handlat om trojaner som försöker skapa en förbindelse genom befintliga säkerhetssystem.[27] En slutsats från 2009 är att den separerade nätverksarkitekturen har gett Försvarsmakten ett relativt gott skydd mot skadlig kod.[28] Det visade sig dock under 2010 när masken Stuxnet spred sig att separerade nätverk inte nödvändigtvis innebär ett definitivt skydd. Anledningen till detta var att Stuxnet kunde spridas genom överföring via USB-minnen.[29]

8.2.1 Bakdörr

En bakdörr är en odokumenterad funktion i ett program som kan utnyttjas till att kringgå normala kontroller vid programmets användning och som därvid exempelvis kan åsidosätta eller kringgå säkerhetsskyddet.[30] Ur ett internet-perspektiv kan åtkomst till ett system innebära att en bakdörr utnyttjas på distans.

[27] Årsrapport Säkerhetstjänst 2009, sid. 23
[28] Årsrapport Säkerhetstjänst 2009, sid. 23
[29] Symantec Internet Security Threat Report,Trends for 2010 Volume 16
[30] SIS HB 550, Utgåva 3, 2007

8.2.2 Farmning

Framning[31] är en omdirigeringsattack som syftar till att leda ett stort antal användare till en falsk webbsida.[32] Väl där kan angriparen till exempel utsätta besökaren för skadlig kod eller lura denne att uppge användarnamn och lösenord.

Vanliga metoder för farmning är bland annat DNS[33]-förgiftning, sökmotor-optimering[34] och förkortade URL:er[35].

8.2.3 Spoofing

Spoofing innebär att en användare eller ett program uppträder under falsk identitet och därigenom erhåller behörighet. Ett exempel kan vara att förfalska sin egentliga avsändaradress för att lura användare eller applikation, ett annat att angriparen logiskt placerar sig mellan de kommunicerande parterna[36] och agerar som om de kommunicerade direkt med varandra.

8.2.4 Webbaserad aktiv kod

Webbaserad aktiv kod är kod som exekveras när en användare besöker en webb-sida. Den behöver därmed inte finnas på användarens dator innan exekveringen kan ske. Webbaserad aktiv kod används normalt för att leverera någon form av funktion från sidan, till exempel video, ljud eller kundvagnen i en webbshop. En angripare kan utnyttja webbaserad aktiv kod för att angripa exponerade sårbarheter på en besökarens dator och därmed åstadkomma en väg in.

På vissa sidor som forum, bloggar eller sociala medier kan den aktiva koden även skapas av andra besökare. Det är därför fullt möjligt för en angripare att placera skadlig webbaserad aktiv kod på en legitim sida.

Koden behöver inte heller befinna sig på den webbsida som användaren besöker utan en angripare kan se till att koden hämtas från en annan server med hjälp av så kallad Cross site scripting eller XSS. Den här typen av attack kan innebära att webbsideinnehavarens normala skyddsåtgärder kringgås.

8.2.5 Användaranpassad webb

Användaranpassad webb är webbsidor som presenterar olika innehåll beroende av vem som besöker sidan. På så vis kan en mer riktad webbsida presenteras för besökaren. Baksidan är att det blir svårare att avgöra vad som är en korrekt

[31] Eng. Pharming
[32] SIS HB 550, Utgåva 3, 2007
[33] Domain Name System, namnsystem som översätter mellan namn och de adresser som används på Internet.
[34] Websense 2010 Threat report sidan 8
[35] Eng. Uniform Resource Locator. Webbadress.
[36] Eng. Man in the middle.

webbsida och vad som kan vara en manipulerad sida, då variationen av korrekta sidor kan vara stor. Det finns en uppenbar risk att de skyddsåtgärder som finns för att undersöka webbsideinnehåll agerar felaktigt och därmed hindrar en användares åtkomst till sidan.

8.2.6 Internetanslutna applikationer

I takt med att användaren utnyttjar alltmer avancerad funktionalitet på Internet har antalet applikationer som behövs för att ta del av innehåll ökat. Det kan röra sig om fristående applikationer, insticksmoduler till webbläsaren eller specifika tilläggsprogram från en viss webbsida. Denna utveckling innebär att antalet mjukvarurelaterade sårbarheter som kan utnyttjas som en väg in från Internet har ökat.

8.2.7 Social manipulering

Social manipulering[37] innebär att en angripare använder kunskap och olika sociala knep för att skapa förtroende som kan nyttjas vid ett angrepp. Det kan till exempel vara kunskap om en persons intressen, relationer eller organisationens rutiner. Användandet av sociala medier har lett till att denna angreppsform har ökat både i omfattning och i komplexitet.[38] Dagens angrepp kan därmed troligen även lura kunniga och vaksamma användare.

8.2.8 Filöverföring

Filöverföring är en grundläggande funktion för internetåtkomst. Samtidigt är den ett betydande hot eftersom en fil kan innehålla vad som helst. Det kan vara en till synes legitim fil men som har dolda egenskaper i form av skadlig kod. Filöverföring kan vara en metod som en angripare använder för initialt angrepp eller verktyg som en angripare använder för att utveckla sitt angrepp. Statistik från Symantec visar att överföring av exekverbara filer fortfarande utgör den vanligaste spridningsmekanismen för skadlig kod.[39]

8.3 Exekvering

Exekvering av skadlig kod är grundläggande för att en angripare skall få kontroll över eller orsaka skada på ett IT-system. Skadlig kod är otillåten programkod som är till för att ändra, röja, förstöra eller avlyssna ett elektroniskt kommunikationsnät eller funktioner eller uppgifter i ett IT-system.[40] Skadlig kod kan vara ett självständigt passivt hot eller en aktiv angreppsmetod och verkar i

[37] Eng. Social engineering
[38] Symantec Internet Security Threat Report, 2010 Sidan 4
[39] Symantec Internet Security Threat Report,Trends for 2010 Volume 16, sedan 7
[40] Försvarsmaktens föreskrifter om säkerhetsskydd, 7 kap. 1 § 9

huvudsak genom att utnyttja sårbarheter eller missutnyttja funktioner i en applikation. Spridningsmetoder utvecklas ständigt och inkluderar webbsidor, bifogade eller nedladdade filer och direkt spridning. Det krävs inte alltid någon aktiv handling av användaren för att drabbas av skadlig kod, det kan räcka med att besöka en webbsida vid fel tillfälle. En möjlig verkan av skadlig kod är att försätta skyddsåtgärder ur spel för att möjliggöra ett vidare angrepp. En annan verkan av den skadliga koden är resursstöld (där en resurs kontrolleras av en utomstående angripare, oftast ingående i ett större nät, ett så kallat botnet), informationsstöld eller sabotage men andra varianter är tänkbara.

För några år sedan var risken för att drabbas av skadlig kod störst för användare som besökte sidor innehållande material med mer eller mindre illegal karaktär. Nyare forskning från 2010 visar dock att skadlig kod numera vanligtvis återfinns på sidor där utgivaren är betrodd, på vilka angripare har lyckats plantera skadlig kod alternativt länka till en annan sida där den skadliga koden finns.[41] Samma forskning visar två tydliga trender. För det första att avståndet från en legitim sida till en sida som innehåller skadlig kod ofta bara är två klick. För det andra att aktuella händelser ofta utnyttjas för att få in besökare till sidor med skadlig kod.

Redan känd skadlig kod utgör endast ett ringa hot förutsatt att datorn är utrustad med ett uppdaterat virusskydd.

Okänd skadlig kod är ett betydande hot som internetanslutna system måste hantera. Detta sker genom att analysera den kod som exekveras och leta efter egenskaper eller beteenden som är specifika för skadlig kod. Dessa beteenden är:

Angreppsvektor: Den skadliga koden försöker utnyttja en sårbarhet eller missutnyttja en funktion i en mjukvara eller ett IT-system för att initiera sitt angrepp. Om detta lyckas kan den skadliga koden därefter leverera sin last i form av oönskade instruktioner till IT-systemet.

Maskering: Om den skadliga koden upptäcks kan den stoppas. Upptäckt kan också leda till ökad vaksamhet hos den angripna organisationen vilket i sin tur kan försvåra fortsatt angrepp. Därför vill den skadliga koden motverka upptäckt genom att dess existens eller egentliga funktion maskeras för IT-systemet.

Oönskade instruktioner: Det sista steget för den skadliga koden är att leverera sin egentliga last, det vill säga sina oönskade instruktioner. Ur angriparens perspektiv är det dessa instruktioner som utgör nyttodelen och det kan exempelvis vara att förvanska eller radera utvalda filer alternativt att skapa en dold kanal för kommunikation.

[41] Websense 2010 Threat Report

8.4 Väg ut

En väg ut innebär två olika typer av hot. För det första kan vägen ut utnyttjas för att åstadkomma ett informationsläckage. För det andra tillåter det angriparen att styra och utveckla angreppet. Sårbarheten väg ut utsätts för följande hot:

8.4.1 Informationsläckage

Informationsläckage är en medveten eller omedveten handling som medför att information hamnar i orätta händer. Det kan exempelvis röra sig om missnöjd personal som medvetet läcker information eller om skadlig kod som stjäl information. Informationsläckage kan vara ett resultat av en datornätverks-operation eller ske oavsiktligt genom att någon är oförsiktig i sin hantering av information[42]. Internetanslutningen kan utnyttjas även om angreppet initieras på andra sätt än via de övriga internetrelaterade sårbarheterna.

8.4.2 Dold kanal

En dold kanal innebär att en kanal upprättas mellan den angripna datorn och en av angriparen kontrollerad dator. Att initiera en sådan kanal från utsidan stoppas av skyddsåtgärder men i och med att den initieras från insidan kan dessa kringgås. Den dolda kanalen kan därefter gömmas i tillåten trafik och i vissa fall dessutom vara krypterad vilket ytterligare försvårar upptäckt. Det är också tänkbart att en dold kanal kan upprättas av personal från insidan för att kringgå en oönskad skyddsåtgärd.

8.4.3 Filöverföring

Möjligheten till filöverföring öppnar för utförsel av stor mängd information från ett internt datanät till en mottagare på utsidan vilket kan leda till omfattande informationsläckage. Detta kan till exempel ske via filöverföringsprotokoll, bilagor i e-post, filuppladdning eller molnbaserade lagringstjänster.

8.4.4 Datadropp

Datadropp är en variant av överföring där angriparen försöker undgå upptäckt genom att föra ut en liten bit information i taget. På så vis är chansen stor för att dataöverföringen försvinner i mängden data. Datadropp sker enligt principen lite data över lång tid.

Datadropp kan också ske genom att en angripare lägger till information på legitim trafik. Trafiken behöver inte vara adresserad till angriparen utan denne kan tillgodogöra sig informationen genom avlyssna trafiken och filtrera bort oönskade delar.

[42] Websense 2010 Threat Report, sidan 19

9 Skyddsåtgärder

Skyddsåtgärder är till för att möta de hot som inte kan hanteras av arkitekturen. Skyddsåtgärderna är byggelement som kan användas för att skapa erforderligt skydd. För att åstadkomma ett bra skydd bör skyddsåtgärderna användas enligt lagerprincipen vilket innebär att skyddsåtgärder med samma uppgift kan finnas på flera platser i ett IT-system.[43]

Nedan presenteras en uppsättning olika typer av skyddsåtgärder samt hur dessa kan användas.

9.1 Behörighetskontrollsystem

Behörighetskontrollsystem eller BKS är system som tillsammans reglerar och registrerar användarens aktivitet i ett system.[44]

Ett BKS kan antingen vara unikt för ett visst IT-system eller omfatta flera sådana. Ett gemensamt BKS möjliggör integration med andra skyddsfunktioner samt minskar hanteringen av användare och roller, ökar spårbarheten och underlättar systemsamverkan. Dock ökar samtidigt BKS utsatthet eftersom det reglerar behörigheter till flera IT-system.

De grundläggande funktioner som bygger upp ett BKS är verifiering av användaridentitet, kontroll av användarens behörighet samt loggning av händelser relaterat till detta.

9.2 Säkerhetsloggning

Säkerhetsloggningen syftar till lagra händelser vilka är av säkerhetsmässig betydelse för en verksamhet eller ett system. Säkerhetsloggen kan därefter analyseras av automatiserade verktyg i syfte att upptäcka brister eller misstänkta intrång. Ett effektivt logg- och analyssystem kan ge larm i nära realtid. Kvalitén på säkerhetsloggningen beror på vilken information som loggas. Det är därför lämpligt att säkerhetsloggningen hämtar information från flera källor i det övervakade systemet.

9.3 Övervakning av skyddsåtgärder

Övervakningen omfattar både administrativa och tekniska åtgärder för att upptäcka, identifiera och bemöta angrepp. Övervakning av ett IT-system och dess skyddsåtgärder är kan vara direkt avgörande för hur omfattande skada ett angrepp orsakar. Med en bra central övervakning är det möjligt att anpassa IT-

[43] Broadband testing, Blue Coat web threat report, Steve Broadhead
[44] SIS HB 550, 3:dje utgåvan, 2007

systemet för att minimera eller eliminera en upptäckt sårbarhet innan den kan utnyttjas.

9.4 Skyddsåtgärder mot skadlig kod

Skyddsåtgärder mot skadlig kod kan ske under transport, vid mellanlagring eller vid exekvering. Detta gör det möjligt att bygga ett skydd mot skadlig kod som finns på flera platser i IT-systemet. Hanteringen av skyddsåtgärderna bör vara central för att kunna samordnas. Skyddsåtgärder mot skadlig kod kan omfatta följande funktioner.

Signaturer: Signaturbaserad kontroll sker genom att söka efter redan kända instanser av skadlig kod. Varje instans av skadlig kod ges unik signatur, en så kallad hash. Denna information distribueras till skyddsåtgärden som sedan använder den för att söka efter skadlig kod. Metoden med signaturer kan liknas med en svartlistning[45] och spar systemresurser genom att hantera den stora mängden redan kända varianter av skadlig kod.

Heuristik: En samlingsterm för undersökning och analys i realtid. Principen är att använda de kända beteenden som skadlig kod har för att söka efter skadliga attribut och karakteristika i icke kategoriserad kod. Det finns betydande skillnader i olika leverantörers heuristik varför det inte är möjligt att göra en samlad värdering av den heuristiska skyddsåtgärden. Vissa leverantörer nöjer sig med att söka efter skadliga delar medan andra låter filen exekvera i en isolerad miljö för att sedan dra slutsatser om den är skadlig eller ej.

Applikationshantering: Applikationshantering innebär att skyddet mot skadlig kod kontrollerar den fil som skall exekveras och jämför den med en statisk lista över godkända applikationer. Är inte applikationen med får den inte exekveras, alternativt kan användaren tillfrågas. Denna åtgärd kan liknas med en vitlistning[46] av tillåtna applikationer. Applikationshanteringen kan också användas för att reglera vilka applikationer som får göra vad, till exempel skriva ut eller kommunicera på datanätet.

Rykte: Rykteshantering är en teknik där en leverantör av skydd mot skadlig kod samlar in genomsökningsstatistik för en fil för att sedan avgöra om den bör godkännas eller ej. Varje fil ges en unik signatur, en så kallad hash som sedan kan användas av skyddsåtgärden för att avgöra om filen är säker. Principen för rykteshantering är att om en fil har genomsökts flera tusen gånger utan att skadlig kod blivit funnen är det rimligt att anta att den inte innehåller virus. Rykteshantering kan ses som en utvecklad variant av vitlistning och erbjuder en mer dynamisk skyddsåtgärd än den förra.

[45] En statisk lista med ej tillåtna filer.
[46] En statisk lista med tillåtna applikationer.

9.5 Statiska filter

Ett statiskt filter är en skyddsåtgärd som skyddar mot obehörig åtkomst mellan datanät genom att kontrollera in och utgående trafik enligt ett givet regelverk. Exempel på parametrar som avgör om trafiken tillåts eller inte kan vara källa, destination, port, protokoll, tidpunkt, användare och applikation. Baserat på regelverket kan trafiken tillåtas, nekas eller omdirigeras.

Statiska filter kan hantera stora mängder trafik vilket gör den lämplig som yttre skydd mot okända datanät.

Det finns protokoll som inte skickar sina svar i samma session som förfrågningarna kom, till exempel FTP[47]. För att dessa protokoll ska kunna användas kan sessionskontroll eller Stateful Packet Inspection (SPI) användas. Sessionskontroll är en teknik som underlättar för dessa protokoll att passera statiska filter genom att följa trafiken och tillåta returnerande trafik. Alternativet vore att anpassa regelverket för att tillåta dessa slumpvis inkommande svar vilket skulle leda till säkerhetsmässiga hål i de statiska filtren.

9.6 Adressöversättning

Adressöversättning innebär att avsändarens lokala adress byts ut mot en annan adress för externt bruk. Mottagaren får då se en fungerande adress men som inte avslöjar något om avsändarens interna nätstruktur. En angripare lär sig på så sätt inte mycket om avsändarens nät även om denne samlar på sig flera adresser.

9.7 Dekryptering av flöden

En angripare kan genom att använda krypterade protokoll försvåra upptäckt av den trafik som angreppet genererar. Krypteringen hindrar genomsökning baserat på innehåll och dessa flöden måste dekrypteras för att kunna säkerhets-kontrolleras.

Dekryptering av flöden kan vara kontroversiellt eftersom det bryter den säkra förbindelsen mellan sändare och mottagare, samt att det kan kränka den personliga integriteten.

9.8 Dynamiska filter

Dynamiska filter är skyddsåtgärder som genomför mer avancerade analyser än statiska filter för att upptäcka och eventuellt stoppa hot. En betydande skillnad mot statiska filter är att de dynamiska filtren ständigt uppdaterar sina indata. Dynamiska filter finns i följande kategorier.

[47] File Transfer Protocol, ett protokoll som används för filöverföring.

9.8.1 Innehållsfilter

Ett innehållsfilter är en skyddsåtgärd som baserat på innehåll och viss indata gör en bedömning av trafik för att avgöra om det skall tillåtas eller ej. Exempel på indata kan vara trafiktyp, innehåll, motpartens trovärdighet, adress, tidpunkt, intern användare och källa.

Leverantörerna av innehållsbaserade filter har byggt upp omfattande nätverk för insamling och analys av nya hot. Denna information skickas sedan till kundernas skyddsåtgärder med filtreringsunderlag. Exempel på sådana nätverk är Websense Threatseeker network[48], Cisco Senderbase[49] och McAfee GTI[50].

De automatiska analyser som sker i leverantörernas nätverk kan i vissa fall även ske i realtid hos kunden.

9.8.2 IDS och IPS

IDS (Intrusion Detection System) och IPS (Intrusion Prevention System) är skyddsåtgärder som bedömer trafikmönstret för att avgöra huruvida trafiken skall tillåtas eller ej. Bedömningen kan ske enligt två metoder. Den första är en analys mot kända mönster eller signaturer av sådana händelser som kan tänkas få negativa följder för IT-systemet. Den andra strategin bygger på att analysera och hitta avvikelser i jämförelse med kända användningsprofiler av IT-systemet.[51]

Kontrollen av kända mönster sker genom att leverantören av skyddsåtgärden tillhandahåller signaturer som den egna trafiken kan jämföras med. Kontrollen av avvikelser sker genom att skyddsåtgärden jämför trafiken med generella regelverk som definierar normal användning för den aktuella installationen. Regelverket kan definieras statiskt eller dynamiskt.

Skillnaden mellan IDS och IPS är att den förstnämnde endast kontrollerar och rapporterar medan den senare även kan vidta automatiska åtgärder. De aktuella åtgärderna kan vara att larma, begränsa eller stoppa trafiken alternativt en kombination av dessa.

9.9 Skyddsåtgärder mot dataläckage

Skyddsåtgärder mot dataläckage eller DLP[52] skall förhindra att uppgifter hamnar hos obehöriga personer genom att stoppa medvetna och omedvetna informationsläckage. Det kan till exempel vara bifogade filer i e-post, filöverföringar, inklistringar eller utskrifter.

---

[48] Websense White Paper, The Websense ThreatSeeker Network, 2008
[49] IronPort Web Reputation: Protect and Defend Against URL-Based Threats, 2008
[50] McAfee White Paper, Reputation: The Foundation Of Effective Threat, 2010
[51] H Säk IT, 2006, sidan 149
[52] Eng. Data Loss Prevention eller Data Leakage Protection.

För att skyddsåtgärderna skall fungera krävs först en identifieringsprocess för att hitta vilken information som skall skyddas. Denna process varierar mellan olika leverantörer men kan exempelvis upptäcka särskilda märkningar eller kombinationer av mönster.

DLP skall skydda informationen under hela livscykeln, vilket omfattar data under användning, data i rörelse och data i vila.[53]

Följande indelning kan vara lämplig för att hantera dessa skyddsåtgärder.

Enhetsbaserad DLP: Denna skyddsåtgärd kontrollerar data under användning genom att kontrollera vilka system- och resursanrop som sker under exekveringen. En användare kan därmed förhindras från att skicka, skriva ut eller kopiera information.

Nätverksbaserad DLP: Datafilter används för att kontrollera data i rörelse, med utgångspunkt från informationsinnehåll. Känslig information kastas på samma sätt som otillåten trafik i ett statiskt filter. En alternativ hantering är att den känsliga informationen rensas bort ur flödet. Exempel på transportsätt kan vara traditionell e-post, webbaserad e-post, direktmeddelanden, sociala medier eller filöverföringar.

Informationsbaserad DLP: Denna skyddsåtgärd används för att identifiera och skydda data i vila, framförallt genom kryptering. Informationsbaserad DLP omfattar genomsökningsfunktioner som skannar nätverkets värdar för att upptäcka information som lagras på ett otillåtet sätt. Lagringen kan omfatta databaser, filsystem, ritningar eller dokument. Informationsbaserad DLP kan även skydda data i rörelse.

9.10 Utbildning

Användarnas kunskap om hot, sårbarheter och risker utgör i många fall den mest avgörande faktorn i säkerhetsarbetet[54]. Det är därför viktigt att ständigt underhålla och fortlöpande uppdatera denna genom relevant information och utbildning till all personal med tillgång till Internet.

[53] Eng. data-in-use, data-in-motion, data-at-rest. (New Technology Prevents Data Leakage, George Lawton, 2008)
[54] Sophos Security threat report 2011

10 Analys

I det här kapitlet värderas de tidigare föreslagna arkitekturerna gentemot de önskemål på funktionalitet som ställts av Försvarsmakten. De arkitekturer som uppfyller funktionaliteten värderas därefter säkerhetsmässigt gentemot de sårbarheter som presenterats i rapporten.

10.1 Terminologi

Inom området informationssäkerhet finns en stor uppsättning begrepp vilka bitvis har överlappande betydelser. Bild 8 beskriver hur de termer och funktioner som används i denna rapport förhåller sig till varandra.

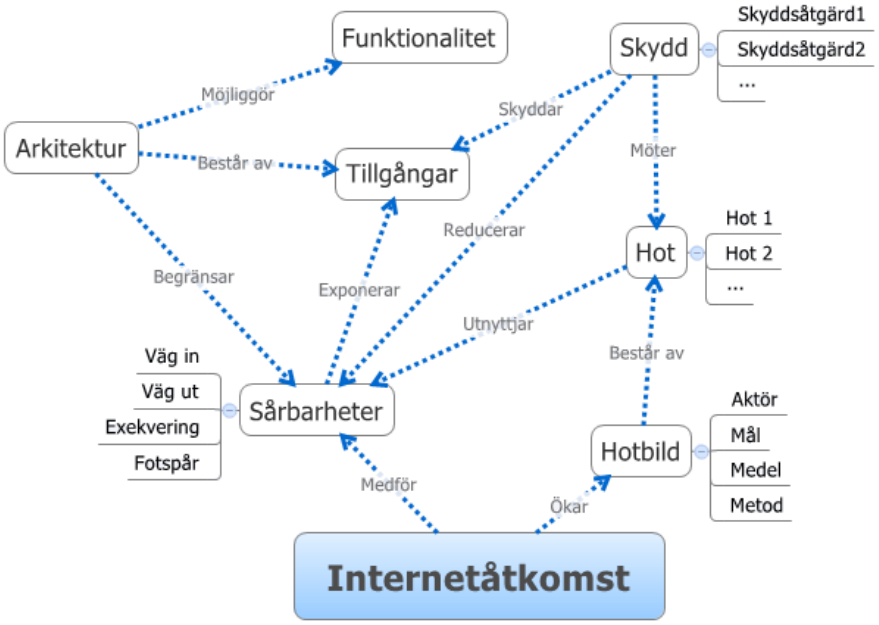


Bild 8, Förhållande terminologi

10.2 Hantering av sårbarheter

All anslutning av interna datanät mot Internet medför att interna IT-system och informationstillgångar exponeras för internetrelaterade hot. Exempel på sådana är internt initierade informationsläckage samt externt initierade intrång.

Anledningen till exponeringen är de internetrelaterade sårbarheter som uppstår i och med anslutningen.

Det är viktigt att poängtera att internetåtkomst inte kan likställas med att det interna datanätet blir allmänt åtkomligt. Det finns idag arkitekturer och skydds-åtgärder som kan användas för att begränsa eller förhindra oönskad åtkomst.

Arkitekturen kan i första hand helt eller delvis begränsa en sårbarhet medan skyddsåtgärden verkar genom att reducera sårbarheten. Arkitekturen kan med andra ord användas för att eliminera en sårbarhet och bör därför vara den primära metoden för att hantera exponeringen. Skyddsåtgärden används sedan där arkitekturen inte räcker till.

Om en angripare lyckas tillförskansa sig direkt kontroll över en dator ansluten till det interna datanätet kan de internetrelaterade sårbarheterna appliceras från en ny position. Sårbarheterna kan med andra ord vara iterativa och det blir relevant att beakta sekundär exponering, det vill säga den exponering som uppstår om en angripare får kontroll över interna datorer.

Den sekundära exponeringen kan betraktas med utgångspunkt från hur ett övertagande angrepp sker. Det första steget kan vara att föra in någon form av skadlig kod på datorn. Detta kan till exempel ske via USB-minnen, cd-skivor eller via den internetrelaterade sårbarheten *väg in*. För att en angripare skall kunna kontrollera och utveckla sitt angrepp bör denne kunna kommunicera med den angripna datorn i realtid. Denna kontrollkanal är endast möjligt att åstadkomma via den internetrelaterade sårbarheten *väg ut* genom att tunnla trafiken via en dold kanal. Om det inte är möjligt att upprätta den dolda kanalen är det heller inte möjligt för angriparen att kontrollera angreppet.

Den sekundära exponeringen kan med andra ord hanteras genom att isolera sårbarheten väg ut från Försvarsmaktens interna IT-system och informations-tillgångar. Samtidigt vill Försvarsmakten förbättra internetåtkomsten från FM AP som skall ha åtkomst till interna tillgångar.

Nyckeln till problemet ligger i att betrakta hur trafikmönster i angriparens kontrollkanal förhåller sig till internetåtkomstens trafikmönster. Skulle internet-åtkomsten ske via en direktansluten arkitektur som har tillgång till de interna tillgångarna är det endast möjligt att stoppa den dolda kanalen med skydds-åtgärder. Men genom att använda indirekta arkitekturer för att tillhandahålla den utökade funktionaliteten kan kommunikationsbehovet mellan FM AP och Internet begränsas. Således är det möjligt att begränsa konsekvenserna av den sekundära exponeringen genom att skilja på exekveringen av internetbaserad kod från åtkomsten till de interna tillgångarna.

10.3 Hotbild

Försvarsmakten fastslår själv att det största enskilda hotet utgörs av dator-nätverksoperationer utförda av främmande makt[55]. Det går dock inte att bortse från asymmetriska datanätverksoperationer och spontana angrepp, då dessa kan innehålla en högre grad av fanatism eller slumpmässighet.

Hotet från en oavsiktlig händelse kan till viss del hanteras genom att erbjuda de funktioner en användare efterfrågar på ett kontrollerat sätt. På så vis elimineras en motiverande faktor för en handling som kan leda till oavsiktliga händelser. Det är också viktigt att genom intern segmentering och behörighetshantering begränsa de eventuella konsekvenserna av en oavsiktlig händelse.

10.4 Arkitekturer

Den arkitektur som väljs skall leverera önskad funktionalitet med så liten exponering av information och IT-system som möjligt. På så vis försvåras ett eventuellt angrepp och det blir färre hot att hantera med skyddsåtgärder.

Vid den säkerhetsmässiga värderingen av arkitekturerna förutsätts att trafik till och från SK-miljön endast kan ske på det sätt som arkitekturen beskriver.

10.4.1 Sammanställning av funktioner

För att kunna värdera respektive arkitektur måste en analys av dess bedömda funktioner genomföras. Det kan bli aktuellt att kombinera flera arkitekturer för att uppnå en önskvärd funktionalitet.

Tabell 5 visar en komparativ studie över hur väl respektive arkitektur uppfyller den funktionalitet som Försvarsmakten efterfrågar.

Tabell 5, Sammanställning arkitektur - funktion

Arkitektur /Funktion	Direktansluten	Virtuell	Sandlåda	Terminalserver	Ombudsserver	
					Filsluss	Innehåll
Surf	U	U	U	U	S	S
Ljud	U	U	U	U	S	S
Video	U	U	U	U	S	S
Skicka filer	U	B	B	U	U	S
Hämta filer	U	B	B	U	U	S

[55] MUST Årsrapport säkerhetstjänst, 2009

Videokonferens	U	U	O	U	S	S
Direktmeddelanden	U	U	O	O	S	S
RSS	U	U	U	U	S	U
Följa länkar	U	S	U	U	S	S
Klipp/klistra	U	B	U	U	S	S
Egna favoriter	U	U	B	U	S	S
Insticksmoduler	U	U	B	B	S	S
Applikationer	U	B-	O	B-	U-	U-
Användbarhet	U	B	B	U	B	U

S = Saknad: Funktionen saknas eller bedöms kraftigt begränsad.

B = Begränsad: Funktionen finns men med vissa begränsningar.

U = Uppfylld: Funktionen bedöms helt uppfylld.

O = Osäker: Funktionens status är okänd.

Den direktanslutna arkitekturen uppfyller samtliga funktionsönskemål. Detta är ett naturligt resultat av att alla IT-baserade system ytterst är avsedda att fungera på en direktansluten klient.

Arkitekturen med den virtuella datorn förutsätts inte ha någon möjlighet till kommunikation med Försvarsmaktens interna tillgångar. Förmågan att skicka och ta emot filer, samt klippa och klistra information blir därför begränsad. Möjligheten att följa länkar i e-post, dokument och på intranät stöds inte med den virtuella datorn. Applikationsstödet bedöms begränsad eftersom applikationerna på den virtuella datorn inte får ha åtkomst till interna IT-system eller informationstillgångar. Användbarheten bedöms begränsad eftersom användaren tvingas växla mellan två datorer.

Sandlådearkitekturen har samma villkor för filåtkomst som den virtuella datorn, vilket medför begränsad funktionalitet för filöverföring. Insticksmoduler och favoriter begränsas eftersom det krävs en särskild hantering för att dessa skall behållas mellan sessioner. Användbarheten begränsas av att isoleringen i vissa fall inverkar på möjligheten att överföra eller behålla information mellan Internet och FM AP. Det finns en osäkerhet kring hur sandlådearkitekturen hanterar externa enheter vilket påverkar videokonferens och direktmeddelanden. Det är inte heller fullt utrett huruvida sandlådearkitekturen kan hantera alla applikationer.

Terminalserverarkitekturen bedöms uppfylla de användarorienterade funktionerna med vissa oklarheter kring direktmeddelanden. Det finns tillgängliga COTS-system för direktmeddelanden som stödjer en terminal-

serverarkitektur men det är oklart om samtliga kända terminalserverarkitekturer stöds. Terminalserverarkitekturen har också vissa begränsningar med insticks-moduler och applikationer eftersom dessa måste installeras på terminalservern. Generellt använda applikationer kan installeras men användarunika applikationer bör undvikas. Om applikationer som exekveras på terminalservern behöver åtkomst till IT-system eller informationstillgångar i SK-miljön ökar exponeringen eftersom isoleringen förloras.

Ombudsarkitekturen är fokuserad på applikationer och är därför inte intressant ur ett användarperspektiv. Filslussen hanterar in och utförsel av filer och kräver en aktiv insats av användaren innan filöverföringen kan slutföras vilket påverkar användbarheten negativt. Innehållsservern mellanlagrar data som kan utnyttjas av olika applikationer och måste anpassas för respektive lösning. När det är igång kommer användaren inte märka någon skillnad mellan ombudsarkitekturen och att gå direkt till en källa på Internet. Det kommer med stor sannolikhet att finnas applikationer och flöden som inte stöds av en ombudsarkitektur.

10.4.2 Sammanställning av sårbarheter

Tabell 6 visar hur respektive arkitektur exponerar Försvarsmaktens IT-system och informationstillgångar för de internetrelaterade sårbarheterna. Ju närmare tillgångarna exekveringen sker, desto högre blir exponeringen.

Tabell 6, Sammanställning arkitektur - sårbarhet

Arkitektur /Sårbarhet	Direktansluten	Virtuell	Sandlåda	Terminalserver	Ombud
Fotspår	**D**	**D**	**D**	**D**	**D**
Väg in	**D**	**I**	**I**	**S**	**S**
Exekvering	**D**	**I**	**I**	**S**	**D**
Väg ut	**D**	**I**	**I**	**S**	**S**

D = Direkt exponerad: Arkitekturen innebär att den interna miljön är direkt exponerad.

I = Indirekt exponerad: Arkitekturen innebär att den interna miljön är delvis eller indirekt exponerad.

S = Skyddad: Arkitekturen skyddar den interna miljön.

Den direktanslutna arkitekturen är direkt utsatt för samtliga internetrelaterade sårbarheter eftersom internetåtkomsten sker från FM AP.

Den virtuella datorn innebär att internetåtkomsten hanteras i FM AP men att all exekvering av internetbaserad kod isoleras mjukvarumässigt. Därmed erhålls en indirekt utsatthet av Försvarsmaktens IT-system och informationstillgångar

enligt tabell. Graden av utsatthet bedöms något lägre än för en sandlåde-arkitekturen eftersom operativsystem och viss hårdvara är helt separerade. Samtidigt innebär förekomsten av det egna operativsystemet och de egna applikationerna en viss sårbarhet i sig.

Sandlådeapplikationen medför att kommunikationen från Internet hanteras av en mjukvara på FM AP vilket medför en indirekt utsatthet enligt tabell. Graden av utsatthet bedöms vara något högre än för arkitekturen med virtuell dator.

Terminalserverarkitekturen innebär att Försvarsmaktens IT-system och informationstillgångar är skyddad från väg in, exekvering och väg ut eftersom trafiken från Internet stannar i en annan säkerhetsdomän. Det är också möjligt att förstärka skyddet av själva terminalservern eftersom användaren inte behöver samma funktioner eller behörigheter som på en arbetsstation.

Ombudsarkitekturen skyddar SK-miljön från väg in och väg ut men är utsatt för exekvering eftersom all data som hämtats från Internet till slut exekveras på FM AP.

10.4.3 Distansarbete

För att användare inom Försvarsmakten skall uppleva en så homogen arbetsmiljö som möjligt bör även distansarbetsförmågan stödjas av arkitekturen. För att FM AP skall kunna användas som distansplattform bör den ha samma skydd som när den är ansluten till Försvarsmaktens fasta nät. Det innebär att skyddsfunktioner utanför FM AP-plattformen, men som är ett resultat av arkitekturen, måste gå att använda i en distanslösning.

10.5 Skydd

Moderna skyddsåtgärder har utvecklats till en nivå där de näst intill kan liknas vid arkitektoniska skydd. Ett datanät utan aktivitet är mycket svårt att få obehörig åtkomst till. Konsekvensen av denna utveckling är att de internetrelaterade hoten i allt högre grad inriktar sig på att lura användaren genom att fokusera på innehåll snarare än trafik och tjänster. Detta innebär att de trafikmässigt ser ut som godkänd trafik vilket kringgår de skyddsåtgärder som endast analyserar grundläggande egenskaper, såsom statiska filter. För att bemöta de innehållsbaserade hoten behövs skyddsåtgärder som utför mer komplexa analyser med fokus på trafikens innehåll, såsom dynamiska filter och DLP-lösningar.

Skyddsåtgärder har olika möjligheter beroende på var de finns. Ett statiskt filter på en dator kan till exempel utnyttja andra parametrar än ett statiskt filter i nätverket. Skyddet bör byggas upp genom att kombinera skyddsåtgärder på flera nivåer i SK-miljön. Skyddet mot intrång kan till exempel inkludera statiska filter på både klienter, servrar och nätverksutrustning.

Det behövs en konceptuell modell för att underlätta beskrivning av en skydds-åtgärd. Den modell som används i H Säk IT (2006) och KSF version 2 omfattar inte alla skyddsåtgärder varför en annan modell behövs. I denna rapport används en modell (bild 9) som kombinerar var skyddsåtgärden finns med var den utförs.

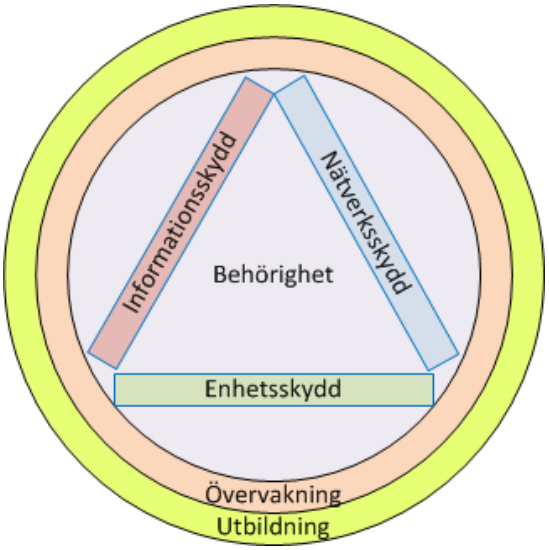


Bild 9, Indelning av skyddsåtgärder

Enhetsskydd:[56] Detta skydd fokuserar på data under användning genom skyddsåtgärder som sker på en dator. Det kan exempelvis vara ett signaturbaserat virusskydd eller ett statiskt filter. Enhetsskyddets primära funktion är att skydda ett IT-system mot exekvering men det kan även hantera övriga sårbarheter.

Enhetsskyddet har möjlighet att kombinera program, filtyper och flöden. Ett exempel kan vara att avgöra vilka program som får kommunicera med nätverket och med Internet.

Nätverksskydd: Skydd som omfattar data i rörelse samt de skyddsåtgärder som sker på utrustning i nätverket, till exempel statiska eller dynamiska filter kallas för nätverksskydd. Dess primära funktioner är att hantera sårbarheterna väg in och väg ut genom att kontrollera vem som får prata med vem.

[56] Eng. Endpoint protection

Nätverksskyddet har möjlighet att kontrollera flöden i nätverket och kan stoppa ett hot innan det når sin destination. Det är också möjligt att hantera sårbarheter på ett gemensamt och resurseffektivt sätt. Ett exempel är ett dynamiskt filter som annars skulle kräva en stor definitionsfil på varje dator i nätverket. En annan egenskap är att nätverksskyddet kan upptäcka angrepp baserat på avvikelser i trafikmönster.

Nätverksskyddet kan även omfatta kryptering av data i rörelse för att skydda mot avlyssning.

Informationsskydd: Dessa skyddsåtgärder fokuserar på data i vila samt de skyddsåtgärder som förhindrar informationsläckage. Det kan till exempel vara filbunden kryptering eller lagringsinventerande DLP-lösningar.

Informationsskyddet har möjligheten att följa med och skydda data oberoende av aktivitet.

10.5.1 Behörighet

Behörighet eller BKS omfattar ett systemövergripande lager som kan utnyttjas av alla skyddsåtgärder. BKS avgör vem eller vad som har behörighet till IT-system och informationstillgångar. Ett gemensamt system för BKS underlättar spårbarhet och förbättrar användarupplevelsen genom att en användare alltid har samma identitet. Nackdelen med ett gemensamt BKS är att det ökar hotet mot systemet eftersom det utgör en nyckel till all åtkomst.

10.5.2 Övervakning

Övervakning är ett systemövergripande lager som omfattar skyddsåtgärderna säkerhetsloggning och övervakning av skyddsåtgärder. Övervakning gör det möjligt att upptäcka, spåra samt hantera eventuella angrepp på ett effektivt sätt och kan vara direkt avgörande för hur omfattande skada en händelse medför.

10.5.3 Utbildning

Utbildning är en icke systembunden skyddsåtgärd och utgör en mycket viktig faktor i säkerhetsarbetet[57]. Det är därför viktigt att ständigt underhålla och fortlöpande uppdatera denna genom relevant information och utbildning.

Oavsett om Försvarsmakten väljer att erbjuda en internetåtkomst med utökad funktionalitet eller ej så använder Försvarsmaktens personal Internet privat. I och med hotet från datanätverksoperationer utförd av främmande makt bör en fortlöpande kompetenshöjande insats om hotbilden genomföras.

[57] Websense 2010 Threat Report

10.6 Sammanställning skyddsåtgärder – hot

I tabellen nedan (Tabell 7) sammanställs de skyddsåtgärder vilka presenterades i kapitel 9 med de hot vilka presenterades i kapitel 8. Tabellen visar var i ett system en skyddsåtgärd kan hantera ett visst hot.

Tabell 7, Sammanställning hot - sårbarhet

Hot/Skyddsåtgärd	Skadlig kod - Signaturer	Skadlig kod - Heuristik	Skadlig kod - Applikation	Skadlig kod - Rykte	Statistiska filter	Sessionskontroll - SPI	Addressöversättning	Dekryptering av flöden	Innehållsfilter	IDS och IPS	Enhetsbaserad DLP	Nätverksbaserad DLP	Informationsbaserad DLP	Utbildning
Digitalt fotspår:														
Sondering	-	N,E	N,E	-	N,E	N	N	-	-	N	-	-	-	
Avlyssning	-	-	E	-	E	-	-	-	-	-	E	N	-	
Öppen information	-	-	-	-	-	-	-	-	-	-	-	-	-	U
Väg in:														
Bakdörr	N,E	N,E	N,E	E	E	-	-	N	N	N,E	E	-	-	
Farmning	-	-	-	-	-	-	-	-	N	-	-	-	-	
Spoofing	-	-	-	-	N	N	-	N	N	N	-	-	-	
Webbaserad aktiv kod	N,E	N,E	-	-	-	-	-	N	N	N	-	-	-	
Användaranpassad webb	N,E	N,E	-	-	-	-	-	N	N	N,E	E	-	-	
Internetanslutna applikationer	N,E	N,E	-	N,E	-	-	-	N	N	-	E	-	-	
Social manipulering	N,E	N,E	N,E	N,E	N,E	N,E	-	N	N	N	-	-	-	U
Filöverföring	N,E	N,E	N,E	N,E	N,E	-	N	N	N	N	E	-	-	
Exekvering:														
Känd skadlig kod	N,E	-	-	-	N,E	-	-	N	N	N	E	-	-	
Okänd skadlig kod														
Angreppsvektor	-	N,E	N,E	N,E	N,E	N,E	N	N	-	N	-	-	-	
Maskering	-	N,E	N,E	N,E	E	-	-	N	-	N	-	-	-	
Oönskade instruktioner	-	N,E	N,E	N,E	E	-	-	N	-	N	E	-	I	
Väg ut:														
Informationsläckage	-	N,E	N,E	N,E	-	-	N	N	N	-	E	N	I	
Dold kanal	-	N,E	N,E	-	-	-	-	N	N	N	-	-	-	
Filöverföring	-	N,E	N,E	-	N,E	-	-	N	N	N	E	N	-	
Datadropp	-	-	-	-	-	-	-	N	N	N	E	N	-	

E = Enhetsskydd, N = Nätverksskydd, I = Informationsskydd

Skyddsåtgärder för behörighetskontroll och övervakning är applicerbara på samtliga hot och utgör ett stöd för övriga skyddsåtgärder. I och med att de ingår överallt är dessa inte med i tabell 7.

Hotet med informationssammanställning av öppen information på Internet kan inte hanteras genom arkitektur eller tekniska skyddsåtgärder. Detta hot måste istället hanteras genom att utbilda personalen i konsekvenserna med att publicera information på Internet.

Informationsläckage är ett hot som kan delas upp i medvetet och omedvetet läckage. Det omedvetna läckaget går att hantera med arkitektur och skydds-åtgärder men det medvetna läckaget är svårare. Anledningen till detta är att det medvetna läckaget oftast utförs av en behörig person och i och med att behörigheten finns hjälper inga skyddsåtgärder. Dagens DLP-system kan i princip endast användas för att försvåra men inte omöjliggöra medvetna informationsläckage.

Utbildning av personalen har inte illustrerats som en generell skyddsåtgärd i ovanstående tabell. Säkerhetsmedveten personal är dock även fortsatt ett av de absolut bästa skyddsåtgärderna varför kontinuerlig utbildning är nödvändig.

11 Slutsatser

Arkitekturen har en större och mer beständig påverkan på exponeringen av interna system än vad skydd och skyddsåtgärder har. Därför kan en bra arkitektur minska exponeringen genom att separera exekveringen av internetbaserad kod och åtkomst till SK-miljöns IT-system och informationstillgångar. Genom att välja en sådan arkitektur och komplettera denna med relevanta skyddsåtgärder är det möjligt att skapa en funktionsmässigt adekvat internetåtkomst med en låg exponering.

Information som publiceras på Internet medför att det kommer att finnas ett digitalt fotspår som alla kan följa. Detta fotspår kan utnyttjas som en informationskälla i sig eller som förberedelse inför ett angrepp. Det finns inga tekniska skyddsåtgärder som idag kan hantera problemet utan det enda motmedlet är utbildning. Problemet med ett digitalt fotspår finns redan idag och påverkas endast delvis av om Försvarsmakten erbjuder en internetanslutning.

Skyddsåtgärder får olika effekt beroende på var i IT-miljön de finns. Därför behövs en modell som beskriver både åtgärd och placering för att beskriva skyddet.

11.1 Föreslagen lösning

Terminalserverarkitekturen och ombudsarkitekturen kan tillsammans erbjuda en utökade funktionalitet som Försvarsmakten efterfrågar. Den funktionalitet som Försvarsmakten efterfrågar kan förvisso uppnås med andra arkitekturer men det sker till priset av en högre exponering. Den direktansluta arkitekturen erbjuder mest funktionalitet men skulle innebära en hög exponering. Alternativen med virtuell dator eller sandlådeapplikationer erbjuder inte den efterfrågade funktionaliteten och skulle innebära en medelhög exponering.

Bild 10 visar hur en kombination av terminalserverarkitekturen med fokus på användarna och ombudsarkitekturen med fokus på applikationer kan se ut. I denna åtskiljs exekveringen av internetbaserad kod från SK-miljön. SK-miljöns IT-system och informationstillgångar placeras dessutom ytterligare en säkerhets-domän bort från exekveringen vilket försvårar angrepp.

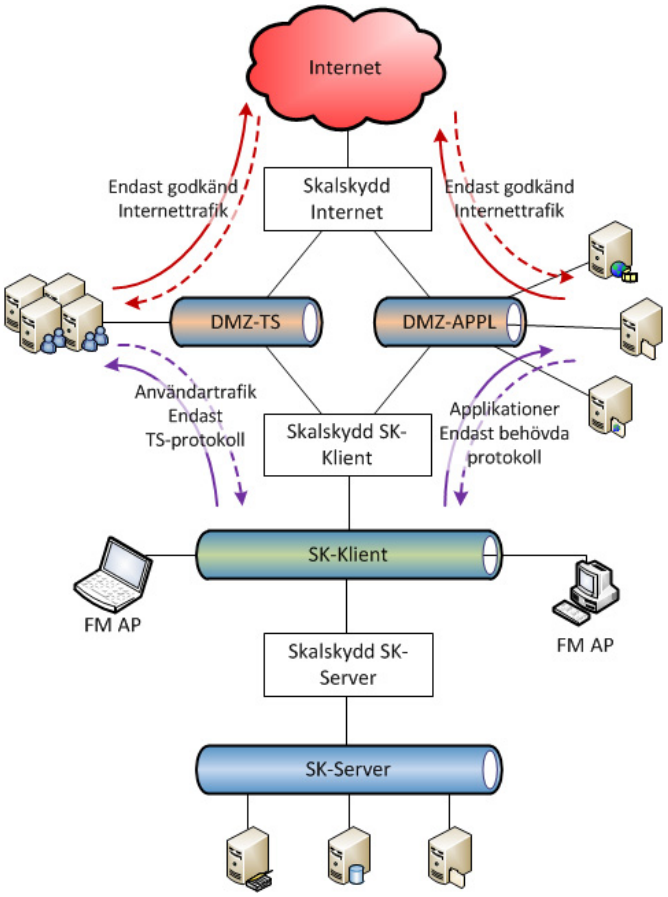


Bild 10, Lösningsförslag

I lösningsförslaget ovan representerar SK-Server, SK-Klient, DMZ-TS, samt DMZ-APPL egna säkerhetsdomäner som åtskiljs av relevanta skyddsåtgärder. De skyddsåtgärder som placeras som nätverksskydd enligt tabell 7 sker antingen i rutorna ”Skalskydd” eller i annan nätverksutrustning. De skyddsåtgärder som placeras som enhetsskydd enligt samma tabell sker på datorerna.

11.2 Distansarbete

Bild 11 visar hur en internetåtkomst kan se ut för distansarbete med FM AP. I princip är det samma arkitektur som används inom Försvarsmaktens lokaler men med skillnaden att FM AP ansluts via en krypterad tunnel över Internet.

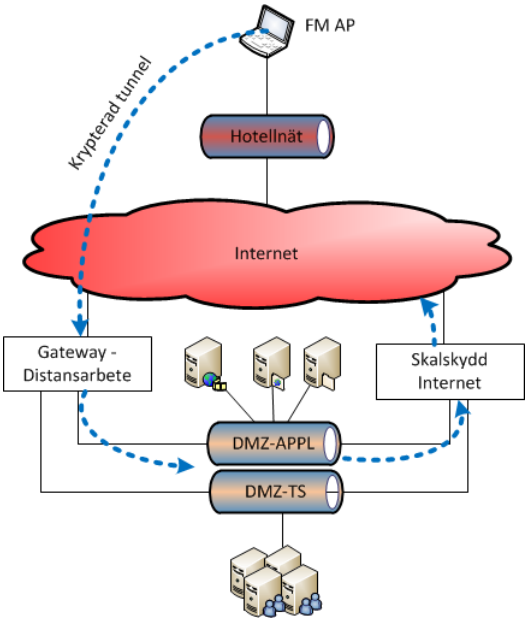


Bild 11, Distansarbete

Denna lösning förutsätter att FM AP utrustas med skyddsåtgärder för att förhindra trafik utanför tunneln. I så fall förblir exponeringen av FM AP mot Internet likvärdig både inom och utanför Försvarsmaktens lokaler.

12 Källförteckning

Handbok för Försvarsmaktens säkerhetsskyddstjänst – Informationsteknik, H SÄK IT, 2006 - (10 440:66817)

Handbok för Försvarsmaktens säkerhetstjänst, Sekretessbedömning Del A, H Säk SekrBed A, 2011 - (10 440:50074)

Krav på säkerhetsfunktioner - grunder, KSF, version 2.0 - (10 750: 78976)

Handbok för Försvarsmaktens Säkerhetstjänst Informationsteknik Hotbeskrivning, H Säk IT-hot, 2001 - (10750:62687)

SIS HB 550, Utgåva 3. Terminologi för informationssäkerhet, 2007

Årsrapport säkerhetstjänst 2009, MUST

Symantec Internet Security Threat Report, Trends for 2010 Volume 16, publicerad April 2011.

Websense 2010 Threat Report, Jon Crotty

Försvarsmaktens gemensamma riskhanteringsmodell (M7739-350012 / 01 310:900666)

Terminologi för informationssäkerhet, SIS HB 550, Utgåva 3, 2007 – (ISBN 978-91-7162-705-6)

Joint Publication 1-02 Dictionary of Military and Associated Terms. Department of Defence, 8 november 2010.

SANS institute Data Loss Prevention, Prathaben Kanagasingham, 2008

Remissförslag, Direktiv om Försvarsmaktens hantering av sociala medier, 2011

Försvarsmaktens föreskrifter om säkerhetsskydd, FFS 2003:7, ISSN 0347-7576

McAfee White Paper, Reputation: The Foundation Of Effective Threat Protection, Jamie Barnett, 2010

McAfee Threats Report: Fourth Quarter 2010, McAfee Labs

McAfee Threats Report: First Quarter 2011, McAfee Labs

IronPort Web Reputation: Protect and Defend Against URL-Based Threats, 2008

Websense White Paper, The Websense ThreatSeeker Network: Leveraging Websense HoneyGrid Computing, 2008

New Technology Prevents Data Leakage, George Lawton, 2008

Sophos Security threat report 2011

Cisco 2010 Annual Security Report

13 Begrepp och ackronymer

Begrepp	Definition
Aktör	En enskild mänsklig individ, eller en sammanslutning av människor: en grupp, ett nätverk, en organisation, en stat eller en sammanslutning av flera stater. (FM Riskhanteringsmodell 2009)
Antagonistiska hot	En mänsklig aktörs möjligheter att medvetet förorsaka en oönskad händelse med negativa konsekvenser. (FM Riskhanteringsmodell 2009)
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations, Samlingsnamn på försvar och anfall av IT-system. Omfattar CNA, CND och CNE.
COTS	Commercial off the Shelf, begrepp för kommersiellt tillgängliga standardprodukter.
FM	Försvarsmakten
Hot	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten (ISO/IEC 13335-1:2004)/Försvarsmaktens gemensamma riskhanteringsmodell
Hotbild	En uppsättning hot som bedöms föreligga mot en viss verksamhet (SIS HB 550 – Utgåva 3)
Händelse	Inträffandet av en särskild uppsättning omständigheter. (ISO/IEC Guide 73:2002)/Försvarsmaktens gemensamma riskhanteringsmodell
Konsekvens	Utfallet av en händelse. (ISO/IEC Guide 73:2002)/Försvarsmaktens gemensamma riskhanteringsmodell

Oönskad händelse	Händelse med en eller flera konsekvenser som är negativa för verksamheten. (FM Riskhanterings-modell 2009)
Risk	En kombination av sannolikheten för att en händelse skall inträffa och dess konsekvens. (ISO/IEC Guide 73:2002)/ Försvarsmaktens gemensamma risk-hanteringsmodell 2009
Sannolikhet	Sannolikheten för att en händelse inträffar. (ISO/IEC Guide 73:2002)/Försvarsmaktens gemensamma riskhanteringsmodell 2009
SK	SK är en infrastruktur under uppbyggnad och motsvarar i stort dagens SWEDI samt FM AP-infrastruktur.
Skadlig kod	Otillåten programkod som är till för att ändra, röja, förstöra eller avlyssna ett elektroniskt kommunikationsnät eller funktioner eller uppgifter i ett IT-system. (Försvarsmaktens föreskrifter om säkerhetsskydd, 7 kap. 1 § 9)
Skydd	Handling, rutin eller tekniskt arrangemang som, genom att minska sårbarheten möter ett identifierat hot. (SIS HB 550 – Utgåva 3)
Skyddsåtgärd	Handling, procedurer eller tekniskt arrangemang som, genom att minska sårbarheten möter identifierat hot. (ISO/IEC 13335-1:2004)/Försvarsmaktens gemensamma riskhanteringsmodell
Sårbarhet	Brist i skyddet av en tillgång exponerad för hot. (SIS HB 550 – Utgåva 3)
Tillgång	Allt som är av värde för organisationen. (SIS HB 550 – Utgåva 3)