Digitalt försvar

Krigföringen i cyberspace utvecklas samtidigt som säkerheten inom IT-området. Säkerhet handlar enligt en av FMVs experter om att ha en bra ledning, trovärdig teknisk struktur samt en effektiv drift.

Mats Ohlin är civilingenjör inom kemisk teknologi och har tidigare arbetat inom FOA och Försvarsstaben. 1979 fick han sitt första säkerhetsuppdrag åt dåvarande ÖB/Säk rörande Försvarets Datacentral. Sedan 1989 finns han inom FM och är en slags intern konsult inom information och säkerhet samt företräder FMV internationellt i dessa frågor.

– Intresset har successivt ökat från att mest ha engagerat branscher som telekom, bilindustrin, bankvärlden och kreditkortsföretagen samt hälso- och sjukvården. I dag är det ett samhällsintresse och viktigt eftersom samhället utsätter sig för allt större risker.

– Det är fortfarande ett spännande område som förändras hela tiden. Utmaningen är den ökande komplexiteten. Krigföringen i cyberspace utvecklas hela tiden, säger Mats Ohlin.

Att vara specialist inom området informationssäkerhet handlar om att vara ständigt uppdaterad. Och de tekniska systemen är bara en del.

– Säkerheten vilar så att säga på tre ben. Det handlar om ledningsfunktioner, att ha en trovärdig teknisk struktur samt att ha en effektiv drift och övervakning, säger Mats Ohlin. Arbetet med de internationella säkerhetskraven har sedan 1990-talet skapat en gemenskap över landsgränser som är nödvändig då hoten inte känner några gränser.

– Innan arbetet började var det delvis helt olika tänk i till exempel Nordamerika och Europa, säger Mats Ohlin.

Samtidigt som systemen blivit allt säkrare är den mänskliga faktorn ett problem:

– Ett klassiskt exempel handlar om angriparen som kollar upp när den IT-ansvarige på ett företag jobbar hemma en helg och är uppkopplat på nätet. Han använder en krypterad förbindelse som angriparen stör. Så ringer de upp, säger att de är från supportavdelningen och undrar om de kan hjälpa till. Självklart svarar förmodligen användaren som är irriterad på störningarna. Angriparen slutar störa och ringer sen upp den tacksamme användaren och ber, som i förbigående, om inloggningskoder eftersom de håller på med en uppdatering, berättar Mats Ohlin.

Angriparna börjar alltså med att skapa ett beroendeförhållande till offret. Detta ingår i vad som kallas social engineering, något som utnyttjas i samband med senare tids omfattande bedrägeriförsök mot enskilda personers internetbankkonton via så kalla nätfiske (se faktaruta). Samtidigt får inte säkerhetssystemen bli för komplicerade – då blir de paradoxalt nog en säkerhetsrisk i sig själva. Det är också viktigt att skapa förtroende för att säkerheten fungerar.

Det var i början av 1990-talet som EU och USA förhandlade fram en lista på strategiskt viktiga utvecklingsfrågor inom IT vilket bland annat innehöll gemensamma internationella säkerhetskriterier. De så kallade Common Criteria är idag kopplade till ISO/IEC och certifieringsarbetet.

Mats Ohlin leder en av undergrupperna inom detta projekt, inom ISO, att ta fram säkerhetsstandarder.

– Det är viktigt med tydliga krav och FMV har en bra erfarenhet kring detta från alla upphandlingar. Certifieringen ska vara lika i alla länder. Idag handlar detta arbete dels om hur vi uttrycker kraven i säkerhetsfunktioner, till exempel vid inloggning, dels kraven på granskningsåtgärder. Det sistnämnda finns idag på sju olika nivåer. Där man kommit längst är de så kallade smartkorten. Deras chip måste göras mycket svåra att manipulera.

Ett problem i arbetet är den snabba teknikutvecklingen. Det kan ibland ta upp till ett år att certifiera ett komplext system och under tiden lanseras ofta en ny version av produkten.

– Kanske ska vi istället börja granska leverantören tidigare än produkten. På det sättet kan vi bättre stimulera leverantören att skapa säkrare produkter och marknaden att ställa högre krav, säger Mats Ohlin.

FAKTA

Mats Ohlin utsedd till ordförande för CCRA Management Committee. Kommittén är det högsta beslutande organet inom Common Criteria Recognition Arrangement,CCRA.
CCRA består av 25 länder och arbetar med ömsesidigt erkännande av certifikat för IT-säkerhet i produkter och system enligt standarden Common Criteria. CCRA arbetar också i samarbete med ISO.

I Sverige är ansvaret för CCRA-samarbetet delat mellan Krisberedskapsmyndigheten, KBM, och FMV.
FMVs CSEC är certifieringsorgan för säkerhet i IT-produkter och system inom ramen för den internationella CCRA-överenskommelsen.

Nätfiske, hämtat från engelskans phishing, är en olaglig metod att komma över känslig information som till exempel ditt kreditkortsnummer, lösenord och andra inloggningsuppgifter.

Mats Ohlin

David Olgart

FOTO: ISABELLE ÅLANDER/FMV

Boktips
"Beyond fear" av Bruce Schneier. En läsvärd bok som inte är teknisk men som resonerar bra kring bland annat säkerhet och ekonomi, enligt Mats Ohlin.

Utbildning viktig säkerhetsfråga

Internt har FMV en gemensam teknisk plattform för den normala datorarbetsplatsen. Det är en viktig förutsättning för överblick och gäller för både fasta och bärbara lösningar i SFAP-konceptet, vilket står för Säker FMV-arbetsplats.

– Det här betyder att vi erbjuder en standardiserad lösning för alla behov. Vi slipper en flora av olika datorer, system och program, säger David Olgart.

Han är FMVs informationssäkerhetschef. Tidigare arbetade David Olgart som sjöofficer men läste sedan till mariningenjör på KTH. Innan han började på FMV tjänstgjorde han vid den Militära säkerhetstjänsten i Försvarsmaktens högkvarter.

Alla inom FMV får en grundbehörighet men därefter får varje enskild individ tala om vad han eller hon behöver i sitt jobb.

– Många gånger utgår man från vad användaren vill ha men vi har så att säga vänt på det. Vi förser användarna med vad de behöver i arbetet. Alla har inte automatiskt behörighet till allt.

– Det finns förstås speciallösningar, utöver SFAP för de som har behov av att jobba med exempelvis hemliga uppgifter.

Riskbedömning är något som måste göras varje dag. Ett ämne som blir allt mer aktuellt med tanke på den snabba tekniska utvecklingen.

– Vi har ständig omvärldsbevakning. Även om en hel del av det praktiska arbetet görs av vår driftleverantör följer vi också med.

Du har haft det här jobbet i två år – hur följer du själv med i utvecklingen?

– Jag gör egna omvärldsanalyser både av eget intresse och för arbetet. Jag använder internet som en källa och följer upp FMVs åtgärder av kända buggar, det vill säga säkerhetshål, som är relevanta för våra system.

Om information om ett nytt hot når David Olgart och hans kollegor gör de snabbt en bedömning om de tekniska systemen kan stå emot det eller om FMV måste vidta ytterligare åtgärder som att till exempel begränsa tillgängligheten till något eller några system.

– Dock är problemen inte de kända hoten utan de okända. De allvarligaste incidenterna upptäcker man oftast i efterhand och då får vi vara "städpatrull"…

– Men vi har ett robust och hållbart skydd även om säkerhet är ett relativt begrepp. 100 procent säkerhet finns inte i praktiken.

Svagaste länken i IT-säkerheten – är det den enskilda individen?

– Nja, jag skulle vilja säga att det handlar om utbildning. Säker informationshantering med hjälp av IT-system kräver idag en hög medvetenhet om hot och motåtgärder. En förutsättning för detta är återkommande utbildning.

Har du något råd kring detta?

– Tekniken är inte allt, den är ett hjälpmedel. Det handlar om regelverk och organisation också. Vi måste kunna lita på att alla följer reglerna, vilket bygger på att vi utbildat. Säkerhet är inte en produkt, det är en kontinuerlig process, säger David Olgart.

TEXT: JANE AF SANDEBERG

FMV SKAPAR SÄKER PLATTFORM

Ett av de verktyg som FMV utvecklat för att säkra Försvarsmaktens systemmiljöer är den så kallade Generell Teknisk Plattform, GTP. En teknisk infrastruktur för nätverks- och tjänstebaserade tillämpningar som ger en säker driftsmiljö.

Plattformen är flexibel och kan användas i systemmiljöer som bygger på operativsystem som Microsoft Windows och UNIX. Centraliserad lagring ger samma miljö och tillgänglighet oavsett från vilken arbetsplats inloggningen sker.

GTP 3.0-1 är färdig att använda och kräver ingen anpassning av nätverk, datorer eller befintlig programvara. GTP tillför säkerhets- och administrationsfunktioner.

GTP består av ett 70-tal säkerhetskonfigurerade komponenter och tillhandhåller tekniska stödkomponenter för till exempel Single Sign-On (SSO) med Försvarsmaktens aktiva kort (TAK2 och TEID).

Via GTP får användaren också e-post, webb och fildelning.

FMV har ansvar för att leverera produkter och system till Försvarsmakten som uppfyller ställda informations och IT-säkerhetskrav. Men ytterst är det Försvarsmakten och dess chefer för olika förband som är ansvariga för säkerheten i de system de använder; där MUST/Säkerhetskontoret har ett särskilt kontroll- och regelverksansvar.