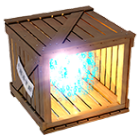
FOI

CRATE
Cyber Range And Training Environment



Nyhetsbrev Informationssäkerhet nr 1, 2024

Välkommen till vårt nyhetsbrev från enheterna Cyberförsvar & Cyberträningscentrum. Vi har försökt samla ihop de utskick vi gör i olika sammanhang från våra enheter till ett gemensamt nyhetsbrev som planeras att komma ut några gånger per år. Vi hoppas att du hittar något intressant att fördjupa dig i här, men skulle du känna att det här var helt fel så finns det en länk längst ner på sidan där du kan avregistrera dig från framtida utskick.
I det här nyhetsbrevet skriver vi om:

- Delat ansvar är ingens ansvar?
- Varför har mjukvaror sårbarheter?
- Digitaliseringens fallgropar i gråzon och krig.
- Unravelling the Myth of Cyberwar.
- Passar jag som är forskarutbildad in på FOI?
- Examensarbete på FOI 2024
- Vi söker nya kollegor!
- IT-incidenthantering i praktiken
- FOI ger stöd till att förbättra Sveriges cyberförsvar, **foi.se/cyber**
- Webbinarium och evenemang
- Välkommen till onlinekurs - Säkerhet i industriella kontrollsystem.
- Självstudieuppgifter - Träna på tekniker och verktyg.
- Rapportsamling - för oss som är speciellt intresserade av Informationssäkerhet.
- Nya kurstillfällen under 2024 i *Elektronisk säkerhet.*

Kontakta oss

Har du frågor om vårt nyhetsbrev - kontakta: Gunilla Friberg

gunilla.friberg@foi.se

Jobba hos oss

Vi söker nya kollegor som brinner för cybersäkerhet och vill bidra till att stärka Sveriges totalförsvar.

Kolla in vår hemsida och se vilka tjänster som finns att söka **Jobba hos oss**

Våra kurser

Elektronisk säkerhet: Följande kurstillfällen är nu öppna för anmälan: **v20 och vecka 40 2024.**

Vi erbjuder även anpassade kurser och utbildningar baserade på vår breda kompetens.

Kurser och utbildningar här finner du kursbeskrivningar och anmälningsformulär till vårt övriga kursutbud.

Delat ansvar är ingens ansvar?

En analys av den svenska statsförvaltningens ansvar och styrning vad gäller svenskt

informations- och cybersäkerhetsarbete

Av: Mattias Svahn, Mathilde Jarlsbo, Miranda Michélsen Forsgren och David Lindahl

Sverige, det svenska samhället och svensk förvaltning genomgår enligt många utredningar och analyser en digital transformation. Den påbörjades för ett trettiotal år sedan och accelererar fortfarande. Utvecklingen mot ett digitalt samhälle medför både innovationer och möjligheter likväl sårbarheter och risker. För att bemöta sårbarheterna och riskerna behöver det svenska samhället ett kontinuerligt pågående och väl styrt informations- och cybersäkerhetsarbete och då i synnerhet i statsförvaltningen. Denna rapport utforskar fördelningen av ansvar för och styrning av svenska myndigheters informations- och cybersäkerhetsarbete i det digitala samhället, hur den fördelningen uppstått och om det finns någon problematik relaterat till den fördelning som finns. Rapporten tar sin utgångspunkt i en litteraturgenomgång av forskningslitteratur, utredningar, regleringsbrev, lagtexter och andra offentligrättsliga dokument. Litteraturgenomgången kompletteras med intervjuer med fem centrala aktörer inom svensk cybersäkerhet. Denna studie identifierar tre genomgående tendenser vilka samtliga speglar den svenska statsförvaltningens informations- och cybersäkerhetsarbete. Den första tendensen är otydlig ansvarsfördelning och styrning. Den andra tendensen är oklarheter i diskursens definitioner och den tredje tendensen är bristande återrapportering. Rapportens resultat speglar aktuell samhällsvetenskaplig forskning i sin belysning av de problem kring ansvar för och styrning av cybersäkerhet i statsförvaltningen som studien uppmärksammar. Studien landar i att det finns en problematik med dagens styrning av cybersäkerhetsarbetet inom statsförvaltningen. Studien landar även i en försiktig optimism för kommande EU-harmonisering på området. Rapporten avslutas med en lista med förslag på framtida forskning. Dessa förslag är förankrade i problembilden som denna rapport redogör för.

Läs hela rapporten på foi.se

Varför har mjukvaror sårbarheter?

En förstudie av: Henrik Karlzén, Daniel Eidenskog och Jerry Falkcrona.

Trots årtionden av forskning och utveckling inom mjukvarusäkerhet fortsätter sårbarheter att förekomma i stor mängd. Denna förstudie utgör

en sammanställning av forskning och annan litteratur som undersöker olika typer av orsaker till varför sårbarheter fortfarande är så vanliga. Syftet med studien är att ge stöd i att förstå faktorerna bakom uppkomsten av sårbarheter och därigenom kunna undvika att de uppstår. I princip förekommer mjukvarusårbarheter i all mjukvara och det finns många olika typer av sårbarheter. De bakomliggande orsakerna till att mjukvarusårbarheter uppstår är många och bland dessa finns organisatoriska faktorer, osäkra programmeringsspråk, svåranvända eller otillräckliga verktyg, brister i utvecklingsmetoder, avsaknad av motivation hos utvecklare och bristande säkerhetskompetens. Utmaningen med att förhindra att mjukvarusårbarheter uppstår är således inte enbart en teknisk sådan; även den mänskliga faktorn behöver beaktas. Trots att det finns en ansenlig mängd befintlig forskning som identifierar potentiella orsaker till att mjukvarusårbarheter uppstår fortsätter nya sårbarheter av samma typ att rapporteras. Detta tyder på att det återstår mycket forskning inom sårbarheternas orsaker och uppkomst. Denna studie identifierar ett antal förslag på vidare forskningsområden.
Läs hela rapportern på foi.se

Digitaliseringens fallgropar i gråzon och krig

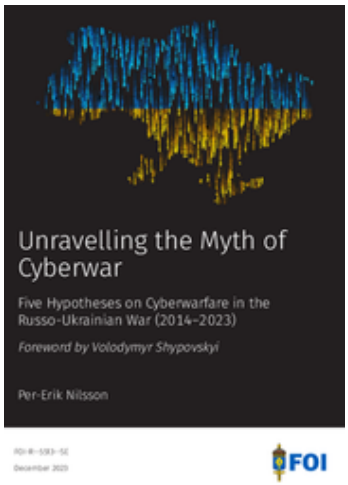
Av Johan Bengtsson, Karin Mossberg Sonnek och Vidar Hedtjärn Swaling

Digitaliseringen inom samhällsviktiga verksamheter har pågått under en längre tid. Syftet har främst varit effektivisering och kostnadsbesparingar, men också att underlätta för anställda inom verksamheterna och för medborgare som tar del av verksamheternas tjänster. Digitaliseringen har många positiva följder, men innebär även utmaningar. Studier och utredningar har visat att exempelvis snabba teknikskiften, omogen teknik, avsaknad av nationell samordning samt bristfällig beställarkompetens gör att sårbarheter byggs in i IT-systemen. Detta är sårbarheter som kan utnyttjas av antagonister i en gråzon eller under ett krig för att förstöra IT-systemen, manipulera data eller sprida desinformation. I denna studie har vi sammanställt problem med digitaliseringen som har identifierats i tidigare FOI-studier. Vi för en diskussion kring hur problemens

karaktär kan ändras när fred övergår till gråzon eller krig. Utgångspunkten är att IT-systemen då i en högre grad blir utsatta för antagonistiska angrepp av en statsaktör eller dennes ombud. Vi presenterar också 15 fallgropar som representerar förhållanden som i fredstid är funktionella men som skapar problem i gråzon och krig. Sammanställningen av problem och fallgropar kan tjäna som ett underlag för beredskapsplanerare inom samhällsviktiga verksamheter i arbetet med att förbereda verksamheter att kunna fortgå även i gråzon och krig.
Läs hela rapporten på foi.se

Unravelling the Myth of Cyberwar

Av Per-Erik Nilsson



Föreliggande rapport diskuterar varför Rysslands full-skaliga invasion av Ukraina inte har levt upp till mångas farhågor beträffande cyberkrigföring. I rapporten granskas fem huvudhypoteser som söker besvara denna fråga. En första hypotes föreslår att ursprungliga förväntningar på Rysslands förmåga inom offensiv cyberkrigföring kan ha varit överdrivna. Detta kan ha lett till vilseledande bedömningar av situationen. Den andra hypotesen framhåller att Ryssland inte har utnyttjat sin fulla potential inom offensiv cyberkrigföring. Detta väcker frågor om hur deras faktiska kapacitet för denna typ av operationer ser ut. Hypotes tre ifrågasätter idén att rysk cyberkrigföring är ineffektiv. Istället betonas den betydande skada som redan har åsamkats, även om det inte utgör bevis för en omfattande cyberkrigföring. Den fjärde hypotesen föreslår att Ukrainas robusta cyberförsvar kan ha avskräckt en mer omfattande cyberkrigföring. Slutligen framhålls i den femte hypotesen att det som kan observeras är i linje med vad som kunde förväntas. En stor del av den tidigare forskningen på området har i över ett decennium påpekat att teorier om storskaliga cyberkrig kan leda teoretiker och beslutsfattare fel. Rapporten understryker vidare vikten av att inte förhasta slutsatser kring någon enskild hypotes. Detta beror främst på att tillgängliga data ännu är ofullständiga. I rapporten betonas även vikten av att skilja mellan fientliga cyberoperationer under krigsförhållanden och de som sker inom en fientlig intrastatlig tävlan eftersom olika förmågor, juridiska och konceptuella ramverk är aktuella beroende på kontext. Slutligen konstaterar rapporten att även om nuvarande bevis tyder på frånvaron av omfattande destruktiv cyberkrigföring, är rysk cyberkrigföring fortfarande en kraft att räkna med, särskilt som en möjliggörare av informationspåverkan och som komplement till militära kinetiska operationer. Framtida lärdomar bör därför bygga på gedigen empirisk evidens för att utveckla effektiva motåtgärder som omfattar

tekniska, organisatoriska, samhälleliga och politiska aspekter baserade på faktiska förhållanden snarare än orealistiska framtidsbilder. Spekulativt tänkande är dock viktigt för att utforska framtida scenarier, men kan inte utgöra grunden för förståelsen av cyberkrigföring. Särskilt bör Ukrainas cyberförsvar och cybersäkerhetsarbete vidare utforskas. Detta kan säkerställa en realistisk och stark respons på det ständigt föränderliga landskapet av cyberhot i krig som i tider av ofred.
Läs hela rapporten på foi.se

Passar jag som är forskarutbildad in på FOI?

Välkommen på Rekryteringsevent för forskarutbildade i Linköping den 15 april.
Vill du bli vår nästa expert inom ett område som du kanske inte ens visste fanns? Du som är forskarutbildad, eller håller på att forskarutbilda dig, är välkommen att anmäla dig till vårt rekryteringevent i Linköping!
FOI befinner sig i en kraftig tillväxtfas och vi behöver bli fler som bidrar till att stärka Sveriges försvar. Därför vill vi gärna träffa dig som är intresserad av nya utmaningar för att berätta mer om vår spännande forskningsverksamhet. Under kvällen träffar du FOI-forskare med olika bakgrund och får under avslappnade former en inblick i vår unika arbetsmiljö och hur det är att jobba hos oss.
Mer information och anmälan

Examensarbete på FOI 2024

Exjobb, uppsats och praktik på FOI innebär spännande utmaningar samtidigt som du utvecklar din egen kompetens. Du jobbar med komplexa problem i en kreativ miljö tillsammans med kunniga experter. Resultaten förverkligas hos våra uppdragsgivare. Ditt bidrag till vår forskning leder till en säkrare värld och ett starkare totalförsvar.

Läs om våra exjobb som finns i kataloger

Brinner du för cybersäkerhet?

Vi söker nya kollegor som brinner för cybersäkerhet och vill bidra till att

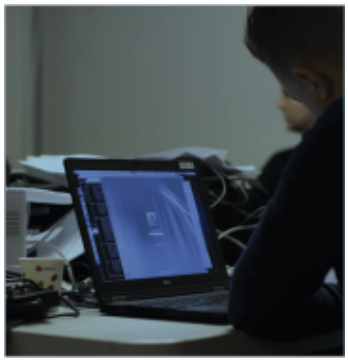
stärka Sveriges totalförsvar, bland annat med hjälp av den **nationella cyberanläggningen Crate.**

På FOI:s hemsida **Jobba hos oss** finns att läsa om de tjänster som annonseras.
Just nu har vi följande annonser inom cybersäkerhetsområdet.
Varmt välkommen med din intresseanmälan.

Framtidens cybersäkerhetsexpert för Sveriges säkerhet
Sommarjobbare - skapa sårbara nätverk
Sommarjobbare - innehållsgenerering i Crate

Är du intresserad och vill få mer information ring eller mejla
Jonas Hallberg, enhetschef Cyberförsvar, 08-555 030 00
jonas.hallberg@foi.se
Pauline Ärlebäck, enhetschef Cyberförsvarscentrum, 08-555 030 00,
pauline.arleback@foi.se

IT-incidenthantering i praktiken



Flera organisationer har bokat in övning ***Incidenthantering i praktiken*** där vi ger deltagarna en unik möjlighet att under realistiska förhållanden öva sin förmåga att hantera IT-relaterade cyberangrepp och incidenter i komplexa IT-miljöer.

Övningen leds av forskare från FOI vars forskningsområde omfattar cybersäkerhet inom samhällsviktiga system.

Vill du diskutera hur vi kan hjälpa dig och din verksamhet, kontakta
pauline.arleback@foi.se

Webbinarium och evenemang

FOI är en av arrangörerna av Källkritikens dag.
Årets tema är **Desinformation, propaganda och lögner – så sprids falska berättelser på nätet.**
Datum: Den 13 mars kl. 14.30-16.30.
Se programmet och anmäl dig på Internetstiftelsens webbplats

Se fler evenemang på foi.se

Onlinekurs med David Lindahl

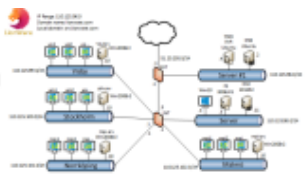
Idag är i stort sett all samhällsviktig verksamhet beroende av industriella kontrollsystem. Samtidigt är dessa system utsatta för en stor mängd cyberhot. För att höja Sveriges totalförsvars-förmåga inom cyberdomänen tillhandahåller FOI tillsammans med MSB därför en webbserie där du får en introduktion i cybersäkerhet, antagonistiska hot samt säkerhetsarbete för samhällsviktiga industriella styrsystem.

Serien omfattar tolv avsnitt och riktar sig till tekniker eller beslutsfattare som arbetar med industriella styrsystem inom samhällsviktig verksamhet. Målsättningen är att få en förståelse för vikten av cybersäkerhet i dessa system samt att ge en grundläggande kunskap om hur denna kan uppnås. I den första delen ges en introduktion till styrsystem samt hur dessa skiljer sig från vanliga IT-system ur ett cybersäkerhetsperspektiv. I den andra delen beskrivs antagonistiska hot riktade mot samhällsviktiga system samt vilka typiska metoder som dessa utnyttjar. I denna del ges också exempel på statsunderstödda cyberoperationer. I den tredje och sista delen beskrivs hur säkerhetsarbetet kan bedrivas för att på sikt höja skyddsnivån för de samhällsviktiga systemen. Vidare ges också exempel på hur incidenter kan hanteras när de uppstår.

Webbserien är framtagen som en del av verksamheten vid Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet – NCS3. NCS3 är ett samarbete mellan Myndigheten för samhällsskydd och beredskap (MSB) och Totalförsvarets forskningsinstitut (FOI). Alla åsikter i serien är forskarnas egna och inte nödvändigtvis en officiell ståndpunkt för varken FOI eller MSB.

Delta i webbserien där du får en introduktion i cybersäkerhet **Onlinekurs med David Lindahl, forskare vid FOI**

Självstudieuppgifter - Träna på tekniker och verktyg



Syftet med dessa uppgifter är att ge dig som arbetar med cybersäkerhet möjlighet att träna på tekniker och verktyg som du kan använda för att upptäcka, analysera och hantera hot och incidenter riktade mot IT och cyberfysiska system. Självstudieuppgifterna är framtagna med hjälp av Crate, Sveriges nationella cyberanläggning för totalförsvaret.

Principen för självstudieuppgifterna är att du hämtar instruktioner och de datafiler som behövs från denna sida, varpå du på egen hand kan lösa uppgifterna. På första sidan i instruktionen hittar du en beskrivning av ett scenario från vilket data har samlats in följt av ett antal konkreta frågor som du kan besvara genom att analysera den tillgängliga informationen. Du hittar också tips, lösningsförslag samt facit så att du på egen hand kan lösa uppgiften.

Glöm inte att återkoppla till oss via de formulär som anges i instruktionen, då det hjälper oss att ta fram och tillhandahålla fler självstudieuppgifter.
Lycka till!

Instruktion och uppgifterna DATALÄCKAGE och BEHÖRIGHETSKONTROLL att lösa!

Kurs i Elektronisk säkerhet

Elektroniska system är en integrerad del av vardagen. Nästan alla verksamheter är beroende av elektroniska system som måste fungera om verksamheten ska fungera normalt, eller om den ska fungera alls. Säkerhetsfrågor i sådana system är verksamhetskritiska i de flesta branscher. FOI erbjuder därför en skräddarsydd kurs i elektronisk säkerhet där FOI på ett unikt sätt bjuder på sin speciella kompetens.

Säkerhet handlar dock inte bara om att system ska vara tillgängliga, utan också om att de inte ska läcka information till obehöriga, och att informationen i dem ska vara korrekt. För att kunna hantera och bedöma frågor som rör säkerhet i elektroniska system krävs en omfattande kunskap om systemen och de hot de är utsatta för. Den här kursen erbjuder en bred genomgång av dagens elektroniska system, både vad gäller normal funktion och säkerhetsproblematik. Vissa delar av kursen berör områden där FOI är ensamma i Sverige om att ha forskningsverksamhet, till exempel radiostörning, radiopejling och IT-vapen.

Målgruppen för kursen är personer som har säkerhet inom sitt ansvarsområde men som inte nödvändigtvis själva är tekniskt verksamma, t.ex. chefer, beslutsfattare, projektledare och tjänstemän.

Är du intresserad och vill få mer information går det bra att ringa eller mejla till kursansvarig, Fredrik Söderström, 08-555 030 00
Hkes@foi.se

En mer detaljerad kursbeskrivning och anmälan hittar du här:

Kurser och utbildningar

Rapportsamling

Du vet väl om att de flesta rapporter som FOI publicerar är tillgängliga i elektronisk form från vår webplats? För att underlätta för oss som är speciellt intresserade av informationssäkerhet så har vi samlat just dessa rapporter i en speciell lista. Listan uppdateras kontinuerligt.

Rapportsamling Informationssäkerhet

Kurser 2024

Vi erbjuder utbildningar, kurser och seminarier inom våra kompetensområden. Vi kan även skräddarsy kurser utifrån din organisations behov

Kontakta oss för mer information.
Kurser och utbildningar

Crate City

OM NYHETSBREVET

FOI, Totalförsvarets forskningsinstitut, *är ett av Europas ledande forskningsinstitut inom försvar och säkerhet. Hos oss arbetar cirka 900 medarbetare med varierande bakgrunder. FOI:s kärnverksamhet är forskning, metod- och teknikutveckling samt analyser och studier. Myndigheten är uppdragsfinansierad och ligger under Försvarsdepartementet.*

Vid synpunkter på innehållet i detta nyhetsbrev kontakta Gunilla Friberg, ***gunilla.friberg@foi.se***
FOI ansvarar inte för länkar som leder till andra webbplatser.

Hantering av personuppgifter
FOI:s nyhetsbrev skickas ut via ett webbverktyg där dina personuppgifter sparas. Du samtycker till behandlingen av dina personuppgifter genom att ange din e-postadress, och i förekommande fall för- och efternamn. Endast de som administrerar verktyget och leverantören av verktyget har tillgång till

personuppgifterna. Dina personuppgifter sparas så länge du prenumererar på nyhetsbrevet. Vill du avsluta din prenumeration på FOI:s nyhetsbrev kan du avanmäla dig genom att klicka på den avprenumerationslänk som finns längst ned i varje nyhetsbrev.
Om du väljer att avanmäla dig raderar vi manuellt dina personuppgifter den första arbetsdagen nöstkommande månad. Om du vill att raderingen ska ske snabbare än så, kontakta FOI.

Läs mer om dataskyddsförordningen, dina rättigheter och kontaktuppgifter till FOI.

Följ oss gärna i sociala medier

För att avbeställa nyhetsbrevet klicka här.