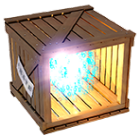
FOI

CRATE
Cyber Range And Training Environment



Nyhetsbrev Informationssäkerhet nr 1, 2025

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:

- Studie om bevisföring för systematisk säkerhet
- Mjukvarors säkerhet beror på utvecklarnas motivationer och hinder
- Tekniker och verktyg som identifierar mjukvarusårbarheter
- Kurs Elektronisk säkerhet
- Crate-CTF en tävling i cybersäkerhet - **se sändningen i efterhand**
- IT-försvarsdagen - **se föreläsningarna i efterhand**
- Krig i vår tid - Försvarsmakten **serie i sex avsnitt**
- Vi söker nya kollegor!
- FOI ger stöd till att förbättra Sveriges cyberförsvar, **foi.se/cyber**
- Självstudieuppgifter - Träna på tekniker och verktyg.
- Välkommen till onlinekurs - Säkerhet i industriella kontrollsystem.
- Rapportsamling - för oss som är speciellt intresserade av Informationssäkerhet.
- Nya kurstillfällen under 2025 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 kurstillfälle är nu öppna för anmälan:
v20 och v40 2025.
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.

Säkerhetsevidens för IT-system - En inledande studie om bevisföring för systematisk säkerhet

Rapport av Daniel Eidenskog och Christian Vestlund
Säkerhetsevidens utgörs av olika typer av artefakter som påvisar

säkerhetsegenskaper hos IT-system, ofta på ganska specifik detaljnivå. Evidens värderas och aggregeras till bevisföring som i sin tur påvisar att IT-systemen uppfyller de säkerhetsbehov som finns på verksamhetsnivå. Denna studie undersöker hur olika metoder och säkerhetsstandarder inom cybersäkerhet och funktionell säkerhet använder evidens för att påvisa att IT-systemen når tillräcklig säkerhetsnivå. Evidensen utgör en viktig bas för att uppnå assurans, där tillräckligt hög tilltro till såväl IT-systemen i sig som till utvecklare och leverantörer har uppnåtts för att kunna använda systemen i säkerhetskritiska tillämpningar. Evidens utgörs av konkreta och spårbara underlag som kan ha producerats genom ett brett spektrum av olika metoder, såsom designgenomgångar, kodgranskning, praktiska tester och formella metoder. De processer och standarder som undersökts i studien rekommenderar olika evidensmetoder men inkluderar endast generella beskrivningar av vad metoderna innebär, varför tolkningsutrymmet är stort avseende vad som faktiskt ska utföras. Värdering och aggregering beskrivs endast på övergripande plan vilket ytterligare ökar oklarheterna kring vad som efterfrågas. Det finns ett stort forskningsbehov inom evidensområdet ända från säkerhetsmål till enskilda evidensmetoder. Området värdering och aggregering tycks vara särskilt outforskat, samtidigt som det finns ett stort behov av att förbättra och utveckla olika evidensmetoder.

Här kan du ta del av hela rapporten.

Mjukvarors säkerhet beror på utvecklarnas motivationer och hinder

Rapport av Henrik Karlzén, Jerry Falkcrona, Daniel Eidenskog och Martin Karresand

Att säkerhetsnivån i mjukvara inte alltid håller måttet visas bland annat av de incidenter som inträffat i säkerhetskritiska it-system, med potentiellt allvarliga konsekvenser till följd. Det finns många samverkande orsaker till att mjukvara inte har tillräckligt säkerhet, däribland mjukvaruutvecklarnas motivation och hinder i säkerhetsfrågor. Att förstå motivationen och hindren är ett viktigt steg i att höja säkerhetsnivån i mjukvaror. Denna rapport

presenterar resultaten från en enkät om mjukvaruutvecklares motivationsfaktorer och hinder när det gäller säkerhet i mjukvara. Enkäten baseras på en tidigare nordamerikansk enkät och har här besvarats av mjukvaruutvecklare som utvecklar säkerhetskritiska system för svenska myndigheter och företag. Resultaten visar att de starkaste motivationsfaktorerna är interna och därmed kommer inifrån utvecklaren. De interna motivationsfaktorerna inkluderar sådant som ansvarstagande och medvetenhet. Externa motivationsfaktorer motiveras utifrån och är svagare, men omfattar bland annat obligatorisk säkerhetspraxis och företagskultur. Hinder bedöms överlag ha mindre påverkan än motivationsfaktorerna. De högst rankade hindren inkluderar bristande konkurrens som gör att säkerhet upplevs som oviktigt samt att utvecklaren inte får skulden för en uppkommen sårbarhet. Andra relativt betydande hinder är låg prioritering av mjukvarusäkerhet samt att ekonomiska resurser saknas.

Här kan du ta del av rapporten.

Tekniker och verktyg som identifierar mjukvarusårbarheter

Rapport av Christian Gustavsson, Christian Vestlund, Viktor Andersson, Daniel Eidenskog, Lovisa Nyholm och Casper Jensen
Att testa och verifiera säkerhetsegenskaper hos mjukvara är ett forskningsområde med hög aktivitet. Denna studie skannar av forskningsområdet för åren 2014-2024 efter tekniker och verktyg som kan upptäcka mjukvarusårbarheter. Sammantaget inventeras 237 verktyg i rapporten, varav de sju med högst bedömd mognadsgrad ligger till grund för en djupare analys och beskrivning. Trots att det finns omfattande forskning inom området innehåller den få verktyg med en hög mognadsgrad. Av alla verktyg som tas upp i rapporten så är de flesta inriktade på att identifiera enstaka typer av sårbarheter, vilket gör deras användningsområde begränsat. Forskning på senare år försöker hitta ett bredare angreppssätt, genom att samla flera tekniker till hybridverktyg eller genom att introducera maskininlärningsmodeller tränade att identifiera brister. Det återstår dock forskning innan de kan betraktas som beprövade tekniker.

Läs hela rapporten.

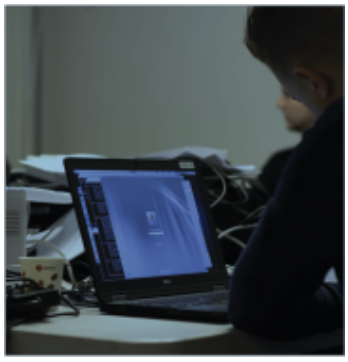
Kurs i Elektronisk säkerhet

HKES 2025
Kurs i Elektronisk Säkerhet

Dagens verksamheter är beroende av olika typer av elektroniska system och säkerhetsfrågor i dessa system är verksamhetskritiska. Kurs i elektronisk säkerhet syftar till att ge deltagaren grundförståelse för olika typer av elektroniska system både vad gäller normal funktion och säkerhetsproblematik. Kursen erbjuder ett brett urval av teman där teori varvas med praktik för både bredd och djup. Passen hålls av kompetenta föreläsare från olika delar av FOI:s verksamhet. Exempel på områden som behandlas är IT-säkerhet, kryptologi, trådlös teknik, mobiltelefoni, satellitnavigeringssystem samt pejling och störning av radiosystem.

Kursen erbjuder även en unik möjlighet till direkt dialog med FOI:s forskare och experter samt nätverkande med andra kursdeltagare.
Mer information om kursen
Anmälan till kurstillfället vecka 20 och 40
Frågor om kursen besvaras av Fredrik Söderström, kursansvarig, forskare på **hkes@foi.se**

Crate-CTF - En tävling i cybersäkerhet



Lördagen den 16 november 2024 genomfördes för femte året i rad Crate-CTF. En så kallad capture the flag- tävling där deltagarna ska lösa olika uppgifter och hitta flaggor i kod. Med 1063 deltagare i 341 lag slog tävlingen alla tidigare rekord i antal deltagare. Alla uppgifter utom en löstes till slut av de vinnande laget RoyalRoppers.

Tävlingen sändes live med inslag om hur man löste uppgifter från tidigare år och föreläsningar med bland annat David Lindahl om IT-säkerhet och mycket mer.

Se hela sändningen i efterhand på YouTube **LIVE:Create-CTF**
Här hittar du källkod för alla våra utmaningar kring CTF-tävlingar från år 2020 till 2024.

IT-försvarsdagen

Vill du ta del av IT-försvarsdagen som genomfördes den 12 december 2024? då har du nu chansen att se någon av föreläsningarna, flera av dem finns tillgängliga **här.**

IT-försvarsdagen är ett årligt återkommande forum för myndighetsanställda att träffas och diskutera problemställning, inriktningar och resultat från aktuell forskning och utveckling inom försvarsrelaterad cyber- och IT-säkerhet.

Årets IT-försvardag innehöll bland annat presentationer av:

- Stora språkmodeller inom försvar. Forskningsprojektet AI för beslutsstöd och kognitiva system forskar kring modern AI inom försvaret.
- Rysslands cyberförsvar på hemmaplan. Första året av ryska anfallskriget mot Ukraina.
- Delat ansvar inget ansvar. En analys av den svenska statsförvaltningens ansvar och styrning vad gäller svenskt informations- och cybersäkerhetsarbete.
- Almost provable security “on the cheap”. We present an experiment in end-to-end security. The result is an “almost formally end-to-end verified” distributed system
- Från event till lärande vid cybersäkerhetsövningar. Vi presenterar pågående forskning med fokus på uppföljning och bedömning av cyberförsvarförmåga.
- Automatisering av röda lag. AI-teknik för att automatisera röda lag under cybersäkerhetsövningar.

Krig i vår tid

Krig i vår tid är en serie som tar upp hoten mot Sverige och vad Försvarsmakten – och vi som land – kan göra för att motverka dem. Under sex avsnitt om cirka 15 minuter belyser vi hoten mot Sverige från flera håll genom att träffa både personer i och utanför

Försvarsmakten. Från FOI deltar bland annat David Lindahl.

Här kan du ta del av alla sex avsnitten.

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 annons inom cybersäkerhetsområdet.
Varmt välkommen med din intresseanmälan.

Expert inom informationssäkerhet som vill stärka Sveriges totalförsvar

Expert inom mjukvarusårbarheter

Utmaningsdriven front-endutvecklare till cyberanläggningen Crate

Operativ IT-ingenjör till FOIs forskningsanläggningar

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

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!

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**

Rapportsamling

Du vet väl om att de flesta rapporter som FOI publicerar är

tillgängliga i elektronisk form från vår webbplats? 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 2025

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 1.300 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 nästkommande 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.