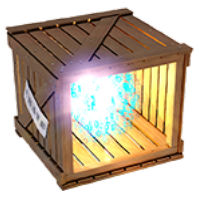
FOI

CRATE

Cyber Range And Training Environment



Nyhetsbrev Informationssäkerhet nr 1, 2026

Välkommen till vårt nyhetsbrev från enheterna *Cybersäkerhet*, *Förmågor i cyberdomänen* och *Cyberanläggningsteknik* som ingår i verksamhetsområde Cyber. Vi har försökt samla ihop de utskick vi gör i olika sammanhang från vårt verksamhetsområde 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:

- Analys av koncept och tekniker för cyberförsvar och informationssäkerhet- Slutrapport
- Automatisk incidenthantering - Erfarenheter från labbförsök.
- Principer för konstruktion av datamängder med mjukvarusårbarheter.
- Försvarbarhet i cyberdomänen - En litteraturstudie.
- En genomgång av säkerhetsincidenter och åtgärder avseende molntjänster.
- Mjukvarusårbarheter och skyddstekniker - Analys av pythonmjukvara.
- En utökad studie av verktyg som identifierar mjukvarusårbarheter.
- Verktyg och teknik för CNO-övningar.
- "Syster-CTF" arrangeras av FRA, Must och Säkerhetspolisen.
- FOI ger stöd till att förbättra Sveriges cyberförsvar, **foi.se/cyber**
- FOI växer och söker nya kollegor! **FOI:s lediga tjänster!**
- Rapportsamling - för er som är speciellt intresserade av Informationssäkerhet.

Kontakta oss

Har du frågor om vårt nyhetsbrev - kontakta:
Gunilla Friberg

gunilla.friberg@foi.se

Publikationer

FOI publicerar rapporter där de flesta är tillgängliga i elektronisk form via

www.foi.se

Våra kurser 2026

Elektronisk säkerhet:
Följande kurstillfälle är nu öppna för anmälan: **v19 och v40 2026**.
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.

Verksamhetsområde Cyber

Kära kollegor,
Det är med stor glädje och förväntan som jag nyligen tillträdde som verksamhetsområdeschef cyber.
Med lång erfarenhet av cybersäkerhet, riskhantering och skydd av kritisk infrastruktur arbetar jag med att stärka Sveriges motståndskraft i ett allt mer komplext och snabbföränderligt hotlandskap.
Under åren har jag haft förmånen att leda människor, grupper och verksamheter igenom kriser, förändring och tillväxt på globala bolag med högteknologiska produkter. Särskilt fokus har varit totalförsvar, i synnerhet telekom, mjukvaru- och halvledarindustrin, samt senast försvarsindustrin.
Jag är imponerad av den unika cyberexpertisen som finns på FOI och jag ser fram emot att tillsammans med er alla bidra till en cybersäkrare värld!
Med vänliga hälsningar,
Foteini Papiri

Analys av koncept och tekniker för cyberförsvar och informationssäkerhet

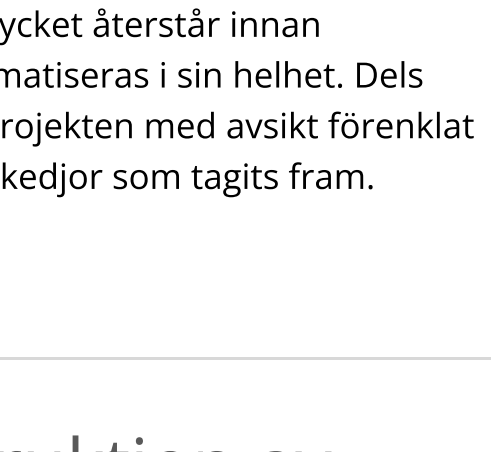
Rapport av Jerry Falkcrona
Denna rapport beskriver det arbete som genomförts inom ramen för FoTprojektet Analys av koncept och teknik för cyberförsvar och informationssäkerhet, åren 2021-2025. Projektet har bedrivits som ett antal fristående studier och har utvärderat tekniker och metoder för att stärka säkerheten i it-system. Rapporten sammanfattar resultatet från dessa studier och beskriver den övriga verksamhet som genomförts inom projektet.
Läs hela rapporten

Automatisk incidenthantering - Erfarenheter från labbförsök

Rapport av Teodor Sommestad och Henrik Karlzén
FOI har deltagit i tre projekt som på olika sätt försökt automatisera incidenthanteringsprocessen. I projekten har ett stort antal tekniska lösningar för olika delsteg tagits fram ihop med förslag på hur de ska sättas samman. FOI har i alla projekt varit ansvariga för arbetet med att skapa testfall där fiktiva incidenter utspelar sig i en labbmiljö. Detta har använts för tester av enskilda tekniker och komponenter samt för mer omfattande demonstrationer där incidenter utspelar sig. Testerna och demonstrationerna pekar på att mycket återstår innan incidenthanteringsprocessen kan automatiseras i sin helhet. Dels finns praktiska hinder som forskningsprojekten med avsikt förenklat bort, dels fungerar få steg i de verktygskedjor som tagits fram.
Läs hela rapporten

Principer för konstruktion av datamängder med mjukvarusårbarheter

Rapport av Christian Vestlund, Christian Gustavsson och Daniel Eidenskog
Verktyg som kan identifiera sårbarheter i mjukvara spelar en viktig roll för att skapa säker mjukvara. Det är dock inte uppenbart hur bra sådana verktyg är på att hitta olika typer av sårbarheter eller hur verktygen bör utvärderas. I forskningslitteraturen används olika datamängder med sårbarheter för att utvärdera och jämföra verktyg. Denna rapport presenterar en litteraturstudie som undersöker vilka datamängder som finns och hur dessa presenteras i litteraturen. Bland annat undersöks vilken kritik som presenteras mot dem och vilka egenskaper hos datamängderna som lyfts fram i publikationerna. I studien har 54 olika datamängder eller verktyg som kan generera datamängder identifierats. Därtill har tio typer av kritik och 22 önskvärda egenskaper identifierats. Resultaten visar en trend mot att datamängder som baseras på sårbarheter i verklig mjukvara har blivit vanligare medan det skapas en mindre andel datamängder



med konstruerade eller injicerade sårbarheter. Brist på realism är dessutom en vanlig kritik mot datamängder, vilket också avspeglas i att realism är en av de vanligaste önskvärda egenskaperna. Studiens resultat visar dock att det saknas en etablerad gemensam bild över vilka egenskaper som behövs för att skapa bra datamängder.
Läs hela rapporten

Försvarbarhet i cyberdomänen

En litteraturstudie av Henrik Karlzén, Hannes Holm och Martin Karresand

Den här rapporten sammanställer forskningslitteratur om skydds- och försvarslösningar som kan påverka förutsättningarna för försvar (försvarbarheten) i cyberdomänen. Rapporten ger en första inblick i det relativt nya begreppet försvarbarhet, genom att bedöma hur forskarnas lösningar förhåller sig till försvarbarhet. Eftersom det finns extremt stora mängder skydds- och försvarslösningar görs här en begränsning till lösningar som använder terminologin i Mitres D3fendramverk. Den allra mesta inkluderade forskningslitteraturen fokuserar på ramverkets taktik benämnd detektion. Den forskningen rör främst nätverkstrafikanalys (77 % av artiklarna), men också användarbeteendeanalys (7 %), filanalys (6 %) med flera. De allra flesta artiklarna (85 %) presenterar lösningar som bedömds underlätta försvarbarheten. Även de flesta av dessa är fokuserade på detektion. De lösningar som tvärtom försvårar försvarbarheten rör mestadels isolering men också härdning, kompletterat med detektion och vilseledning. Försvarbarhet verkar alltså underlättas av främst detektion, men försvåras av flera olika taktiker. Det talar också för att detektion i huvudsak ökar försvarbarheten, medan arkitektoniska förändringar som härdning och isolering mer troligt minskar försvarbarheten. Artiklarna själva diskuterar inte lösningarnas påverkan på försvarbarheten. Anledningen till de uteblivna diskussionerna tyder på att de som föreslår tekniska lösningar inte brukar beakta försvararens roll. En del av artiklarna nämner dock människan och främst då hur lösningarna kan ge visualisering av loggar. För att bedöma hur applicerbara forskarnas lösningar är i praktiken gör rapporten också bedömningar av lösningarnas mognad och kvalitet samt vilken typ av indata de använder för utvärdering och framförallt om det är data från verkligheten. De allra flesta lösningar som forskningen producerat är på sin höjd prototyper i labbmiljö (TRL 3-4). Enbart 16 % av alla artiklar bedömdes vara av hög kvalitet. Av de studerade 198 artiklarna bedriver 192 någon typ av datainsamling. Det finns bara 29 artiklar (15 %) som använder publika dataset med data från riktiga system.
Läs hela rapporten

En genomgång av säkerhetsincidenter och åtgärder avseende molntjänster

Av John Ziegenbein och Viktor Bergström

Molnteknologi har under senare år fått en betydande ökning i användning, bland annat som en lösning på det kontinuerligt växande behovet av beräkningskapacitet, exempelvis inom områden för artificiell intelligens. Samtidigt ökar antalet säkerhetsincidenter i molntjänster varje år, vilket understryker behovet av fördjupad kunskap om molnsäkerhet för att

möjliggöra användning i säkerhetskänsliga sammanhang. Denna rapport syftar till att utvärdera incidenter och säkerhetsåtgärder relaterade till molnsäkerhet. Genomgång av fem populära säkerhetsramverk utförs för att identifiera överlappande åtgärder och säkerhetskategorier. Vidare analyseras 157 rapporterade molnincidenter från de senaste 10 åren. Incidenterna analyseras med avseende på orsak till incidenten, med hjälp av de säkerhetskategorier som identifieras i tidigare steg. Även konsekvenserna av dessa incidenten analyseras. Slutligen analyseras hur de vanligast förekommande orsakerna bakom molnincidenterna kunde ha förhindrats baserat på de identifierade säkerhetsåtgärderna. Resultaten av analysen pekar på att incidenterna i stor utsträckning beror på enklare felkonfigurationer, främst inom områdena identitets- och åtkomsthantering, infrastruktur samt dataskydd. En vanligt återkommande orsak till incidenter är publikt åtkomliga molnbaserade resurser utan tillräcklig åtkomstkontroll eller utan kryptering av känslig information. Säkerhetsramverken är omfattande och komplexa, vilket gör dem svåra att följa i praktiken. Samtidigt finns flera säkerhetsåtgärder som återkommer i alla ramverk, vilket tyder på en viss samsyn inom branschen. Dessa gemensamma åtgärder presenteras och diskuteras i rapporten. Resultaten visar också att molnsystem ofta snabbt blir komplexa, något som många organisationer har svårt att hantera på ett säkert sätt. Att använda säkerhetslösningar från molnleverantören kan underlätta, men kräver ofta specialiserad kompetens.
Läs hela rapporten

Mjukvarusårbarheter och skyddstekniker - Analys av pythonmjukvara

Av Casper Jensen, David Ekman, Henrik Karlzén, Daniel Eidenskog och Jerry Falkcrona

Mjukvara har en central roll i många verksamheter. Samtidigt har det visat sig att det är mycket svårt att utveckla mjukvara utan sårbarheter. Rapporten beskriver resultatet av en studie som undersöker vilka som är de vanligaste sårbarhetstyperna i kod skriven i programmeringsspråket Python. Studien undersöker också vilka som är de vanligaste skyddsteknikerna för att åtgärda sårbarheterna. Studien presenterar en taxonomi för skyddstekniker samt sambandet mellan sårbarhetstyper och skyddstekniker. Resultaten visar att de vanligast förekommande sårbarhetstyperna är bristande hantering av indata samt bristande autentisering och åtkomstkontroll. Resultaten visar även att skyddstekniken indatavalidering är vanligast vid åtgärdandet av sårbarheter.
Läs hela rapporten

En utökad studie av verktyg som identifierar mjukvarusårbarheter

Av Christian Gustavsson, Lovisa Nyholm, Viktor Andersson, Christian Vestlund, Casper Jensen och Daniel Eidenskog

Rapporten presenterar en utökad analys av verktyg som identifierar mjukvarusårbarheter och som publicerats vetenskapligt under perioden 2014-2024. Av totalt 273

verktyg beskrivna i litteraturen bedöms 27 vara särskilt intressanta: antingen har de haft en hög teknologisk mognadsgrad redan vid sin ursprungliga publicering, eller så har de fortsatt utvecklas på ett sätt som kan öka deras praktiska användbarhet. Resultaten visar att de vidareutvecklade verktygen i huvudsak använder fuzzning, dataflödesanalys och symbolisk exekvering, ofta i hybridform. Flera verktyg har hittat nya sårbarheter i produktionsmjukvara, varav många tilldelats CVE-nummer.Studien identifierar även tydliga beroenden inom forskningsområdet,där ett fåtal forskargrupper står bakom en stor del av verktygen. Verktygens målsystem domineras av C/C++ och inbyggda system, men omfattar även Java, Android, Rust och komplexa indataformat.

Läs hela rapporten

Verktyg och teknik för CNO-övningar - Slutrapport

Av Hannes Holm

Utförande av cyberangrepp krävs för att uppnå en god cyberförsvarsförmåga, exempelvis för att identifiera sårbarheter, träna logganalytiker och för att anpassa intrångsdetektionssystem. Projektet Verktyg och teknik för Computer Network Operations (CNO) övningar (VECNO) bedrev från 2021 till 2025 forskning rörande automatisering av cyberangrepp. Forskningen operationaliserades huvudsakligen genom verktyget Lore som automatiserar cyberangreppsplaner utan krav på operatör eller förkunskap om mål. Lore var före 2021 ett relativt enkelt verktyg som utförde ett fåtal typer av angrepp och som enbart hade använts till ett fåtal tekniska tester. Genom arbetet inom projektet har Lore vidareutvecklats på olika sätt, och idag har verktyget ett omfattande modulstöd och har använts för diverse ändamål. Lore har exempelvis använts för åtta cybersäkerhetsövningar, för forskning kring cyberförsvarsmekanismer, samt för en säkerhetstävling. Projektet har även involverat flera utvärderingar av Lore, i synnerhet huruvida det erbjuder samma upplevelse som mänskliga inspel för logganalytiker som deltar i cybersäkerhetsövningar. Resultaten visar att den upplevda realismen var ungefär lika hög, och att inspelen var ungefär lika lärorika, oavsett om Lore eller mänskliga inspel nyttjades som källa för cyberangrepp.

Läs hela rapporten

"Syster-CTF" genomförs 21 mars

Vår "syster-CTF" Undutmaning arrangeras av myndigheterna FRA, Must och Säkerhetspolisen och har kört årligen sedan 2022. I år är det dags lördag den 21:a mars 12:00-20:00 (UTC+1).

Websida: https://undutmaning.se/
Discord:

https://discord.com/invite/fwBkQJRD

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.
Följande kurstillfälle är nu öppna för anmälan: **v19 och v40 2026**.
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

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 ut nu.
Sidan uppdateras kontinuerligt med nya jobbtillfällen.

Just nu söker vi
Nyfiken ledare som vill driva utvecklingen av totalförsvarets cyberanläggning
Junior cybersäkerhetsexpert

Varmt välkommen med din intresseanmälan.
Är du intresserad och vill få mer information ring eller mejla
Foteini Papiri, verksamhetsområdeschef Cyber, 08-555 030 00
foteini.papiri@foi.se
Jonas Hallberg, enhetschef Cybersäkerhet, 08-555 030 00
jonas.hallberg@foi.se
Pauline Ärlebäck, enhetschef Förmågor i Cyberdomänen**,** 08-555 030 00**,** **pauline.arleback@foi.se**
Jonas Wiman, Tf enhetschef Cyberanläggningsteknik, 08-555 030 00**,**
jonas.wiman@foi.se

Rapportsamling

Du vet väl om att de flesta rapporter som FOI publicerar är tillgängliga i elektronisk form från vår webplats? För att underlätta för er som är speciellt intresserade av informationssäkerhet så har vi

samlat just dessa rapporter i en speciell lista. Listan uppdateras kontinuerligt.
Rapportsamling Informationssäkerhet

Kurser 2026

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 1600 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