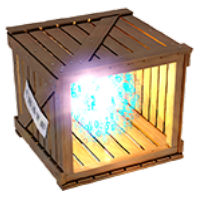
CRATE

Cyber Range And Training Environment

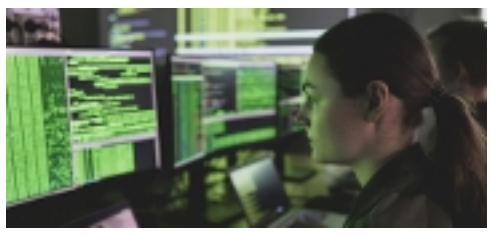


Nyhetsbrev Informationssäkerhet nr 1, 2023

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:

- Framtida cybersoldater.
- Verktyg som döljer skadlig kod.
- Detektion av illasinnad exfiltrering av data via nätverk.
- Digitaliseringens risker i hälso- och sjukvård.
- IT-incidenthantering i praktiken.
- FOI ger stöd till att förbättra Sveriges cyberförsvar, **foi.se/cyber**
- Självstudieuppgifter - Träna på tekniker och verktyg.
- Välkommen till onlinekurs - Säkerhet i industriella kontrollsystem.
- Examensarbete på FOI 2023.
- Vi söker nya kollegor!
- Rapportsamling - för oss som är speciellt intresserade av Informationssäkerhet.
- Nya kurstillfällen under 2023 & 2024 i *Elektronisk säkerhet samt grund-och påbyggnadskurs Säkerhet i industriella informations- och styrsystem*. Vi erbjuder även kurs i *Praktisk incidenthantering i industiella informations- och styrsystem.*

Vi testar framtida cybersoldater



Försvarsmakten startade år 2020 en elva månader lång utbildning av värnpliktiga cybersoldater – en militär grundutbildning med bland annat akademiska kurser. Cybersoldater förväntas få en växande roll i framtidens försvar. Forskare på FOI bidrar till att rätt personer antas till den verksamheten.
Testerna av de värnpliktiga mäter främst två områden:

- Kognitiv förmåga; en komplettering av Plikt- och prövningsverkets tester inom områden som matematik och logik.
- Kunskap inom cyberområdet; generell datorkunskap likväl som kunskap om säkerhet och nätverk.

Det här är en testning som passar perfekt in i FOI:s kompetensområden, säger Christian Valassi, biträdande projektledare.

Ta del av hela intervjun med Christian Valassi.

Verktyg som döljer skadlig kod - En systematisk granskning

Rapport av Hannes Holm, Erik

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

Elektronisk säkerhet: Följande kurstillfällen är nu öppna för anmälan: **v43 2023** (pga schemaläggningskrock flyttat från tidigare placering v40) respektive **v4 2024**.

Kurstillfället v19 2023 är fulltecknat. Mejla oss om du är intresserad av eventuella restplatser, **hkes@foi.se**

Grundläggande kurs: Säkerhet i industriella informations- och styrsystem (gk-SI3S), intresseanmälan via **ics@msb.se**

Påbyggnadskurs: Säkerhet i industriella informations- och styrsystem (pk-SI3S), intresseanmälan via **ics@msb.se**

Praktisk incidenthantering i industriella informations- och styrsystem (I4S), intresseanmälan via **ics@msb.se**

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.

Hyllienmark och Mats Persson

Denna rapport beskriver en systematisk granskning av verktyg som döljer skadlig kod. Verktygen identifierades via Github, en databas som huvudsakligen innefattar mjukvaruprojekt skrivna som öppen källkod. Totalt kategoriserades 174 verktyg enligt fyra huvudkategorier - allmän projektinformation, vilka arkitekturer och filformat som stödjs, vilka försvar mot statisk granskning som erbjuds, samt vilka försvar mot dynamisk granskning som erbjuds. Resultatet visade att de allra flesta verktyg tillämpade en applikation för att kryptera den skadliga koden, och en annan applikation för att dekryptera och exekvera den på en dator. Det visade också att de flesta verktyg troligen skapades i utbildningssyfte snarare än för att effektivt dölja skadlig kod.
Läs hela rapporten

Detektion av illasinnad exfiltrering av data via nätverk

En systematisk litteraturgenomgång av Henrik Karlzén och Christian Valassi

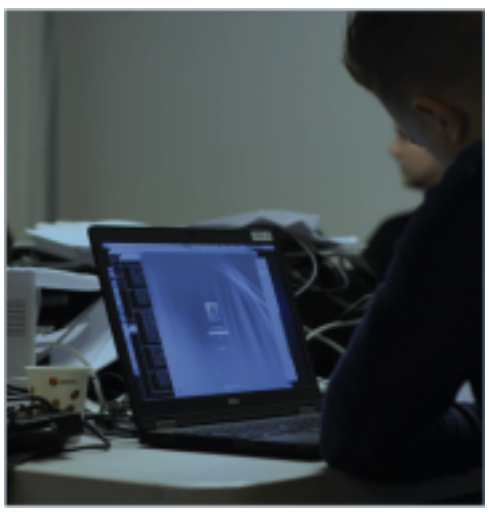
Den här rapporten presenterar en systematisk litteraturgenomgång om detektion av illasinnad nätverksbaserad dataexfiltrering. Sådan exfiltrering utgörs av angripares överföring av information från målmaskin till angriparmaskin. Eftersom det är mycket svårt att hålla alla angripare ute ur nätverken är detektionen av exfiltrering en viktig del i försvaret. Litteraturgenomgången inkluderar 48 forskningsartiklar utgivna 2012-2022. Genomgången visar att artiklarna har tydliga syften men däremot oftast otydligt beskrivna hypoteser. Därtill visar genomgången att artiklarna fokuserar på labbmiljöer som efterliknar universitetsnät medan bara en artikel har en militär nätverksmiljö. Artiklarna beskriver i undantagsfall vilka data exfiltreringen rör. Det rör sig då om kreditkortsuppgifter, inloggningsuppgifter och dokument. Det är också ovanligt att artiklarna beskriver tänkta hotaktörer. Artiklarna försöker detektera exfiltrering som döljs på olika sätt. Oftast rör det sig om döljande i form av placering av data i pakethuvuden, användning av protokoll som normalt inte nyttjas för användares dataöverföring eller av kryptering. Artiklarnas exfiltrering genomförs oftast via protokollet DNS, vilket har sitt legitima bruk i översättning av domännamn till IP-adresser. Detektionsmetoderna baseras på olika förändringar som exfiltreringen ger upphov till. Det rör sig om nätverksmässiga skillnader i entropi, tidsaspekter, stränglängder, trafikflöden samt pakethuvudinnehåll. Algoritmerna är vanligen baserade på djupinlärning eller traditionell maskininlärning. Detektionsmetoderna utvärderas relativt knapphändigt i artiklarna. Rapportens bedömning är att mer forskning behövs om framförallt detektion av exfiltrering som sker via videomöten, blockkedjenätverk, DNS över HTTPS, IPv6 och andra nyare protokoll. Därtill behövs forskning som snarare än att försöka detektera specifika tekniker tar fram mer generella algoritmer som kan detektera fler exfiltreringstekniker.
Läs hela rapporten

Digitaliseringens risker i hälso- och sjukvård

Rapport av Daniel Eidenskog, Ulrika Eckersand och Eva Mittermaier

Hälso- och sjukvården genomgår en omfattande och nödvändig digitalisering för att möta framtidens vårdbehov. Digitaliseringen öppnar för många nya möjligheter till förbättringar, såsom effektivare vårdflöden, effektivare informationsdelning, bättre diagnosstöd, effektivare behandlingar och högre tillgänglighet. Samtidigt för den nya tekniken med sig nya risker om de digitala systemen angrips eller fallerar. För patienterna kan hälso- och sjukvårdens digitala system vara direkt livsavgörande, varför såväl cyber- som informationssäkerhet måste säkerställas. Därtill kan beroenden av digitala system ge stor påverkan på den vardagliga verksamheten när dessa angrips eller fallerar. Olämpligt utformade digitala system kan även försämra beredskapen att hantera kriser. Effektiv digitalisering innebär inte bara införandet av digitala verktyg, utan kräver även att processer och arbetssätt förändras. Digitalisering är inte ett självändamål, utan en del i verksamhetsförändringar. Dåligt genomförd digitalisering kan dessutom bli ett stort arbetsmiljöproblem. Tydlig ansvarsfördelning, flexibel organisation och upplevd delaktighet bland personalen är viktiga för en lyckad digitalisering. När digitala system används är det mycket viktigt att göra en bred bedömning av såväl förväntade som potentiella konsekvenser av oönskade händelser i systemen. Personsäkerhet, informationssäkerhet, cybersäkerhet och krisberedskap byggs inte in i systemen per automatik utan måste hanteras med stor medvetenhet under systemens hela livscykel.
Läs hela rapporten

IT-incidenthantering i praktiken



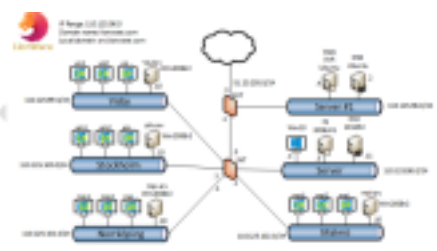
Flera organisationer har bokat in övning ***Incidenthantering i praktiken*** där vi ger deltagarna en unik möjlighet att under realistiska förhållanden öva sin förmåga att hantera IT-relaterade cyberangrepp och incidenter i komplexa IT-miljöer.

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

Vill du få ytterligare information om verksamhetsspecifik anpassad övning, **Läs här!**

Vill du diskutera hur vi kan hjälpa dig och din verksamhet, kontakta **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**

Examensarbete på FOI 2023

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 ut nu.
Just nu har vi följande annonser inom cyberområdet.
Varmt välkommen med din intresseanmälan.

Systemtekniker med känsla för virtualisering

Cybersäkerhetsexpert som vill stärka totalförsvaret

Cybersäkerhetstalang som vill utvecklas i en stimulerande miljö

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

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, Christian Valassi, 08-555 030 00
Hkes@foi.se

En mer detaljerad kursbeskrivning och anmälan hittar du här:

Kurser och utbildningar

Kurs Säkerhet i industriella informations- och styrsystem

Det finns ett stort behov av att kunna kommunicera med allt fler system idag. Behovet gäller inte bara kontorssystem utan även produktionssystem i tidigare mer avgränsade miljöer. Utvecklingen mot mer uppkopplade system och en ökad användning av kommersiell programvara gör att produktionssystem idag är mer exponerade mot omvärlden än tidigare.

Grundläggande kurs: Säkerhet i industriella informations- och styrsystem (gk-SI3S) belyser den förändrade hotbild mot kontrollsystem som uppstår när kommersiell programvara blir vanligare samt vad en ökad exponering via uppkopplade system kan få för konsekvenser. Kursen riktar sig till dig som arbetar operativt med industriella informations- och styrsystem.

Dagens industriella informations- och styrsystem bygger idag på en hög grad av kommersiell programvara och ett stort behov av att kunna kommunicera med andra både innanför och utanför de egna systemen. Det finns därför ett stort behov av att kunna skydda dessa system mot oönskad påverkan, dels genom att förstå vad ens egna system kan göra, dels genom att förstå hur man kan skydda sina egna system.

Påbyggnadskurs: **Säkerhet i industriella informations- och styrsystem (pk-SI3S)** bygger vidare på den grundläggande kursen, med ett större fokus på hur man kan förbättra skyddet av egna system mot antagonistiska hot. Kursen riktar sig till dig som arbetar operativt med industriella informations- och styrsystem.

Kursen organiseras av MSB. Intresseanmälan kan göras via **ics@msb.se**

Är du intresserad och vill få mer information går det bra att ringa eller mejla Pauline Ärlebäck (kursansvarig), 08-555 030 00, **pauline.arleback@foi.se**

En mer detaljerad kursbeskrivning och anmälan hittar du här **Kurser och utbildningar**

Kurs Praktisk incidenthantering i industriella informations- och styrsystem

Alla Industriella informations- och styrsystem drabbas någon gång av incidenter. Dessa incidenter kan orsakas av allt från olycksfall till riktade angrepp från en antagonist.
För att kunna hantera incidenter krävs förberedelse och en möjlighet att upptäcka att incidenten har inträffat.
Under kursen ***Praktisk incidenthantering i industriella informations- och styrsystem (I4S)*** ges deltagarna en unik möjlighet att under realistiska förhållanden öva förmågan att hantera IT-relaterade incidenter och angrepp i en IT-miljö med industriella informations- och styrsystem. Kursens huvudmoment är en övning där du arbetar i ett lag med andra med målet att skydda ett företags nätverk mot angrepp. Kursen riktar sig till dig som arbetar med IT i miljöer där OT finns i närheten.

Kursen organiseras av MSB. Intresseanmälan kan göras via **ics@msb.se**

Är du intresserad och vill få mer information går det bra att ringa eller mejla Pauline Ärlebäck (kursansvarig), 08-555 030 00, **pauline.arleback@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 2023

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