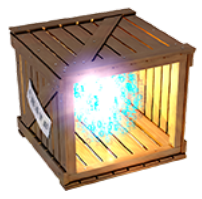
FOI

CRATE

Cyber Range And Training Environment



Nyhetsbrev Informationssäkerhet nr 1, 2021

FOI om Informationssäkerhet

Välkommen till årets första nyhetsbrev från enheten Informationssäkerhet och IT-arkitektur. Vi har försökt samla ihop de utskick vi gör i olika sammanhang från vår enhet 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:

- Statsattribuerade cyberangrepp under 2020.
- Cyberattacker mot samhällsviktig verksamhet.
- Cyberfysiska sårbarheter i tunga fordon.
- Cyberoperationer, en slutrapport.
- Mjukvarudefinierade nätverk.
- Biometriska metoder för teknisk bevakning.
- Vi presenterar resultatet från 20/20 CTF - tävling i cybersäkerhet.
- Vad är CRATE?
- Rapportsamling - för oss som är speciellt intresserade av Informationssäkerhet.
- Nya kurstillfällen 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 söker nya kollegor som brinner för cybersäkerhet och vill bidra till att stärka Sveriges totalförsvar med hjälp av den nationella cyberanläggningen CRATE. Om du eller någon du känner är intresserad, titta på FOI:s hemsida **Jobba hos oss**
Just nu, eller i en nära framtid, kommer där att finnas två annonser, en riktad mot *Systemtekniker med hackermentalitet* och en riktad mot *Pedagogisk cybersäkerhetsexpert.*

Omvärldsbevakning statsattribuerade cyberoperationer 2020

Ta del av **David Lindahl** sammanfattande reflektioner kring förmodade statsstödda cyberoperationer.

David har skrivet en kort och lättläst sammanfattning över några av förra årets statsattribuerade cyberangrepp. Han har utgått från en publik databas över angrepp och fyllt på med andra öppna data.
Memot innehåller övergripande reflektioner och slutsatser rörande cyberincidenter som rapporterats i media och andra öppna källor från mitten av oktober 2019 till november 2020.
Läs hela memot

Cyberattack mot samhällsviktig verksamhet

Se **David Lindahl** på FOI:s Youtube kanal om cyberhot mot hälso- och sjukvård.
Filmen har skapats av **Mikael Wedlin** och **David Lindahl** och presenterades under *Folk och Försvar Rikskonferens 11-12 januari 2021.*
Se filmen här!

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

Avancerad kurs i IT-incidenthantering, (AKUT-CYBER)
Kursen erbjuds som företagskurs under 2021.
Är ditt företag/organisation intresserad, ring eller mejla Mikael Wedlin (kursansvarig)
mwe@foi.se

Elektronisk säkerhet:
Kurstillfälle v40 2021 respektive v4 2022 är öppna för anmälan.

Kurstillfället v18 2021 är för närvarande fulltecknat. Om framtida pandemirestriktioner tillåter kan ytterligare platser eventuellt tillkomma.

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.

Vi har anpassat våra kurser efter rådande situation och

följer folkhälsomyndighetens råd och rekommendationer.

David Lindahl, Birgitta Liljedahl och Annica Waleij har skrivit ett memo kring hur Covid-19-pandemin utnyttjas för att främja cyberangrepp. FOI har utfört omvärldsbevakning kring hur Covid-19-pandemin har utnyttjats av olika aktörer för att främja cyberangrepp. Memot tar upp olika exempel på bedrägerier, skadlig kod och misstänkta statsaktörers operationer som rapporterats under de första tre månaderna av pandemin och diskuterar slutsatserna som kan dras från dessa.
Läs hela memot

Läs även memot IT-sårbarheter i hälso- och sjukvårdssystemet - exemplet med Wannacry och cyberattacken på British National Health Service av **David Lindahl, Birgitta Liljedahl och Annica Waleij.**
Digitalisering i allmänhet och inom hälso- och sjukvårdssektorn i synnerhet erbjuder såväl möjligheter som utmaningar kring den snabba utvecklingen av IT-infrastruktur, Internet of Things (IoT) och nya IT-baserade verktyg.
En av utmaningarna är att ökat beroende av datatjänster också ökar riskerna vid cyberangrepp mot dessa tjänster.

En föreläsning av **David Lindahl och Birgitta Liljedahl**
I skuggan av pandemin: Cyberattackerna ökar

Cyberfysiska sårbarheter i tunga fordon

Christian Valassi och **Martin Karresand** har skrivit en rapport om digital utrustning i tunga fordon.

Fordon blir allt mer digitaliserade och förses med olika gränssnitt för uppkoppling mot internet och annan digital utrustning. Detta gäller inte minst tunga fordon, där olika påbyggnader från tredje part ytterligare ökar gränsytorna mot omvärlden. Samtidigt utgör en stor del av den tunga fordonsflottan en viktig del av samhällsviktig verksamhet. MSB har därför initierat en studie av cybersäkerhet i tunga fordon, med särskild inriktning mot fordon av vikt för civilförsvaret, för att belysa aktuell status och framtida trender inom området. Studien har bedrivits inom NCS3-samarbetet och bygger på en litteraturstudie inom området samt intervjuer med personal på olika befattningar inom räddningstjänsten och fordonstillverkare. Resultatet visar att cybersäkerhetsarbetet inom branschen ännu är i sin linda, men att tillverkningssidan har börjat anamma cybersäkerhetsprinciper vid nyutveckling. Trots att cybersäkerhetsnivån i tunga fordon är låg samtidigt som angreppsytorna ökar motverkar delvis det traditionella fokuset på tillförlitlighet och personsäkerhet (eng. safety) risken för framgångsrika angrepp. Vår bedömning är att för närvarande utgör något slags tillgänglighetsangrepp det största hotet.
Beställ rapporten

Cyberoperationer

Henrik Karlzén har skrivit en slutrapport om cyberoperationer under åren 2017-2020 åt Försvarsmakten.

Cyberoperationer utgörs av militärt agerande som syftar till att påverka cyberdomänen och därmed nå en bestämd målsättning. Agerandet kan vara både defensivt och offensivt. Rapporten utgör en slutrapport för det projekt om cyberoperationer som utförts vid FOI åren 2017-2020 åt Försvarsmakten. Fokus ligger därför på Försvarsmaktens behov av ökad förmåga att utföra cyberoperationer. Rapporten sammanfattar projektbakgrunden och det arbete som utförts i projektet, inklusive rapporter, memon, forskningsartiklar och webbinarier.
Sex forskningsfrågor besvaras och framtida forskningsmöjligheter föreslås. Nedan ges en sammanfattning av rapportens slutsatser.
Forskningen om modellering på området är ganska begränsad. Ofta fokuserar modellerna på tekniskt arbete och är förenklade så att operationer sker i steg utan cykler, med inslag av manuell styrning under tiden samt med generella syften. Att uppnå situationsförståelse på området är svårt på grund av att tekniska delar måste sammanföras med organisatorisk ledning. Det är också svårt att attribuera genomförda operationer eftersom aktörer inte är öppna med vad de gör. Utpekanden

av angripare efter angrepp verkar göras på svag grund.
Cyberoperationer verkar i huvudsak handla om underrättelseinhämtning. Cybersabotage är ovanligare vilket kan bero på att sabotage är enklare att utföra utanför cyberdomänen. I öppna källor framgår att en stor del av cyberoperationernas offer hör hemma i USA, vilket kan bero på att det där finns attraktiva mål eller att källorna fokuserar på USA.
Cyberoperationer beskrivna i öppna källor verkar inte ha krävt så mycket sofistikation för att utföra. Men det kan finnas ett mörkertal av sofistikerade operationer som inte upptäcks. Källorna tyder i alla fall på att det främst är resursstarka och mogna organisationer som utför operationer. Cyberoperationer kan på teknisk nivå övas i cyberanläggningar. Avsaknaden av data om riktiga cyberoperationer ger dock begränsningar i realismen. Det är dessutom en utmaning att kombinera tekniska övningar med diskussionsövningar på ledningsnivå.
Folkrättsligt saknas klara regler för vad som är tillåtet i cyberdomänen även om sammanslutningar som EU och Nato börjat ta fram egna regler och tolkningar. En svårighet är att militära och civila cybersystem ofta är sammanflätade varför det i cyberdomänen saknas klara distinktioner mellan vad som är militärt och vad som är civilt.
Läs hela rapporten

Mjukvarudefinierade nätverk

Daniel Eidenskog, Erik Hyllienmark och Caroline Bildsten har skrivit en rapport med syftet att ge läsaren en grundläggande kunskap om mjukvarudefinierade nätverk och de byggstenar som används i dem.

Mjukvarudefinierade nätverk ändrar modellen för hur trafikflöden styrs i nätverk genom att styrlogiken centraliseras och samtidigt separeras från nätverkskomponenternas datavägar. Tekniken syftar till att möjliggöra administrativt enklare styrning av trafikflöden, som dessutom kan ske på högre abstraktionsnivå. Mjukvarudefinierade nätverk är väl etablerade på marknaden, vilket innebär att flera populära kommersiella lösningar använder tekniken. Mjukvarudefinierade nätverk är vanliga i datacenter och trenden tycks vara att tekniken blir allt vanligare även i enklare systemlösningar. Syftet med denna studie är att ge läsaren en grundläggande kunskap om mjukvarudefinierade nätverk och de byggstenar som används i dem. Kunskapen är främst avsedd att underlätta diskussioner kring mjukvarudefinierade nätverk i samband med utveckling och förvaltning av IT-system inom Försvarsmakten och andra offentliga organisationer. Rapporten tar upp vad mjukvarudefinierade nätverk är, vilka byggstenar som krävs för att bygga sådana nätverk, hur de kan påverka nätverken ur olika aspekter och vilka effekter de kan få i IT-systemperspektivet. Rapporten har sin grund i vetenskaplig litteratur, som till största del centreras kring öppna lösningar för mjukvarudefinierade nätverk, då information saknas i djupet om proprietära lösningar. Många av de problem som hanteras med hjälp av mjukvarudefinierade nätverk kan även lösas med andra tekniker. Mjukvarudefinierade nätverk för dock även med sig andra fördelar, exempelvis underlättandet av administrationen av nätverket. Dessutom förbättrar tekniken möjligheterna för nyttjandet av andra lösningar så som tjänstekedjor eller mikrosegmentering. Mjukvarudefinierade nätverk för dock inte endast med sig fördelar utan introducerar även nya angreppsytor och fallgropar, såsom att den centrala styrlogiken blir ett attraktivt mål för angripare.
Läs hela rapporten

Biometriska metoder för teknisk bevakning

Ta del av rapporten skriven av **Henrik Karlzén, Christian Valassi, Johan Bengtsson och Amund Gudmundson Hunstad** om biometriska metoder.

Rapporten beskriver vilka biometriska metoder som kan vara användbara för teknisk bevakning i Försvarsmakten.

Biometriska metoder utgår från mänskliga individers biologiska eller beteendebaserade kännetecken (exempelvis fingeravtryck eller gångstil) för att automatiskt känna igen individerna. Teknisk bevakning utgörs av teknik som används för övervakning och skydd i syfte att kontrollera egen personal och upptäcka antagonister. Vilka biometriska metoder som är användbara för Försvarsmakten utvärderades på två olika sätt. Den ena utvärderingen baserades på olika källors beskrivningar av de biometriska metoderna och hur väl metoderna fungerar teoretiskt eller i generella praktiska situationer (labbmiljöer). Källornas sätt att studera problemet varierar. Framförallt beaktar få av dem användningsmiljön, de igenkändas personliga integritet eller den biometriska metodens motståndskraft mot angrepp såsom imitering. Den andra utvärderingen bedömde hur väl metoderna fungerade i olika användningsfall som är representativa för Försvarsmakten och dess behov av teknisk bevakning. Det visade sig att de bästa och mest relevanta metoderna är igenkänning baserat på iris, fingeravtryck, ansikte respektive öron. Även dessa utvärderingar är dock gjorda på en ganska övergripande nivå. För specifika situationer och produkter behöver Försvarsmakten utvärdera ytterligare, inte minst för att jämföra med icke-biometriska alternativ. Det finns också rena forskningsmässiga utmaningar, exempelvis med att ta fram säkrare biometriska metoder där individer inte kan imiteras utifrån läckta databaser över biometriska data.
Läs hela rapporten

Resultat 20/20 CTF - En tävling i cybersäkerhet

FOI arrangerade i september 2020 en cybersäkerhetstävling kallad 20/20 CTF. Tävlingen genomfördes som en så kallad Capture The Flag (CTF), ett format som används för att bedöma deltagarnas färdigheter inom cybersäkerhet och hantering av IT-system.
Tävlingen genomfördes över internet och deltagarna fick via en webbportal tillgång till ett antal uppgifter som skulle lösas inom en viss tid. I varje uppgift fanns en flagga i form av en krypterad eller på annat sätt dold textsträng. Deltagarna tilldelades poäng genom att hitta flaggan och redovisa dess innehåll via webbportalen. Flest poäng när tiden hade laget watevr och stod därmed som vinnare. På andra plats kom laget LionHack och på tredje plats kom laget KTHCTF0x1. Läs mer om genomförandet i vårt **referat från tävlingen**.

20/20 CTF byggde på det så kallade Jeopardy-formatet, där varje uppgift innehåller en egen flagga. Uppgifterna varierade från nybörjarvänliga till avancerade och var fördelade i kategorierna Exploatering, Kryptografi, Reversering, Webb och Övriga.
Namnet 20/20 CTF är dels inspirerat av det år som den första upplagan genomfördes, dels en ordlek på den beskrivning av synskärpa som tagits fram av American Medical Association, 20/20 vision som ett mått på god syn. Det senare associerar till projektets uppgift om att använda CTF-formatet som en metod för att mäta deltagarnas kompetens inom cybersäkerhet.
20/20 CTF finansierades av Myndigheten för samhällsskydd och beredskap (MSB). Syftet med tävlingen var att bygga upp kunskap om CTF-formatet för att kunna nyttja det i framtida projekt. Exempel på framtida användning kan vara att verifiera kompetens vid rekrytering eller att väcka ett intresse för cybersäkerhet. Detta kan vara en metod för att tillgodose framtida kompetensbehov inom cybersäkerhet för det svenska totalförsvaret. FOI utvärderade hur den nationella **cyberanläggningen CRATE** kan nyttjas för att arrangera CTF-tävlingar samt hur tävlingsformatet kan anpassas för att inkludera industriella informations- och styrsystem.

Vad är CRATE?

Vid FOI i Linköping finns en av Europas första och största cyberanläggning. Anläggningen kallas för CRATE och utvecklas i samverkan mellan FOI, Försvarsmakten och Myndigheten för

samhällsskydd och beredskap. I CRATE emuleras komplexa IT-miljöer, samhällsviktiga styrsystem och cybersäkerhetsscenarier för att möjliggöra utbildning, träning, övning, demonstrationer, utvärdering och framtagande av ny kunskap för att utveckla totalförsvarets förmåga i cybermiljön. För att snabbt, korrekt och effektivt kunna skapa och underhålla miljöer och scenarier nyttjas i en hög grad av automatisering i CRATE.

Avancerad kurs i IT-incidenthantering (AKUT-Cyber)

Hur länge sedan är det som er IT-organisation fick öva på att hantera incidenter? Kommer ni att vara beredda nästa gång det händer?

Kursen ger en möjlighet att på ett realistiskt sätt få öka kunskapen och öva förmågan att hantera IT-incidenter.
Utbildningen sker i FOI:s cyberanläggning CRATE, en miljö som utvecklats med stöd av MSB och Försvarsmakten. Den används nu för bland annat studier av säkerhet i industriella informations- och styrsystem. I kursen AKUT-Cyber har ni möjlighet att öva i denna unika miljö.

Läs mer om kursen **AKUT-CYBER**
Är du intresserad och vill få mer information går det bra att ringa eller mejla Mikael Wedlin (kursansvarig) 013-37 80 96, **mwe@foi.se**

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

Kurs i Elektronisk säkerhet

Kursen är bred och behandlar många delar av elektronisk säkerhet, samtidigt som den ger möjlighet att träffa och diskutera med andra personer med liknande intressen. Kursen har genomförts två gånger per år sedan 2007 och den har genomgående varit mycket uppskattad. De senaste åren har tre kurstillfällen per år genomförts.

Är du intresserad och vill få mer information går det bra att ringa eller mejla Amund Hunstad (kursansvarig), 013 - 37 81 18, **amund.hunstad@foi.se**

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

Information via mejl om kursen Elektronisk säkerhet har tills nu distribuerats via en enklare mejllista. Avsikten är att framöver istället informera via detta mera ambitiösa nyhetsbrev tillsammans med andra informationssäkerhetsnyheter från FOI.

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.

Kurserna 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 Lars Westerdahl (kursansvarig), 013 - 37 80 32, **lars.westerdahl@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 Lars Westerdahl (kursansvarig), 013 - 37 80 32, **lars.westerdahl@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 2021

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