Cybersäkerhet för ökad konkurrenskraft

Slutredovisning

IVA
Kungl. IngenjörsVetenskaps Akademien

Innehåll

Förord

»Syftet med denna slutredovisning är att ge en sammanfattande bild av projektarbetet, förslagen och publika aktiviteter.«

I takt med att digitaliseringen blivit en förutsättning för verksamheter i alla delar av samhället blir cybersäkerhet allt viktigare. Sverige ligger i en internationell jämförelse långt fram när det gäller digitalisering. Men det finns ett glapp mellan tätpositionen och det faktum att vi ligger efter andra länder vad gäller förmågan att skydda oss mot cyberhot. Glappet måste slutas om Sverige ska kunna dra nytta av digitaliseringens alla fördelar.

Detta var bakgrunden till IVAs projekt *Cybersäkerhet för ökad konkurrenskraft*, som påbörjades i juni 2021 och avslutades i juni 2023. IVA har länge arbetat med digitaliseringsfrågorna, bland annat genom projektet *Digitalisering för ökad konkurrenskraft* där informationssäkerhet också var en viktig del. Inför starten av *Cybersäkerhet för ökad konkurrenskraft* utvecklade en grupp IVA-ledamöter, tillsammans med projektledningen, projektplanen som sedan förankrades hos viktiga intressenter och medfinansiärer inom akademi, näringsliv och offentlig sektor.

En styrgrupp och tre arbetsgrupper, med tillsammans ett 50-tal experter har arbetat i projektet. Den politiska referensgruppen med riksdagsledamöter från riksdagens åtta partier har följt hela projektet. En rad aktiviteter har genomförts, med svenska och internationella medverkande. De många publika evenemang projektet genomfört har fått stor uppmärksamhet.

I oktober 2022 presenterades projektets huvudrapport med förslag inom fem fokusområden. Därefter har implementeringsaktiviteter genomförts för att förankra och vidareutveckla några av områdena.

Syftet med denna slutredovisning är att ge en sammanfattande bild av projektarbetet, förslagen, publika aktiviteter och de många personer som har bidragit till projektets analyser, slutsatser och förslag.

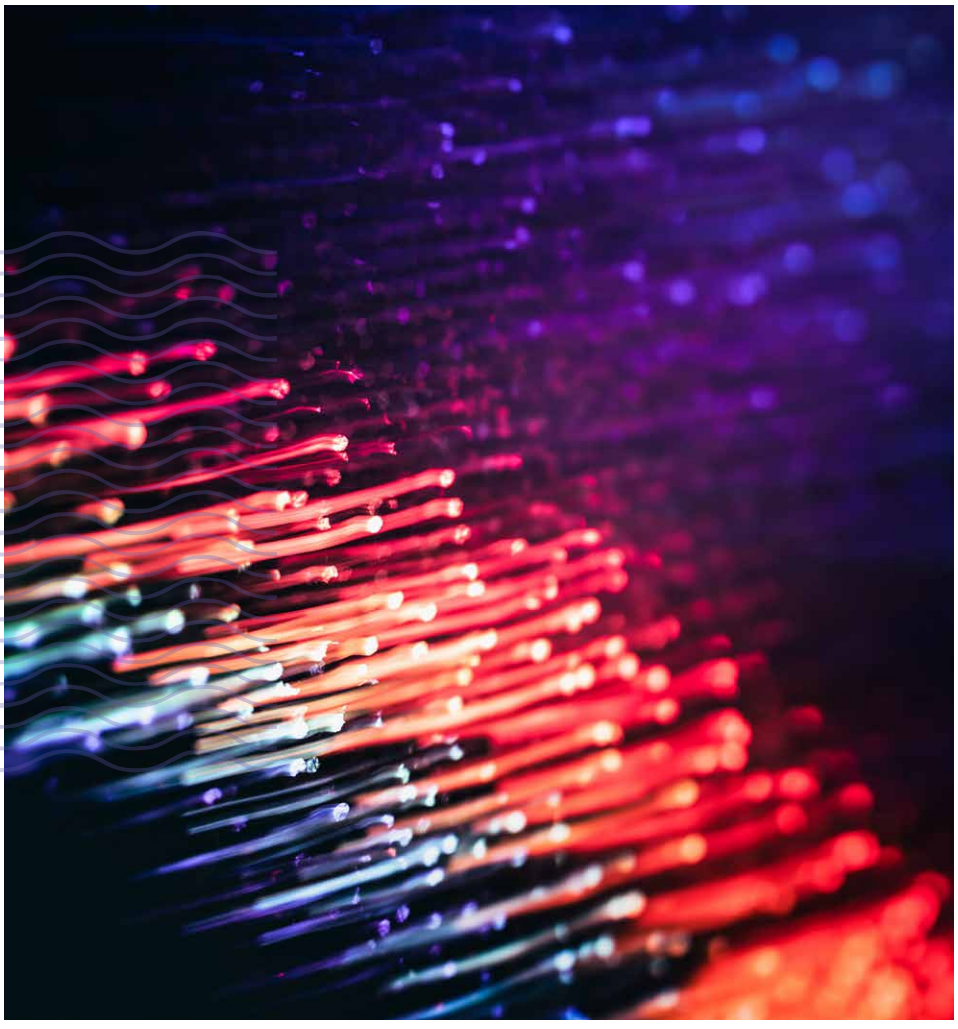
Stockholm i juni 2023

Håkan Buskhe, styrgruppens ordförande
Per Hjertén, huvudprojektledare

Styrgruppen för Cybersäkerhet för ökad konkurrenskraft
Håkan Buskhe, styrgruppens ordförande,
vd FAM AB, IVAs avd Maskinteknik
Anne-Marie Eklund-Löwinder, Amelsec,
IVAs avd Informationsteknik
Erik Ekudden, CTO Ericsson, IVAs avd Informationsteknik
Patrik Fältström, Säkerhetsskyddschef Netnod, IVAs avd Informationsteknik
Pontus Johnson, professor KTH, IVAs avd Elektroteknik
Lena Klasén, forskningsdirektör Polismyndigheten,
IVAs avd Informationsteknik
Hans Lindberg, vd Svenska Bankföreningen,
IVAs avd Ekonomi
Charlotte Lindgren, chef Cyberverksamheten FRA
Jan Nygren, IVAs avd Utbildning och forskning
Staffan Truvé, forskningsdirektör Recorded Future,
IVAs avd Informationsteknik

Projektledning
Per Hjertén, projektledare
Staffan Eriksson, delprojektledare
Eva Lagerblad, projektkoordinator
Jan Westberg, delprojektledare och kommunikationsansvarig

Finansiärer
Vinnova, FRA, FMV, Trafikverket, Svenska Bankföreningen, Ericsson, Saab, Internetstiftelsen, Teknikföretagen, SNUS (Swedish Network Users' Society)



Bestående brister i svensk cybersäkerhet

»Insikten om det nära sambandet mellan cybersäkerhet och konkurrenskraft är fortfarande för liten i Sverige.«

När IVA startade projektet *Cybersäkerhet för ökad konkurrenskraft* sommaren 2021 var en av utgångspunkterna en oro för att Sveriges cybersäkerhet är otillräcklig. Det faktum att många aktörer inom olika samhällsområden inte tog cybersäkerheten på tillräckligt stort allvar bidrog till oron.

I det närmaste alla delar av vårt samhälle är beroende av digitala system och är därmed möjliga måltavlor för cyberangrepp. I allt för många verksamheter leder dock inte detta till handling. Trots en rad incidenter går uppbyggnaden av ett effektivt cyberskydd, som kräver både tekniska och organisatoriska åtgärder, långsamt. Vi skulle aldrig acceptera storleken på de risker vi tar när det gäller cybersäkerhet inom andra områden som arbetsmiljö och trafiksäkerhet.

Att skydda sig mot cyberangrepp är en uppgift för både det militära och civila försvaret. Förutsättningarna för att lösa uppgiften har förändrats dramatiskt efter Rysslands angrepp på Ukraina. Våra satsningar på det militära försvaret har ökat mycket snabbt. Det behöver de också göra inom det civila försvaret, inte minst inom cybersäkerhetsområdet.

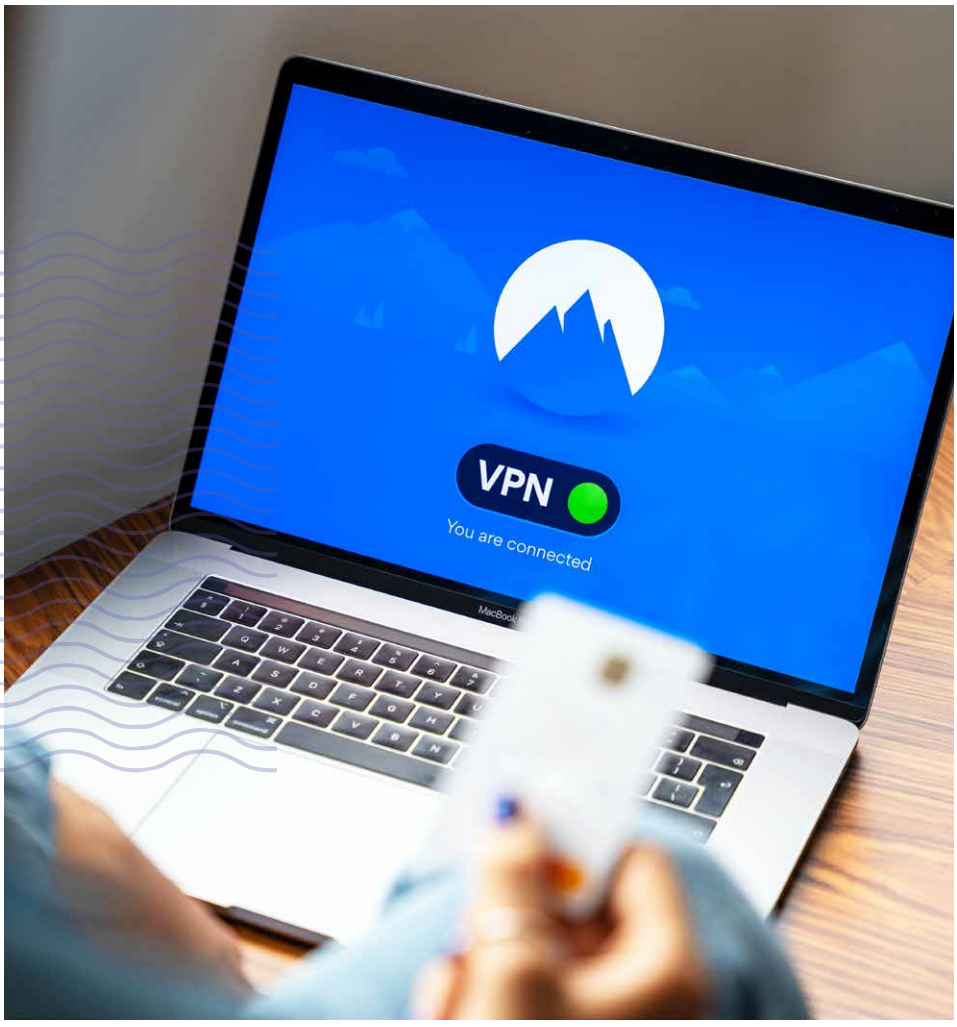
Ett krig så nära oss i Europa innebär en ovan situation för Sverige. Det ställer nya krav på politik, förvaltning och privata verksamheter. Besluts- och förnyelseprocesser måste gå snabbare, fienden och kriget väntar inte. Vi måste också snabbt öka satsningarna för att få till stånd en tillräckligt effektiv kompetensförsörjning med utbildade på både akademisk- och breddnivån.

I vår rapport från oktober 2022 jämförde vi Sveriges cybersäkerhetsarbete med en rad andra länders. Projektets slutsats var att vi har mycket att lära och låta oss inspireras av länder som Storbritannien, Frankrike, Finland, Norge och USA.

Insikten om det nära sambandet mellan cybersäkerhet och konkurrenskraft är fortfarande för liten i Sverige. På den nationella nivån handlar det om att i ett genomdigitaliserat land kunna garantera att vitala samhällsfunktioner klarar cyberangrepp. På företagsnivå påverkas ännu så länge inte värderingen av ett företags cybersäkerhet på samma sätt som bedömningen av dess hållbarhetsarbete. Men det kommer inte att dröja länge innan cybersäkerheten, genom dess påverkan på drift- och leveranssäkerhet, kommer att vara en variabel av stor vikt när marknaden bedömer ett företag.

Cybersäkerhet är en integrerad del av utvecklingen av digitala system och tjänster. Utbyggnaden av 5G och planeringen för 6G innebär helt nya möjligheter. Men den innebär också stora krav på att bygga in säkerhet från början i framtagningen av system, produkter och tjänster. Det förutsätter standarder.

För ett litet exportberoende land som Sverige med många stora internationella företag, är det viktigt med ett begränsat antal internationella standarder som gör det möjligt att använda teknik och system på olika delar av världsmarknaden. Därför är det oroande att protektionistiska tendenser och nationella särkrav gör att förutsättningarna för utveckling och användning av system kommer att begränsas. Det kommer att påverka Sveriges konkurrenskraft negativt.



Förslag inom fem områden

»I oktober 2022 presenterades projektets huvudrapport med förslag inom fem fokusområden.«

Område 1: Politisk styrning

FÖRSLAG

Ett cybersäkerhetsråd inrättas inom statsrådsberedningen. I rådets arbete deltar justitie-, försvars-, närings- och utrikesministrarna eller deras ersättare, cheferna för myndigheterna där cybersäkerhet ingår som del i deras huvudansvar. Till rådet knyts ett kansli.

Rådet ska ha till uppgift att:

- Följa upp och styra implementeringen av regeringens strategi för informations- och cybersäkerhet samt bereda eventuella förändringar av strategin.
- Tillse att myndigheternas verksamhet inom Nationellt cybersäkerhetscenter utformas på ett mer ändamålsenligt sätt för att få den verkanskraft som cybesäkerhetscenter i många andra länder har. Detta innebär bland annat kraftigt ökad personalstyrka och budget jämfört med idag.

Område 2: Effektivare utbyte och användning av information

FÖRSLAG

- Inrätta en gemensam plattform för informationsdelning i cyberdomänen med inspiration av den finska HAVARO där kommersiella aktörer samarbetar med Finlands cybersäkerhetscenter (TRAFICOM). Naturligt är att den bedrivs inom ramen för Nationellt cybersäkerhetscenter. Informationsdelningen bör ske utifrån ett strategiskt, operativt och taktiskt perspektiv.
- Uppmana branschorganisationer inom sektorer med samhällskritisk infrastruktur, att ta initiativ till och säkerställa kontinuiteten i olika ISAC, det vill säga förtroendebaserade plattformar för informationsutbyte.
- Ge MSB-enheten CERT-SE i uppdrag att ge tydliga råd utifrån svensk och internationell incidentrapportering. CERT-SE kan tillsammans med dem som råkat ut för angrepp föreslå åtgärder samt till vilka företag och organisationer informationen genom riktade insatser ska spridas för att förhindra att samma misstag upprepas.

FÖRSLAG

Inrätta en kommission som hanterar incidenter och "haverier" relaterade till cybersäkerhet. Kommissionen ska genom analys, diskussion, råd och rekommendationer skapa möjligheter för olika aktörer att dra nytta av erfarenheterna från inträffade cyberangrepp och de sårbarheter som upptäckts. Kommissionen ska bemannas av en kärna av fast anställda samt ett nätverk av experter och nyckelaktörer inom cybersäkerhetsområdet. Olika alternativ för huvudmannaskap och organisationsform är möjliga. Frågan om kriterier och regelverk för kommissionens arbete bör därför snabbutredas av en grupp bestående av företrädare för myndigheter och näringsliv.

Område 3: Operativ förmåga inom organisationer

FÖRSLAG

Vi föreslår att arbetet med en cybersäkerhetsnorm med det syfte, de grundkomponenter och egenskaper vi beskrivit i huvudrapporten, startas under 2022. Vår bedömning är att normen har förutsättningar att bli brett accepterad, och därmed på allvar fylla sin funktion, inom tre till fem år. Vi menar att det är naturligt att arbetet bedrivs inom ramen för Nationellt cybersäkerhetscenter.

Område 4: Forskning, innovation och kompetensförsörjning

FÖRSLAG

Vi stödjer det pågående arbetet med att inrätta ett nationellt cybercampus. Uppgiften ska vara att bedriva forskning, utbildning och stimulera innovation kring olika aspekter av hur den digitala infrastrukturen ska skyddas. Campuset ska vara en mötesplats för avnämarna i det svenska cyberekosystemet. Basen utgörs av ett antal samverkande universitet, forskningsinstitut och yrkeshögskolor. Företag är viktiga partners liksom myndigheter med uppgifter inom cybersäkerhetsområdet.

Centret bör finansieras av staten med bidrag från näringslivet. Den nödvändiga långsiktiga investeringsnivån ligger på flera hundra miljoner kronor per år.

Område 5: Mobilisering av resurser

FÖRSLAG

Inför en nationell övnings- och teststrategi med tillhörande ramverk för cyberdomänen. Övningar och tester bör ske utifrån ett brett spektrum av scenarier, inklusive simulering av extrema men troliga cyberangrepp. De bör också utformas för att kunna utmana både privata och offentliga verksamheter.

FÖRSLAG

Skapa en kompetenspool av frivilliga som kan bistå vid extraordinära situationer till följd av cyberangrepp. Kompetenspoolen kan organiseras som en del av de frivilliga försvarsorganisationerna för att garantera att lämplighets- och säkerhetsprövningar görs på ett systematiskt sätt.

FÖRSLAG

Initiera nationella incitamentsdrivna program av Bug Bounty-karaktär för granskning av sårbarheter som ett komplement till dagens penetrationstester och säkerhetsgranskningar. Programmet ska vara inriktat mot verksamheter inom samhällskritiska områden och initieras av centrala aktörer inom dessa.

Steg i rätt riktning – men mycket återstår och tempot är för lågt

»Det finns många positiva händelser och initiativ, som ligger i linje med de frågor projektet uppmärksammat och förslag vi lagt fram.«

Det finns all anledning att vara orolig för Sveriges cybersäkerhet och att nödvändiga förändringar inte sker tillräckligt snabbt. Men samtidigt är det viktigt att understryka att det finns många positiva händelser och pågående initiativ, som ligger i linje med de frågor vi uppmärksammat och förslag vi presenterade.

Det är naturligtvis omöjligt att slå fast hur projektet exakt påverkat de aktuella frågorna. Men IVA har, tillsammans med andra aktörer, bidragit i den pågående förändringsprocess vars nuläge, i juni 2023, vi beskriver nedan:

- **Ökad uppmärksamhet för cybersäkerhet**. Cybersäkerhetsfrågorna har fått större uppmärksamhet. De debatteras mer i media och vi ser nu regelbundet intervjuer med experter inom området med allt från ett säkerhetspolitiskt till ett företagsnära fokus. Bland andra Krigsvetenskapsakademien och Tech Sweden har, förutom IVA, kommit med rapporter som innehåller analyser och förslag.

- **Arbetet i Regeringskansliet**. En minister med ansvar för cybersäkerhet inom civilförsvarsområdet finns med i den nya regeringen. Denna har också tillsatt en nationell säkerhetsrådgivare vars uppdrag innefattar cybersäkerhetsfrågor.

- **Cybersäkerhetsstrategin**. Riksrevisionen har kritiskt granskat den svenska cybersäkerhetsstrategin och påpekat de stora brister som även IVA gjorde i projektets rapport. Detta har lett till åtgärder från regeringen som visar på ett större intresse för cybersäkerhet jämfört med tidigare regeringar, med olika partisammansättningar.

- **Cybersäkerhetscentrets** nuvarande konstruktion, som innebär att det inte är en egen juridisk enhet, försvårar verksamheten. Regeringen beslutade i april att centret ska bli en del av FRA. Det är nu upp till bevis för centret att det kan fylla samma viktiga funktion som sina motsvarigheter i exempelvis Storbritannien och Frankrike.

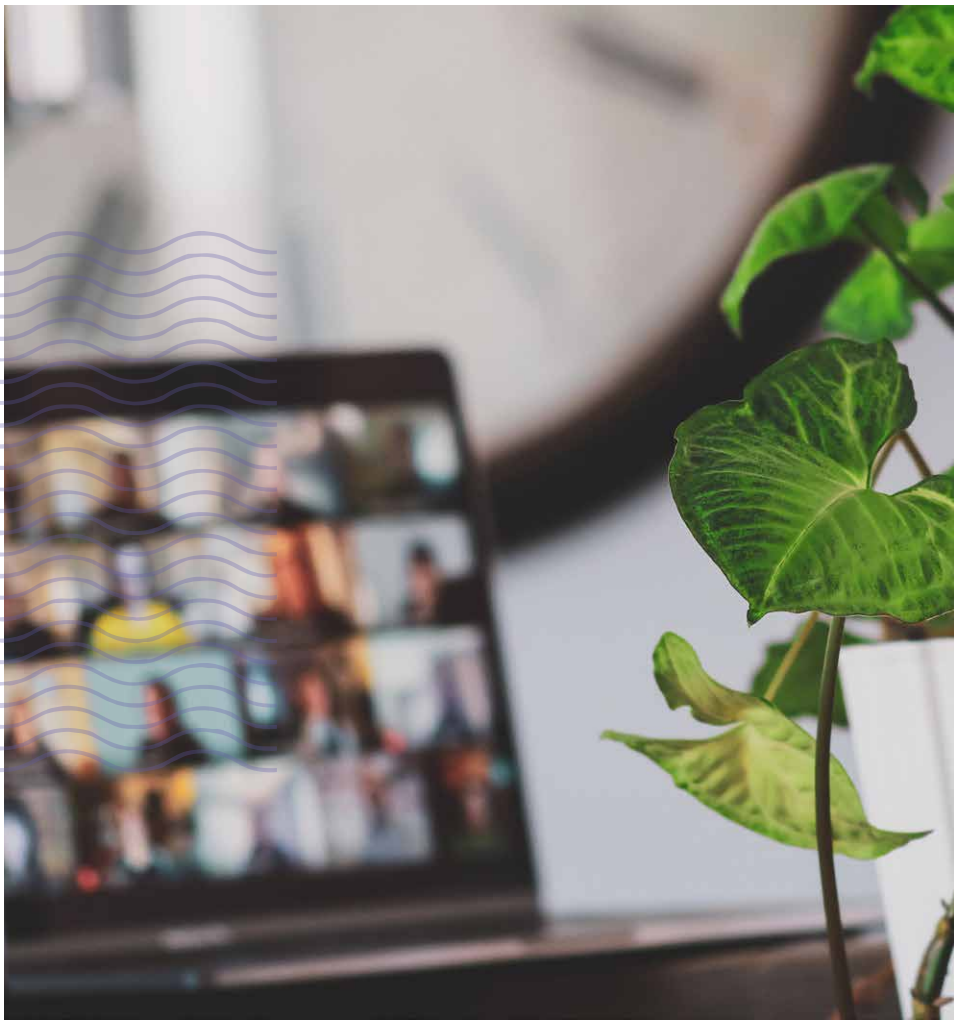
- **Dialogen mellan stat och näringsliv kring cybersäkerhet**. Regeringen offentliggjorde i en debattartikel i DN (2023-04-26) att det nationella cybersäkerhetscentrets organisatoriska hemvist blir FRA. Samtidigt underströk man att en viktig uppgift blir att förbättra dialogen med näringslivet. Förväntningarna är med rätta stora i denna fråga som är av så stor betydelse för Sveriges konkurrenskraft.

- **Cybersäkerhet håller långsamt på att bli en strategisk fråga**. Frågan börjar långsamt men bestämt gå från att ha varit en teknisk till att bli en strategisk fråga. Att konceptet security by design blir alltmer spritt är ett tecken på detta. Men medvetenheten och handlingsberedskapen i många delar av näringslivet och offentliga verksamheter är fortfarande för låg.

- **Cybercampus**. Från Vinnova har Cybercampus fått finansiering som täcker den inledande etableringsfasen. Under hösten 2023 förväntas vi oss att samarbetspartners kan börja anslutas, och att den allra första verksamheten kan komma till stånd. Ytterligare finansiering krävs för fortsättningen. I en debattartikel i Ny Teknik (2022-08-31) skrev nuvarande försvarsministern att Moderaterna vill säkra finansieringen för Cybercampus. Ännu återstår för regeringen att infria detta löfte.

- **Incidentrapportering**. Verksamheter med samhällskritisk verksamhet har skyldighet att rapportera cyberincidenter till MSB som kommer att öka sitt arbete med att återkoppla denna till uppgiftslämnarna.

- **Mobilisering av resurser** FRO (Frivilliga Radioorganisationen) fick under hösten 2022 i uppdrag från Försvarsmakten att utveckla verksamheten inom cyberförsvar och cybersäkerhet.



Aktiviteter och engagerade i projektet

Möten med projektets olika grupper

- Styrgruppen sammanträdde 15 gånger under perioden juni 2021 till juni 2023.
- Projektets tre arbetsgrupper sammanträdde cirka fem gånger per grupp under perioden november 2021 till april 2022.
- Deltagare från styrgrupp och arbetsgrupper träffades i två gemensamma arbetsmöten i februari och augusti 2022.
- Den politiska referensgruppen sammanträdde tre gånger under perioden september 2021 till oktober 2022.

Seminarier, event och övriga aktiviteter

September 2021

- Lanseringsseminarium 16 september med medverkan av projektdeltagare och riksdagspolitiker (blivande politisk referensgrupp). Drygt 200 deltog i seminariet. https://www.youtube.com/watch?v=Z9Z0vgS2Rmg

Oktober 2021

- Avstämningsmöten genomfördes med fokus på hot och lägesbild samt arbetsgruppernas uppdrag och projektets arbetssätt. Representanter från MSB, SKF, Avanza, Ericsson, Scania, SOFF (Säkerhets- och försvarsföretagen) och SNUS (Swedish Network Users Society) deltog.
- Projektet presenterades för CIO-nätverket inom IVAs Näringslivsråd.

November 2021

- Ett antal mindre avstämningsmöten genomfördes med representanter från Svenskt Näringsliv, Tech Sverige, Business Sweden i Österrike med flera.

December 2021

- Projektet medverkade vid Vinnovas/RISE samverkanskonferens tillsammans med ett tjugotal andra cybersäkerhetsrelaterade projekt finansierade av Vinnova.
- Projektet publicerade en sammanfattning av hot- och lägesbild som underlag för fortsatt arbete: https://www.iva.se/publicerat/ivas-cybersakerhetsprojekt-lanserar-hot--och-lagesbild

Februari 2022

- Presentation för projektets deltagare av EU-initiativen Cyber security act och ICT rolling plan – Johan Dahlgren, SIS medverkade.

Mars 2022

- Therese Naess, chef för NCSC (Nationellt Cybersäkerhetscenter) besökte projektets arbetsgrupp "Styrning, samverkan och ansvarsfördelning".
- Avstämningsmöte med Riksrevisionen angående deras planer på revision av hanteringen av Sveriges nationella cybersäkerhetsstrategi.

April 2022

- Presentation av projektet för CIO-nätverk för statligt ägda bolag.
- Presentation för projektets deltagare av Frankrikes nationella cybersäkerhetsarbete. Eric Lambert, partner och Head of Government Affairs på Victanis Advisory Services i Paris medverkade. En intervju med Eric L finns publicerad här: https://www.iva.se/publicerat/cybersakerhet-ur-ett-franskt-perspektiv

Maj 2022

- Projektet presenterades för RISE Cybernod – styrgrupp och referensgrupp.
- Projektet deltog i Cybercampus workshop.

Juni 2022
- Projektet presenterades för MSB:s informationssäkerhetsråd.
- Avstämningsmöte med NCSC om privat-offentlig samverkan.
- Presentation för projektdeltagare av representanter från det brittiska National Cyber Security Center https://www.ncsc.gov.uk

Augusti 2022
- Avstämningsmöte med representanter från MSB inför bildandet av nationellt kompetenscenter NCC-SE.
- Avstämningsmöten med fokus på nationell styrning och samordning av cybersäkerhetsfrågor med representanter för centrala myndigheter med ansvar inom cybersäkerhetsområdet: MSB, SÄPO, FRA, Polismyndigheten, FM+MUST, PTS, FMV.
- En delegation ur styrgrupp och projektledning besökte Tallinn och ett antal cybersäkerhetsrelaterade organisationer och myndigheter, däribland NATO CCDCOE, RIA + CERT EE, Ministry of Economic Affairs and Communications, CR14 och Estlands försvarsministerium medverkade.

Oktober 2022
- Rapportseminarium den 18 oktober på IVA med presentation av projektets huvudrapport inkl. ett antal förslag till åtgärder för förbättrad cybersäkerhet:
  - Seminariet kan ses här: https://www.iva.se/det-iva-gor/tidigare-evenemang/cybersakerhet-for-okad-konkurrenskraft
  - Rapporten finns tillgänglig här: https://www.iva.se/publicerat/kraftsamling-kravs-for-att-mota-cyberhot/
- Projektet deltog i Cybercampus workshop.
- Presentation av projektet på FSPOS (Finansiella Sektorns Privat-offentliga samverkan) seminarium med fokus på samverkan och övning- och test.

November 2022
- Projektet deltog i Cybercampus workshop.
- Presentation i riksdagen med ett 40-tal riksdagsledamöter anordnat av RIFO (Föreningen Riksdagsledamöter och Forskare).

December 2022
- Seminarium med IVA Syd i Lund om projektets teman.
- Presentation av projektet på IVAs seminarium för RIFO med cirka 100 gäster varav flertalet riksdagsledamöter.

Januari 2023
- Seminarium om Digital Forensik tillsammans med Digital Forensics Sweden: https://www.youtube.com/watch?v=A4_P7W0xJok
- Projektet deltog i samverkanskonferens med RISE Cybernod och ett 30-tal andra cybersäkerhetsprojekt finansierade av Vinnova, SSF och MSB.
- Avstämningsmöte med Haverikommissionens generaldirektör John Ahlberk och hans kollega.

Februari 2023
- Seminarium med IVA Väst i Göteborg om cybersäkerhet i vården. https://www.youtube.com/watch?v=yCuGF-aWJjc
- Avstämningsmöte med FROs (Frivilliga Radioorganisationen) generalsekreterare Fredrik Färnqvist och hedersordförande Ulf Johansson.
- Besök hos RISE Cybernode och Cyber range. Informationsmöte med chefen för centrum för cybersäkerhet och hans kollega.
- Nationell säkerhetsrådgivare Henrik Landerholm besökte projektets styrgrupp.
- Ministern för civilt försvar Carl-Oskar Bohlin besökte IVA.

Mars 2023
- Presentation av projektet för Vinnovas personal.
- Projektet anordnade rundabordssamtal om möjligheterna att införa Bug Bounty-program inom svensk offentlig sektor.

April 2023
- Webbinarium med presentation av AstaZeros verksamhet och cybersäkerhetsrelaterade aktiviteter.

Maj 2023
- Seminarium i Luleå tillsammans med IVA Nord och Norrlandsfonden om cybersäkerhet hos små och medelstora företag.

- Seminarium i Linköping tillsammans med nätverket Cyberly Linköpings Science Park och Kista Science City om cybersäkerhet hos små och medelstora företag.
- Seminarium på IVA i Stockholm med anledning av projektets avslut: https://www.iva.se/det-iva-gor/tidigare-evenemang/cybersakerhet--vad-kravs-for-att-sakra-konkurrenskraften/

Om projektet

IVAs projekt Cybersäkerhet för ökad konkurrenskraft startade i juni 2021 och avslutades i juni 2023. Projektets leddes av en styrgrupp som inledningsvis beslutade om den plan som innehåller projektets mål, syfte och arbetsprocess.

Stora delar av det operativa projektarbetet har bedrivits i tre arbetsgrupper. Dessa har rapporterat till, och fått återkoppling från, styrgruppen. Den politiska referensgruppen, som består av riksdagsledamöter från riksdagens åtta partier, har interagerat med projektet i arbetsmöten.

Styrgrupp

Håkan Buskhe, FAM AB (styrgruppens ordförande)
Erik Ekudden, Ericsson
Patrik Fältström, Netnod
Pontus Johnson, Kungliga Tekniska Högskolan (KTH)
Lena Klasén, Polismyndigheten
Hans Lindberg, Svenska Bankföreningen
Charlotte Lindgren, Cyberverksamheten
Försvarets radioanstalt (FRA)
Anne-Marie Eklund-Löwinder, Amelsec
Jan Nygren, ledamot IVAs avdelning
för Utbildning och forskning
Staffan Truvé, Recorded Future

Arbetsgrupper

Styrning, samverkan och ansvarsfördelning
Hans Lindberg, Svenska Bankföreningen (ordförande)
Johan Andersson, Trafikverket
Annika Avén, Säkerhets- och försvarsföretagen (SOFF)
Peter Göransson, Svenska Bankföreningen
Karl Lallerstedt, Svenskt Näringsliv
Mats Nilsson, Ericsson AB
Mats Nordqvist, Teracom Group
Jan Nygren, ledamot IVAs avdelning
för Utbildning och forskning
Margareta Palmqvist, Myndigheten
för samhällsskydd och beredskap (MSB)
Amanda Renström, Försvarsmakten
Fredrik Sand, TechSverige
Carl Fredrik Wettermark, Utrikesdepartementet (UD)
Jan Westberg, IVA (delprojektledare)

System, teknik och beteenden
Patrik Fältström, Netnod (ordförande)
Kristina Blomqvist, Vattenfall
Fredrik Börjesson, Militära underrättelse-
och säkerhetstjänsten (MUST)
Thomas Dahlbeck, Internetstiftelsen
Magnus Danielson, Swedish Network Users' Society (SNUS)
Daniel Fäldt, Saab
Magnus Jacobson, Svenska Bankföreningen
Ulrik Janusson, Scania CV
Lena Klasén, Polismyndigheten
Camilla Lundahl, Avanza
Peter Lorincz, SKF
Simin Nadjm-Tehrani, Institutionen för datavetenskap,
Linköpings universitet
Mats Nilsson, Ericsson AB
Jan Smith, Swedish Network Users' Society (SNUS)
Staffan Truvé, Recorded Future AB
Per Hjertén, IVA (projektledare)

Kunskap och kompetensförsörjning
Pontus Johnson, Kungliga Tekniska Högskolan, KTH
Nils Alenius, Säkerhetspolisen
Annika Andreasen, Svenska institutet för standarder (SIS)
Martin Bergling, Research Institutes of Sweden (RISE)
Anne-Marie Eklund Löwinder, Amelsec AB
Arvid Kjell, Försvarets Radioanstalt (FRA)
Eva Listi, Systembolaget
Patrik Sandgren, Teknikföretagen
Tommy Schönberg, Vinnova
Mikael Schönström, Försvarets Materielverk (FMV)

Daniel Wengelin, Saab
Staffan Eriksson, IVA (delprojektledare)

Politisk referensgrupp
Åsa Eriksson (S)
Margareta Fransson (MP)
Hanna Gunnarsson (V)
Pål Jonsson (M)
Caroline Nordengrip (SD)
Micael Oscarsson (KD)
Niels Paarup-Petersen (C)
Allan Widman (L)

Projektledning

Per Hjertén, projektledare
Staffan Eriksson, delprojektledare
Eva Lagerblad, koordinator
Jan Westberg, delprojektledare, kommunikationsansvarig

Kungl. Ingenjörsvetenskapsakademien är en fristående akademi med uppgift att främja tekniska och ekonomiska vetenskaper samt näringslivets utveckling. I samarbete med näringsliv och högskola initierar och föreslår IVA åtgärder som stärker Sveriges industriella kompetens och konkurrenskraft. För mer information om IVA och IVAs projekt, se IVAs webbplats: www.iva.se.

Utgivare: Kungl. Ingenjörsvetenskapsakademien (IVA), 2023
Box 5073, SE-102 42 Stockholm
Tfn: 08-791 29 00

IVA-M 544
ISSN: 1100-5645
ISBN: 978-91-89181-43-4

Projektledning: Per Hjertén, Staffan Eriksson, Jan Westberg, IVA
Redaktör: Jan Westberg, IVA
Layout: Pelle Isaksson, IVA

Denna slutredovisning finns att ladda ned på www.iva.se

Kungl. IngenjörsVetenskaps
Akademien