Cybersäkerhet för ökad konkurrenskraft

IVA
Kungl. Ingenjörs Vetenskaps Akademien

Innehåll

Förord

»Projektet vill bidra till diskussionen om ett starkt och samordnat arbete för att stärka Sveriges cybersäkerhet och konkurrenskraft.«

I takt med att digitaliseringen blivit en förutsättning för verksamheter i alla delar av samhället blir cybersäkerhet allt viktigare. Sverige ligger i internationell jämförelse långt fram när det gäller digitalisering. Men det finns ett glapp mellan denna tätposition 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.

Hotaktörer attackerar dagligen vårt samhälle. För att möta dessa krävs både teknik i framkant och organisatorisk effektivitet. Det behövs också en bred kunskap hos beslutsfattare inom näringsliv och offentlig sektor om cyberhoten och möjligheterna att hantera dessa.

Syftet med projektet *Cybersäkerhet för ökad konkurrenskraft* är att bidra till en bred och nyanserad diskussion om vikten av ett starkt och samordnat arbete för att stärka Sveriges cybersäkerhet. Denna rapport är en del i detta arbete. Vårt fokus är hur nivån på Sveriges cybersäkerhet påverkar konkurrenskraften för svenskt näringsliv och samhället i stort. Vi lägger också fram förslag vars gemensamma nämnare är att de ska bidra till ett effektivare arbete med cybersäkerhet i näringsliv och offentliga verksamheter.

IVAs styrka som en oberoende aktör är att engagera individer med stor kompetens och erfarenhet inom de områden akademien arbetar. Ett femtiotal personer har medverkat i de workshopar och seminarier projektet genomfört samt i de tre arbetsgrupper som arbetat med cybersäkerhet ur olika perspektiv: *Styrning, samverkan och ansvarsfördelning, System, teknik och beteenden* samt *Kunskap och kompetensförsörjning*. Jag vill tacka er alla för ert stora engagemang.

Rapportens analyser och förslag bygger till stor del på underlagen från de tre arbetsgrupperna. Men styrgruppen ensam ansvarar för rapportens innehåll.

Jag vill framföra ett varmt tack till medlemmarna i styrgruppen för deras stora engagemang och bidrag till rapporten. Som i alla IVA-projekt medverkar medlemmarna i sin personliga kapacitet och inte som företrädare för organisationerna där de är verksamma.

Projektet pågår fram till sommaren 2023. Lanseringen av rapporten är inledningen till en rad seminarier, möten och andra aktiviteter runt om i landet. Vi ser fram emot att möta dig i dessa sammanhang – Sverige behöver en nyanserad och faktabaserad diskussion om cyberhot och cybersäkerhet.

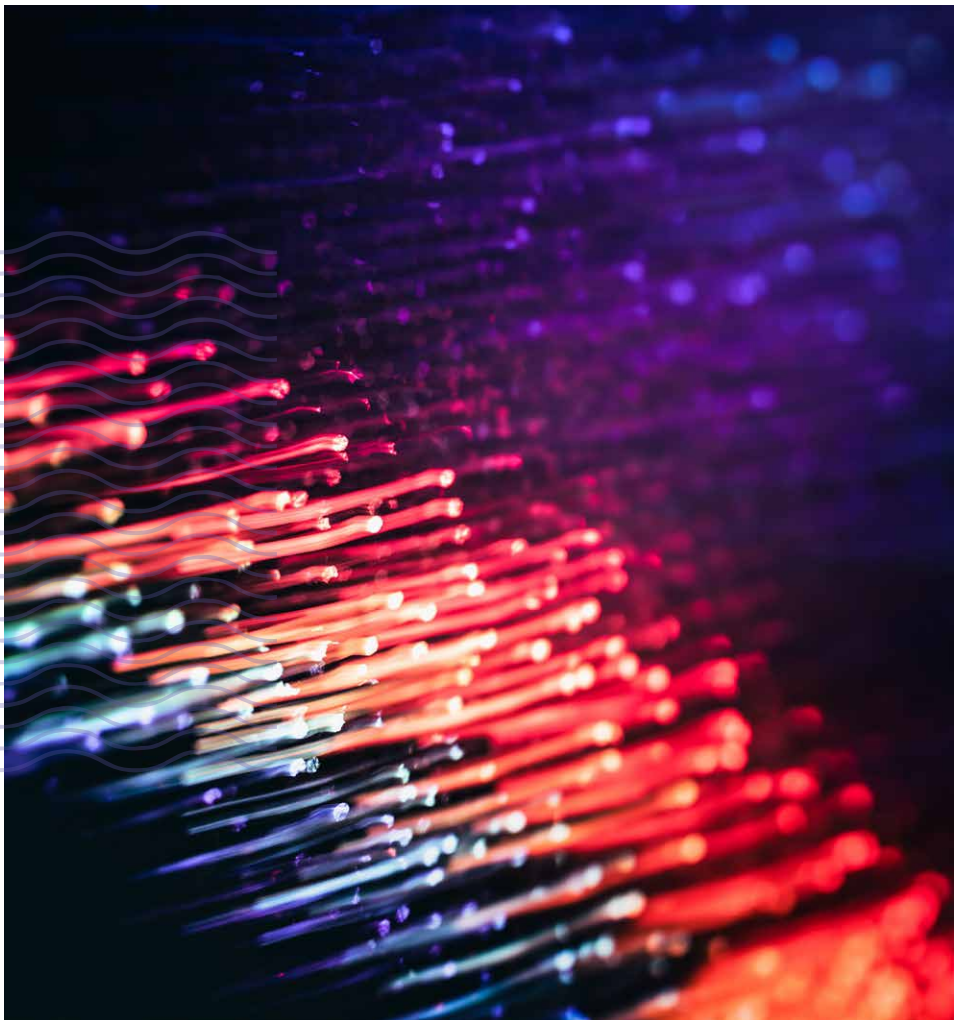
Stockholm i oktober 2022

Håkan Buskhe, styrgruppsordförande

Styrgruppen för Cybersäkerhet för ökad konkurrenskraft, oktober 2022
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)



Sammanfattning

IVA har sedan juni 2021 drivit projektet *Cybersäkerhet för ökad konkurrenskraft*. Denna rapport sammanfattar arbetet och projektets förslag. Vårt fokus är cyberhot och den cybersäkerhet som krävs för att möta hoten. Syftet är att lägga fram förslag som kan öka Sveriges cybersäkerhet och därmed vår konkurrenskraft.

Med digitaliseringen följer nya sårbarheter, där effekterna av cyberangrepp tillhör de största hoten. Förmågan att hantera cybersäkerhetsfrågor är central för Sveriges konkurrenskraft, både för näringslivet och samhället i stort. Svenska företag utvecklar världsledande, högteknologiska produkter för den globala marknaden inom en rad områden."Security by design", det vill säga förmågan att bygga in säkerhet under hela livscykeln, är fundamental för produkternas konkurrenskraft.

Samspelet mellan politik och näringsliv ger viktiga förutsättningar för näringslivet. Därför är konkurrenskraften sedd ur ett samhällsperspektiv viktig för företagen. Exempel på områden där politiska beslut och initiativ på samhällsnivå påverkar cybersäkerhetsarbetet och därmed företagens konkurrenskraft är kompetensförsörjning, lagstiftning, utbyggnad av vital och säker infrastruktur samt förmågan att anpassa och ompröva regelverk i takt med den tekniska utvecklingen.

För att effektivt hantera cybersäkerhetsfrågor inom en nation krävs samordnade åtgärder och initiativ från politik, myndigheter, näringsliv och andra delar av samhället. Det gäller inom områden som lagstiftning, myndighetsutövning och FoU. Internationell reglering och lagstiftning på EU-nivå har stor påverkan på detta arbete.

I Sverige drivs cybersäkerhetsarbetet ambitiöst och många gånger effektivt i olika delar av cyberekosystemet. Men vår slutsats är att det finns mycket att lära av andra länder som arbetat längre och mer fokuserat med implementeringen av cybersäkerhetsstrategier. Det gäller områden som politisk styrning, ansvarsfördelning och samverkan mellan myndigheter och näringsliv samt större nationella satsningar på forskning och kompetensförsörjning.

Vår slutsats är att Sverige inte är tillräckligt rustat för att möta cyberhoten:

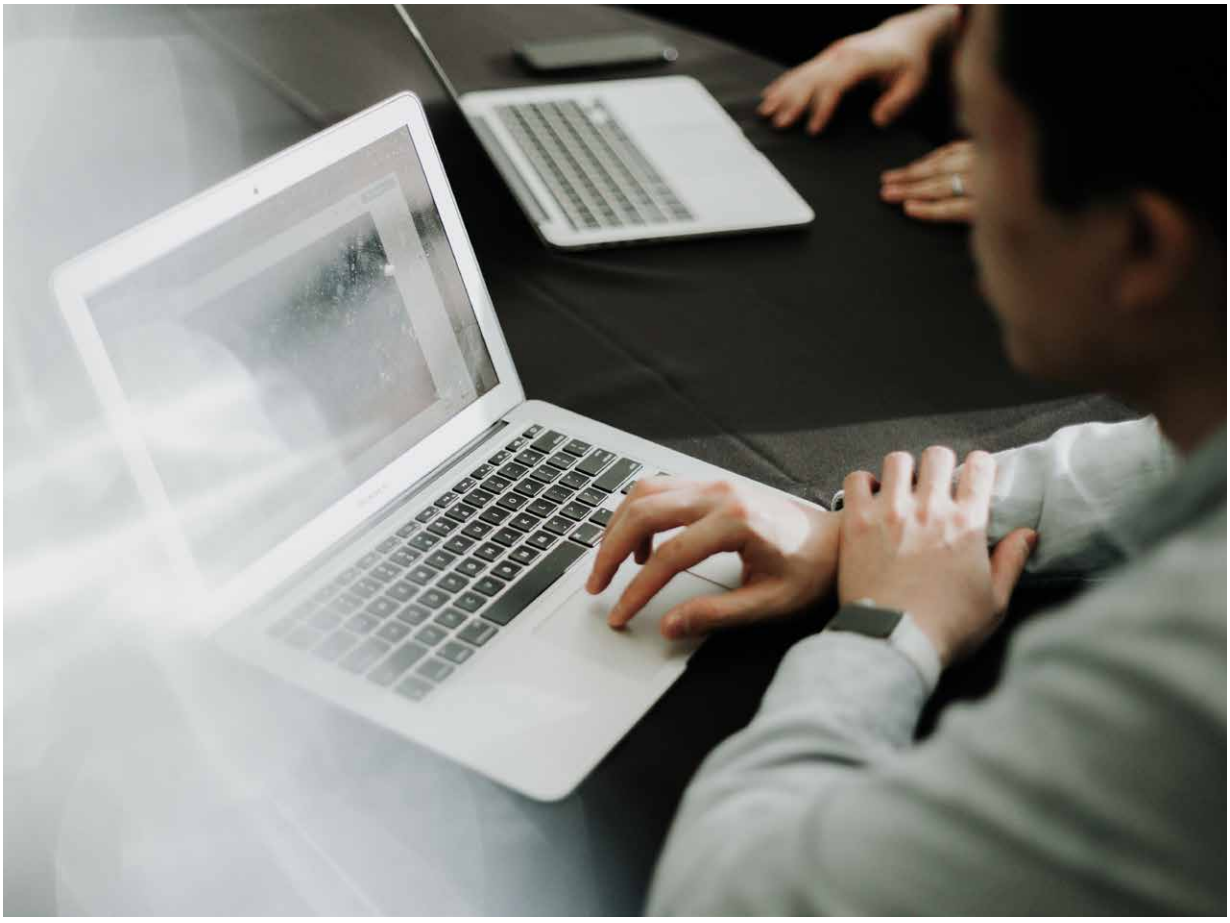
- Vi tar inte cyberhoten på tillräckligt stort allvar.
- Det brister i insikterna om sambandet mellan cybersäkerhet och konkurrenskraft.
- Samarbetet mellan privata företag och statliga aktörer kring cybersäkerhet är inte tillräckligt.
- Vår beslutskraft på central politisk nivå är inte tillräcklig för att möta cyberhoten som ökar och förändras i snabb takt.
- Vi klarar inte kompetensförsörjningen inom cybersäkerhetsområdet.
- Vi förbereder och kraftsamlar inte tillräckligt.

I projektets tre arbetsgrupper och styrgrupp har vi identifierat fem nyckelområden. Inom dessa lägger vi fram förslag till åtgärder för att stärka Sveriges cybersäkerhet och konkurrenskraft:

- **Politisk styrning på nationell nivå behöver förbättras.** Därför föreslår vi att ett cybersäkerhetsråd inrättas inom statsrådsberedningen. Uppgiften ska vara att följa upp och utveckla den nationella cybersäkerhetsstrategin samt tillse att myndigheternas

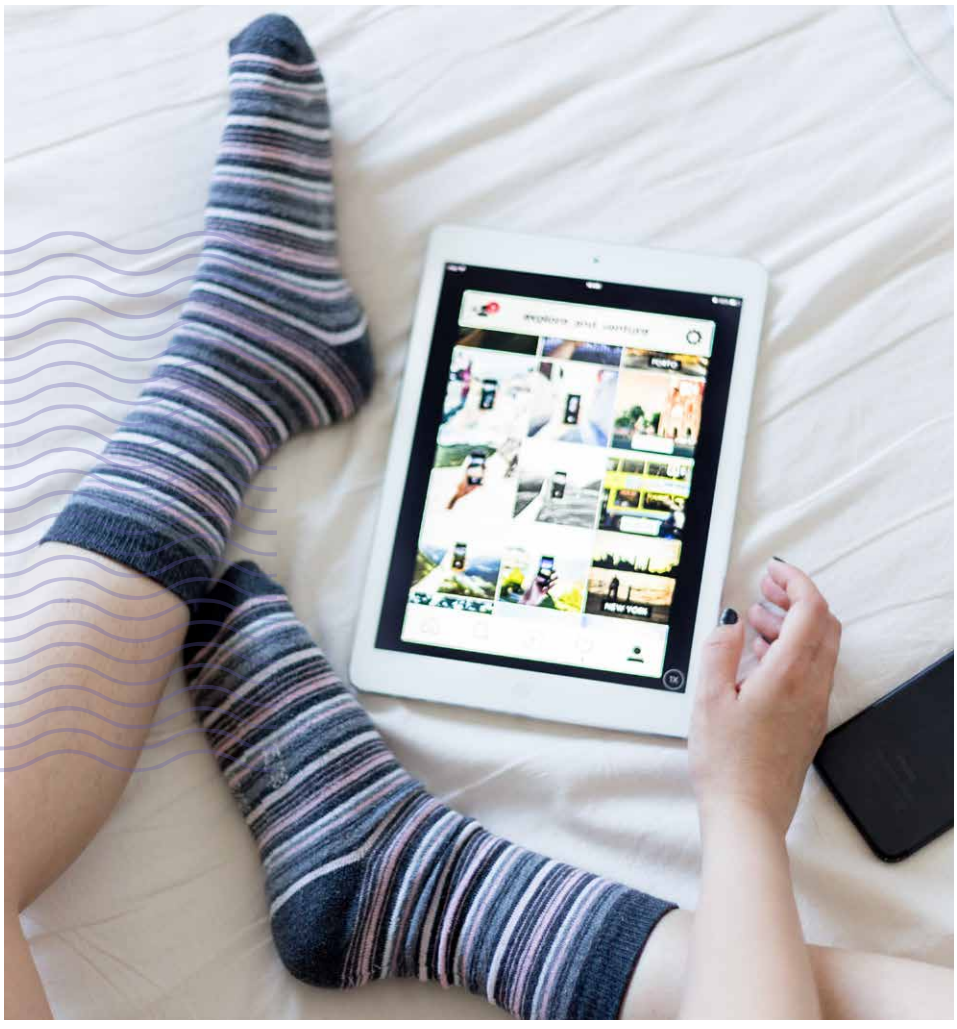
verksamhet inom det Nationella cybersäkerhetscentret utformas på ett ändamålsenligt sätt.

- **Utbytet och användningen av information behöver förbättras.** Vi föreslår fyra åtgärder för att göra detta: en gemensam plattform för informationsdelning i cyberdomänen att stimulera branschorganisationer att ta initiativ till och säkerställa kontinuiteten i olika ISAC (Information Sharing and Analysis Centers) samt att MSB-enheten CERT-SE får i uppdrag att ge tydliga råd utifrån de incidentrapporter som kommit in. Vi föreslår även att en haverikommission för cyberincidenter inrättas.
- **Den operativa förmågan inom organisationer behöver stärkas.** Vi föreslår därför att det Nationella cybersäkerhetscentret får i uppdrag att samordna arbetet med att ta fram en nationell cybersäkerhetsnorm med syftet att bli en nationell modell för att hantera cybersäkerhet. Syftet med normen är att vara ett stöd, inte minst för styrelser och ledningar, genom konkreta verktyg och principer så att det blir ”lätt att göra rätt”.
- **Forskning, innovation och kompetensförsörjning.** Sverige behöver kraftsamla för att klara



kompetensförsörjningen, inte minst av spets-kompetens, inom cybersäkerhetsområdet. Det finns också ett behov av breda bildnings- och utbildningsinsatser. Som ett led i att möta en del av dessa behov föreslår vi att ett nationellt cybercampus inrättas. Uppgiften ska vara att bedriva forskning, utbildning och stimulera innovation kring olika aspekter av hur den digitala infrastrukturen ska skyddas. Centret ska även bidra till att säkerställa att kompetens inom "security by design" finns tillgänglig i Sverige så att näringslivet kan utveckla produkter som är konkurrenskraftiga på en global marknad.

- **Mobilisering av resurser.** Fler aktörer behöver mobilisera sina resurser för att hantera och förebygga incidenter. Vi föreslår att en nationell övnings- och teststrategi med tillhörande ramverk för cyberdomänen upprättas, att en kompetenspool av frivilliga som kan bistå vid extraordinära situationer till följd av cyberangrepp skapas samt att ett nationellt incitamentsdrivet Bug Bounty-program initieras för samhällskritiska verksamheter.



En ny verklighet

»I den nya verkligheten är digitalisering detsamma som att utsätta sig för cyberhot. Alla delar av det svenska samhället är potentiella måltavlor för cyberangrepp.«

Vårt samhälle är digitaliserat. Utvecklingen har accelererat under de senaste två årtiondena. Därmed har förutsättningarna för verksamheter i alla samhällssektorer förändrats. Det innebär många nya möjligheter för individer, företag och välfärd. Men det innebär också risker.

I denna rapport ligger vårt fokus på cyberhot och den cybersäkerhet som krävs för att möta hoten. Syftet är att lägga fram förslag som kan öka Sveriges cybersäkerhet och därmed konkurrenskraften. Det gör vi på sidan 26 och framåt.

Under projektets arbete med att ta fram förslagen har frågor rests från olika håll om probleminsikten – vår sense of urgency – kring cyberhot och cybersäkerhet är tillräcklig i Sverige. Oron har gällt om tillräckligt många i ledande positioner inom politik, myndigheter och näringsliv inser situationens allvar. Efter de många diskussioner och möten vi haft i projektet delar vi denna oro.

Vi menar att vi måste förstå att i den nya verkligheten är digitalisering detsamma som att utsätta sig för cyberhot. Vi måste också inse att alla delar av det svenska samhället är potentiella måltavlor för cyberangrepp. Visserligen görs det ett gott arbete kring cybersäkerhet inom många myndigheter och företag. Men det krävs mer. Vi måste orka se sanningen i vitögat – cybersäkerhetskejsaren i Sverige är bara halvklädd. Vi menar att tre utgångspunkter är nödvändiga för att nå denna insikt:

1. Digitalisering innebär att utsätta sig för cyberhot

Årsrapporterna från Säkerhetspolisen, Militära underrättelsetjänsten och Försvarets radioanstalt visar att cyberangreppen på Sverige ökar i antal och att de är bredare och mer komplexa än tidigare (SÄPO 2022, MUST 2022, FRA 2022). Detta är en del av en internationell utveckling. Den ansedda amerikanska tankesmedjan Council of Foreign Relations beskriver utvecklingen av internet:

Verkligheten har sprungit om den ursprungliga visionen om ett öppet, pålitligt och säkert globalt nätverk. Idag är internet mindre fritt och mer fragmentariserat. Länder runt om i världen, speciellt auktoritära regimer, ökar sin kontroll över internet genom att spåra data, blockera och moderera innehåll samt genomföra kampanjer för att påverka den politiska utvecklingen i andra länder. Delar av internet – dark web – är marknadsplatser för brott och utpressning (Fick m.fl. 2022).

2. Alla delar av det svenska samhället är potentiella måltavlor för cyberangrepp

Större delen av det svenska samhället använder sig av digitala system. Det innebär att de är potentiella mål för de cyberangrepp som är en vardagsrealitet. Kungl. Krigsvetenskapsakademien konstaterar i sin rapport *Svensk säkerhetspolitik i ofärdstider* att vi redan idag är i elektronisk och kognitiv strid med främmande makter. Visserligen befinner vi oss i ett fredstillstånd, men situationen gör att vi måste rusta och förbereda oss utifrån denna krigsliknande situation (Lundin m.fl. 2022, KKRvA 2022).

3. Sverige är inte tillräckligt rustat för att möta cyberhoten

I vårt arbete har vi gjort ett antal observationer:

- **Vi tar inte cyberhoten på tillräckligt stort allvar.** Vi är attackerade av främmande makt. Många samhällskritiska verksamheter är regelbundet utsatta för cyberangrepp. Samtidigt som vi tar risken för stora skogsbränder på allvar, förbereder oss och drar lärdom av tidigare misstag, arbetar vi inte på samma systematiska sätt när det gäller cybersäkerhet.

- **Vi förbereder och kraftsamlar inte tillräckligt.** Många myndigheter och företag gör viktiga insatser inom olika delar av cybersäkerhetsområdet. Men för att få effekt måste samordning och samverkan bli bättre. Den är inte tillräcklig idag och vi måste anstränga oss mer.

- **Vår beslutskraft på central politisk nivå är inte tillräcklig för att möta cyberhoten vilka ökar och förändras i snabb takt.** Utvecklingen av digital teknik går mycket snabbt. Även cyberhoten utvecklas i hög takt. Detta ställer krav på att de politiska besluten sker med hänsyn till den realitet de snabba förändringarna innebär. Sverige lever inte upp till dessa krav idag. Vi påverkar och deltar inte heller i tillräcklig grad i de för Sverige så viktiga politiska processerna inom EU.

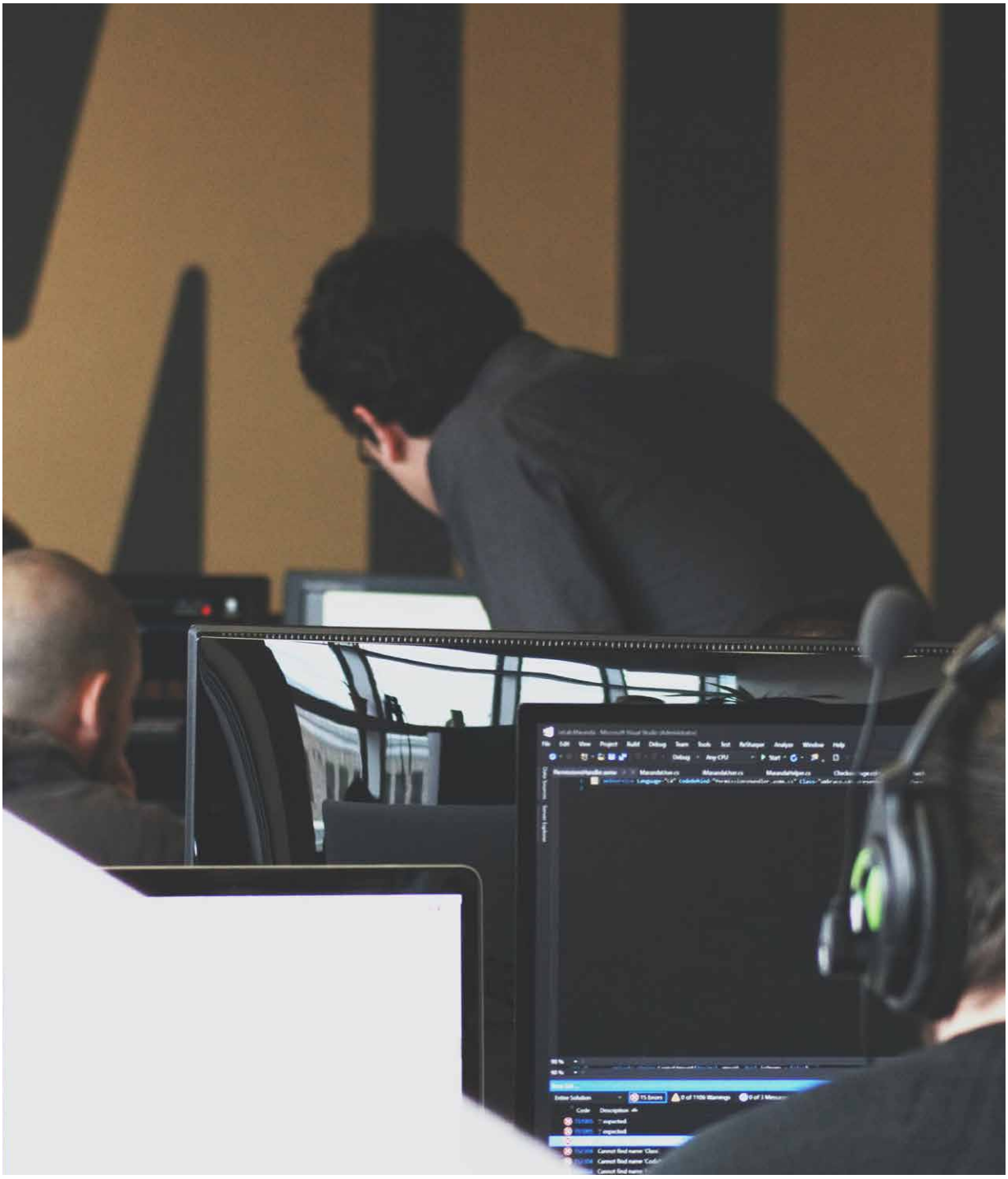
- **Det brister i insikterna om sambandet mellan cybersäkerhet och konkurrenskraft.** Cybersäkerhet har en mycket stor påverkan på konkurrenskraften, både på företags- och samhällsnivå. När ett företag som väljer var investeringar ska göras, är en god nationell cybersäkerhet lika viktigt som företagsklimat, effektiv lagstiftning och ett väl fungerande rättssystem. Dessutom finns en marknadsekonomisk aspekt där en större kompetens vid offentliga upphandlingar leder till en marknad med bättre produkter, förbättrad cybersäkerhet och därmed ökad konkurrenskraft.

- **Samarbetet mellan privata företag och statliga aktörer kring cybersäkerhet är inte tillräckligt.** Fundamentet för vår digitala infrastruktur är ett statligt regelverk som anger ramarna för de många privata aktörer som verkar på olika nivåer inom infrastrukturen. IVA har beskrivit denna som ”Lasagnemodellen” med många nivåer och aktörer (IVA 2019). Den bristande insikten om potentialen i detta samarbete påverkar negativt våra företags och därmed vårt samhälles konkurrenskraft. Den försvårar därmed för svenska växande företag inom cybersäkerhetsbranschen.

- **Vi klarar inte kompetensförsörjningen inom cybersäkerhetsområdet.** Det råder brist på kompetens inom hela IT-sektorn och därmed också inom cybersäkerhetsområdet (SOU 2021:63). Vi saknar den spetskompetens som är nödvändig om Sverige ska ha ambitionen att ha världsledande företag inom cybersäkerhet. Vi utbildar inte tillräckligt många inom universitet och högskola, satsar för lite och hittar inte nya former för att vidareutbilda personer med yrkeserfarenhet. Högre kompetens i Sverige ger nödvändiga förutsättningar för att hantera cyberhot bättre och ställa högre krav på produkter och tjänster på både kort och lång sikt.

- **Cybersäkerhet kommer in för sent i produktutvecklingen.** Ett flertal svenska företag utvecklar världsledande produkter för den globala marknaden inom flera högteknologiska områden såsom sjukvård, elförsörjning, tunga fordon, telekommunikation och försvar. Cybersäkerhetsaspekter måste komma in tidigt i produktutvecklingen som ofta påbörjas fem år innan lanseringen av en produkt eller tjänst. Till exempel pågår redan idag utveckling av nästa generations mobilkommunikation, 6G.

- **Andra länder arbetar snabbare och bättre med cybersäkerhet än Sverige.** Det gäller allt från central politisk nivå, samverkan mellan myndigheter till hur näringslivet engageras. Sverige har ett lägre tempo i beslutsfattande och implementering än andra länder som har samma höga digitaliseringsgrad som vårt land. Vi har mycket att lära av exempelvis Estland, Frankrike, Storbritannien och våra nordiska grannländer. Men vi gör det i alldeles för liten utsträckning. I för hög grad är vi oss själva nog. Det är en ohållbar attityd.



Hot och sårbarheter

Hotbilden kring cybersäkerhet är under ständig förändring. Det är en följd av hur aktiva olika hotaktörer är, hur de förändrar sina metoder och kapacitet för att göra cyberangrepp. Sverige tillhör de länder som har en mycket hög digitaliseringsgrad. Vår förmåga att hantera cybersäkerhetsfrågor är central för konkurrenskraften ur ett företags- och samhällsperspektiv.

SÅRBARHETER OCH METODER FÖR CYBERANGREPP

Gemensamt för de flesta hotaktörer är att de utnyttjar olika typer av sårbarheter i IT-systemen som exempelvis:

- Brister i behörighetshantering
- Undermålig IT-arkitektur
- Programkod av låg kvalitet
- Avsaknad av rutiner för underhåll och uppdatering av programvara
- Brister i konfiguration
- Anslutning av icke godkänd programvara

Trots att många sårbarheter är kända sedan länge fortsätter de att utnyttjas framgångsrikt och i stor omfattning. Detta visar att cybersäkerhet handlar om mer än teknik. Styrning och ledning av organisationers säkerhetsarbete brister ofta till följd av låg medvetenhet och kunskap om cyberhoten. Rutiner för säkerhetsarbetet saknas och åtgärdsplaneringen är bristfällig.

Okända sårbarheter kallas zero-day-sårbarheter. Dessa utgörs av nya sårbarheter i system som en hotaktör upptäcker och som kan utnyttjas fram till de åtgärdas. Hotaktörer handlar sinsemellan med zero-day-sårbarheter ofta med mäklare som mellanhand.

Lösenordsbaserade cyberangrepp är en vanlig metod för angrepp. Hotaktören kan antingen utnyttja de typer av sårbarheter som beskrivits ovan för att komma åt lösenord, eller köpa tillgång till redan läckta sådana.

En annan metod är att helt enkelt ringa upp användare och utge sig för att vara supportpersonal. Man kan också få tillgång till IT-system genom att rekrytera en person på insidan av organisationen.

Det mänskliga beteendet utnyttjas också för att angriparen ska kunna dra nytta av tekniska sårbarheter. Vanliga tillvägagångssätt är att dela ut USB-minnen eller skicka epost, ofta med länk till en falsk webbsida. Syftet är att användaren ska installera programvara med skadlig kod eller lämna ut inloggningsuppgifter. Bredare epostbaserade angrepp kallas phishing eller nätfiske. Är de riktade till speciella grupper eller enstaka individer benämns de spear phishing eller riktat nätfiske.

Angriparen kan också använda sig av spionerі för att lura till sig lösenord eller annan strategisk information.

Källa: Beskrivningen av sårbarheter och metoder för cyberangrepp bygger på översikter från NCSC (2020), och RISE (2022).

HOT OCH HOTAKTÖRER

Hotaktörerna kan delas in i statliga, kriminella, ideologiskt motiverade samt hobbyhackare. Den gemensamma nämnaren i de flesta cyberangrepp är att angriparen tar sig in i ett IT-system. Väl där arbetar de för att identifiera fler sårbarheter och skaffa sig utökad behörighet. Därefter kan hotaktörerna stjäla data, modifiera eller lägga till skadlig kod som exekveras vid en bestämd tidpunkt. Överbelastningsattacker är en annan typ av angrepp. Målet är då att överbelasta systemet utan att ta sig in i det. Exempel på detta är svenska banker som under de senaste tio åren drabbats av överbelastningsattacker.

Statliga
Statliga hotaktörer är ofta en del av en nations underrättelse- eller säkerhetstjänst. Deras uppgift är att uppfylla nationella säkerhetspolitiska intressen, bland annat genom att påverka politiska processer i andra länder. Sanktioner och handelshinder försvårar traditionella affärsrelationer inom vilka teknikutbyte är en del. Om ett sådant inte är möjligt på legal väl ökar incitamenten för cyberangrepp för att komma åt resultat och innehåll i FoU och IP.

De statliga hotaktörerna har stora resurser som ger förmåga till hög aktivitetsnivå under en längre tid. Kategorin kallas ibland Advanced Persistent Threats (APT). Den svenska säkerhetslagstiftningen är inriktad mot att skydda landet mot statliga hotaktörer.

Kriminella
Kriminella hotaktörer vill på enklaste sätt tjäna maximalt med pengar. Ibland kan de agera på uppdrag av statliga hotaktörer. Då blir det svårare att avgöra om en kriminell hotaktör agerar på eget eller andras initiativ.

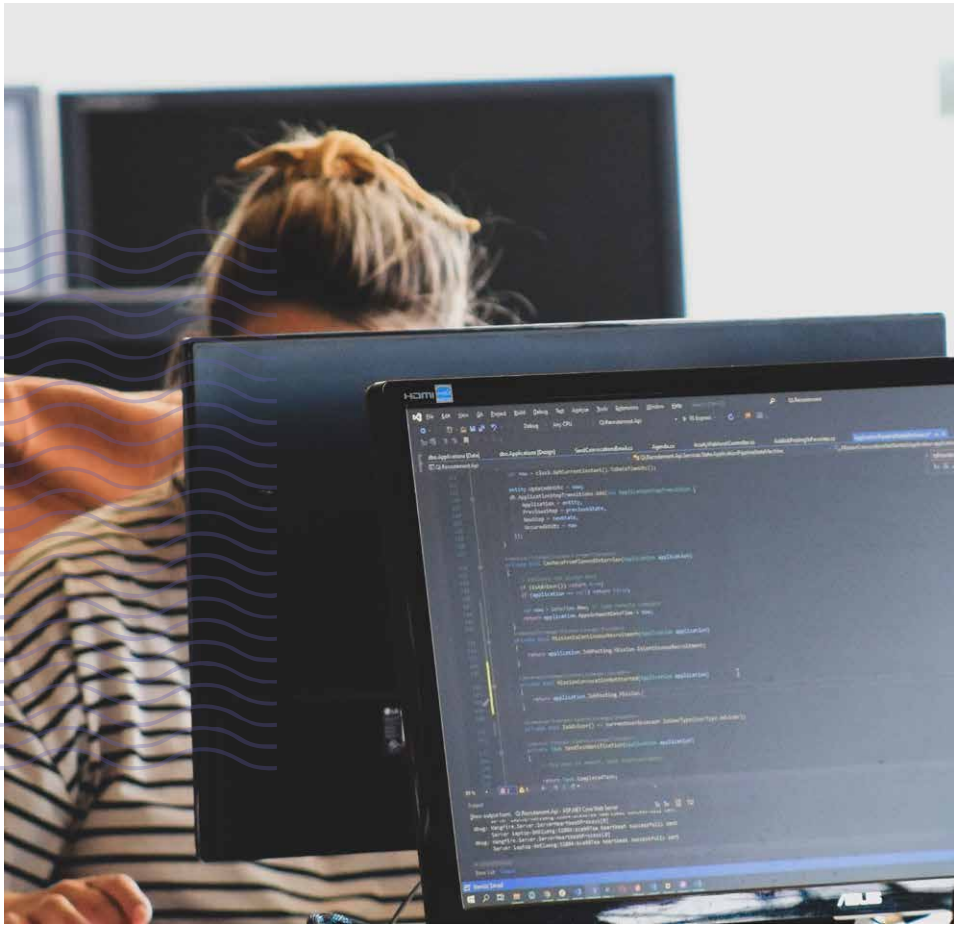
Jämfört med de statliga hotaktörerna är de kriminella mindre sofistikerade och använder i regel existerande, välbeprövade metoder. Men de utgör ofta allvarliga hot mot företag genom att de utnyttjar system som används vid angreppen på ett avancerat och uthålligt sätt.

För de kriminella hotaktörerna spelar det liten roll om målet för attackerna är ett privat företag, en myndighet eller annan organisation. De slår helt enkelt mot de mål där risken för upptäckt är låg. Rena stölder av pengar, information, identiteter samt bedrägerier är vanliga. Låsning av system och information, följt av krav på lösensumma riktade mot globala tjänster och digitala leverantörskedjor har visat sig lönsamma och därför ökat i omfattning.

Ideologiskt motiverade
Ideologiskt motiverade hotaktörer agerar utifrån egna agendor för att nå ut med sitt budskap. De kan manipulera opinionsbildningen för att exempelvis påverka inför ett val. De kallas ibland hacktivister och kan ha terrorkopplingar. De ideologiskt motiverade hotaktörerna består av allt från organisationer till enstaka individer. Deras resurser och förmågor varierar kraftigt.

Hobbyhackare
Denna kategori hackar därför att det helt enkelt är roligt eller för att imponera på vänner. Sedan länge har denna kategori av aktörer varit viktiga. På 1990-talet hette den mest kända gruppen Cult of the Dead Cow. Under 2022 har gruppen Lapsus$ figurerat i nyhetsflödet efter att ha hackat företag som Microsoft, Nvidia, Samsung och Okta.

Källa: Beskrivningen av hot- och hotaktörer bygger på översikter från NCSC (2020), och RISE (2022).



Cybersäkerhet och konkurrenskraft

»Sverige har en mycket hög digitaliseringsgrad. Vår förmåga att hantera cybersäkerhetsfrågor är därmed avgörande för konkurrenskraften ur både ett företags- och samhällsperspektiv.«

Sverige tillhör de länder som har en mycket hög digitaliseringsgrad (DESI 2022). Vår förmåga att hantera cybersäkerhetsfrågor är därmed avgörande för konkurrenskraften ur både ett företags- och samhällsperspektiv.

I ett *företags- och branschperspektiv* ligger fokus på hur effektivt företagen producerar och säljer sina varor och tjänster. I detta perspektiv har Sverige en stark konkurrenskraft. Denna bygger på att en stor del av vår BNP kommer från företag med framskjutna positioner på globala marknader, där de många gånger är världsledande. Svenska företag utvecklar världsledande produkter inom flera högteknologiska områden som sjukvård, elförsörjning, fordon, telekom och försvar.

Ett företags konkurrenskraft påverkas av förmågan att hantera cyberhot mot den egna verksamheten. I samma takt som hoten ökat, har effektiviteten i cybersäkerhetsarbetet blivit allt viktigare i den finansiella marknadens värderingar av företag. Cybersäkerhetsfrågor är därför i högsta grad en angelägenhet för ägare, ledning och styrelse (ISC2 2018).

Ett företags konkurrenskraft påverkas i hög grad av den miljö de verkar i. Samspelet mellan politik och näringsliv ger därmed viktiga förutsättningar för verksamheten. Därför är konkurrenskraften sedd ur ett *samhällsperspektiv* väsentlig för företagen. Denna bestäms av kvalitet och leveransförmåga inom områden som skola, högre utbildning och forskning, infrastruktur, boende och levnadsmiljö, kultur, villkor för företagande samt kapacitet och kvalitet i offentlig sektor (IVA 2015).

Vi kan idag se områden där politiska beslut och initiativ på samhällsnivå påverkar viktiga områden för cybersäkerhetsarbetet och därmed företagens konkurrenskraft:

- Det råder stor brist på kompetens inom hela IT-området. Detta gäller inte minst den spetskompetens som behövs för att Sverige ska kunna behålla sin internationellt starka ställning inom sektorn. Staten ansvarar för den högre utbildningen. Hittills har universitet och högskolor inte utbildat tillräckligt många med rätt kompetens inom området. Man har heller inte utnyttjat de möjligheter yrkeshögskolorna ger (Tech Sverige 2020).

- Lagstiftning och regeltillämpning ger förutsättningarna för lösningar på företagsnivå inom cybersäkerhetsområdet. Men staten kan också påverka genom upphandlingar och gemensamma projekt. Sverige har en historia av samarbeten mellan stat och näringsliv som framgångsrikt bidragit till utvecklingen av exempelvis telekom- och försvarsindustrierna (IVA 2015). Idag är förutsättningarna annorlunda genom EUs konkurrenslagstiftning. Men andra länder utnyttjar på ett bättre sätt de möjligheter att stimulera företag inom cybersäkerhetsområdet som regelverket faktiskt ger. Detta påverkar vår konkurrenskraft negativt (Tech Sverige 2022).

- Utbyggnaden av vital digital infrastruktur går inte tillräckligt snabbt. Sverige är sena i 5G-utbyggnaden.

TEKNISK UTVECKLING INOM CYBERSÄKERHETSOMRÅDET – ROLLFÖRDELNINGEN MELLAN POLITIK OCH NÄRINGSLIV

Teknik och produktutveckling inom IT-området, där cybersäkerhet är en del, är global och drivs till allra största delen av privata företag. Branschen är stor och omsätter betydligt mer än USAs hela försvarsbudget (SIPRI 2022, The Business Research Company, 2022).

Avgörande för att en marknad ska fungera effektivt är en tydlig och fungerande rollfördelning mellan marknadsaktörer och regulatorer, i en nation eller inom ramen för internationella avtal. Exempelvis ställer EUs NIS-direktiv krav på säkerheten i nätverk. Reglerna omfattar leverantörer av samhällsviktiga tjänster och vissa digitala tjänster. Dessa leverantörer kan verka både inom privat och offentlig sektor. EUs Cyber Security Act (som rör cyberssäkerhetscertifiering av produkter och tjänster) tar fram valideringsscheman för utrustning inom kritisk digital infrastruktur. Figur 1 nedan visar rollfördelningen mellan kravställare på internationell och nationell nivå och de privata marknadsaktörerna som omsätter kraven i system och teknik.

Dagens komplexa digitala system kan inte skyddas med enbart skalskydd, eftersom ett sådant aldrig kan nå upp till en hundraprocentig säkerhetsnivå. Ytterligare en anledning är att komplexa system alltid innehåller delsystem, programvaror och komponenter vars säkerhet av olika skäl inte kan garanteras fullständigt. Attacker kan även komma inifrån skalskyddet. Ett antal av världens största cyberattacker har skett via bakdörrar i mjukvara från betrodda leverantörer. Förutom skalskydd på olika nivåer måste systemen därför innehålla inbyggda säkerhetsfunktioner som kan avslöja och agera på cyberattacker som initierats inifrån. Ytterst handlar det om att varje informationsöverföring, internt och externt, måste säkras var för sig.

Detta koncept brukar kallas zero trust och innebär att systemets olika delsystem, programvaror, komponenter och användare har olika krav på säkerhetslösningar inom varje nivå, vilket man kallar en trust stack.

Rätt tillämpat kan detta angreppssätt skapa hög säkerhet trots att inte alla tiotusentals ingående delar kan vara hundraprocentigt säkrade. Konceptet trust stack måste tillämpas redan under tidiga stadier av produkters och tjänsters utveckling (även kallat security by design) och kräver att industrin har god tillgång till spetskompetens inom cybersäkerhet.

Vi ligger idag långt under EU-snittet (18 procent jämfört med 66 procent) vad gäller 5G-täckning i befolkade områden (DESI 2022). Detta skadar konkurrenskraften och påverkar cybersäkerheten negativt eftersom avancerat cyberskydd är inbyggt i de nya näten. En förklaring till att vi ligger efter är långsam ärendehantering hos myndigheter och formulering av säkerhetskraven. Avvägningen i dessa processer mellan säkerhet och företagens möjligheter att dra nytta av den nya tekniken påverkar vår konkurrenskraft.

- Globala nät ger möjlighet att driva verksamheter på många platser inte minst genom olika molntjänster.

Detta ger nya förutsättningar för svenska internationella företag. Samtidigt pågår en alltmer omfattande politisering med protektionistiska förtecken i frågor med anknytning till användningen av molntjänster och dataflöden. Det gäller såväl på nationell svensk nivå som inom EU och USA (Fick m.fl. 2022). Avvägningen mellan generella cybersäkerhets- och specifika företagsintressen påverkar därmed direkt företagens konkurrenskraft. Den påverkas även av politikens förmåga att anpassa olika regelverk när nya tekniska lösningar förändrar förutsättningarna inom IT-området.

Figur 1: Schematisk bild över marknadsdynamiken och relationerna mellan marknaden och staten. I Sverige genomför regeringen sin politik genom myndighetsutövning. Bilden visar myndigheter med särskilt ansvar inom cybersäkerhetsområdet och Nationellt cybersäkerhetscenter med sin samverkansuppgift. Utöver dessa finns fler myndigheter med särskilt ansvar inom cybersäkerhetsområdet, till exempel Finansinspektionen, Energimyndigheten, Svenska Kraftnät, Inspektionen för vård och omsorg och Länsstyrelsen.

Svenskt cybersäkerhetsarbete i ett europeiskt perspektiv

»I Sverige drivs cybersäkerhetsarbetet ambitiöst och effektivt i enskilda delar av ekosystemet. Men samordningen är svagare, liksom för andra delar av digitaliseringen.«

För att hantera cybersäkerhetsfrågor effektivt inom en nation krävs åtgärder och initiativ från politik, myndigheter, näringsliv och övriga delar av samhället. Det gäller områden som lagstiftning, myndighetsutövning, FoU och säkerhetsarbetet inom företag.

Vi kan tala om ett ekosystem för cybersäkerhet där samspelet mellan och effektiviteten i olika delar av systemet avgör hur framgångsrikt en nations samlade arbete är. Avgörande är om rollfördelningen mellan olika aktörer är tydlig. Förmågan att hitta gemensamma prioriteringar och kraftsamla kring dessa måste också vara stor. De nationella cybersäkerhetsstrategiernas utformning och implementering spelar en viktig roll i detta arbete.

I Sverige drivs cybersäkerhetsarbetet ambitiöst och många gånger effektivt i enskilda delar av ekosystemet. Men samordningen är svagare, liksom för andra delar av digitaliseringen (IVA 2019). För att bedöma vår nivå och identifiera möjliga förbättringar är det viktigt att jämföra med länder som har liknande förutsättningar som Sverige vad gäller digitaliseringsgrad, demokratiskt styrelseskick och legala förutsättningar i form av EU-medlemskap eller nära anknytning till EU.

Länder som Finland, Frankrike, Nederländerna och Storbritannien har kommit långt när det gäller att bygga upp ett effektivt ekosystem kring cybersäkerhet. Många delar av samhället är engagerade. Rollfördelningen mellan politik och näringsliv är tydlig och samverkan utvecklad. Riktade satsningar på forskning och utbildning görs för att säkerställa behovet av spets- och breddkompetens. Frågan om att hantera risker när komponenter och system från globala marknader används adresseras. Erfarenheter från cyberangrepp analyseras och tas tillvara.

Strategierna

Sverige presenterade 2017 *Nationell strategi för samhällets informations- och cybersäkerhet* (Skr 2016/17:213) som sträcker sig fram till 2023. Uppföljning sker i första hand genom att involverade myndigheter årligen redovisar sina handlingsplaner utifrån strategin och hur dessa uppfylls. Någon samlad uppföljning av strategin görs inte.

Områden med anknytning till Försvarsmakten, Polisen och andra statliga myndigheter med relevans för cybersäkerhetsarbetet dominerar. Näringslivet har en mer undanskymd roll.

Andra europeiska länder har arbetat med cybersäkerhetsstrategier betydligt längre än Sverige. Norge är inne på sin fjärde och Storbritannien på sin tredje. Finland fick sin första strategi 2013. Strategierna i sin helhet utvärderas mer regelbundet än i Sverige. I Nederländerna sker det varje år (SOU 2021:63).

Fokuset i de andra ländernas strategier är, jämfört med Sverige, bredare och täcker mycket mer än operationella samhällskyddsfrågor. Storbritanniens strategi är ett bra exempel på detta. Den syftar till att säkerställa samhällets utveckling i en säker och digitaliserad värld. Viktiga delar av strategin är samverkan med näringslivet, ambitioner kring tekniskt ledarskap och suveränitet, konkurrenskraft i ett internationellt marknadsperspektiv, geopolitik och allians-frågor samt handel och innovation. Detta påverkar självklart prioritering av insatser när strategin ska implementeras (National Cyber Strategy 2022).

Politisk styrning

I Sverige är ansvaret för cybersäkerhetsfrågor uppdelat mellan flera departement med tillhörande myndigheter. Samordningen är svag, vilket till en del förklaras av den svenska förvaltningsmodellen. (Detta är bakgrunden till ett av de förslag vi presenterar, se förslaget om ett cybersäkerhetsråd på sidan 28). Vi har heller inte en utpekad enhet som representerar Sverige internationellt i cybersäkerhetsfrågor. I flera andra länder fyller cybersäkerhetscentret eller ett departement denna funktion (SOU 2021:63).

Det politiska ansvaret kring cybersäkerhetscentren är tydligare i andra länder. I Norge är ansvaret uppdelat i detalj mellan olika departement. I Storbritannien och Frankrike finns motsvarande uppdelning mellan olika ministrar och departement. Dessa länder har stora departement och tillämpar ministerstyre, vilket ger andra förutsättningar än Sveriges förvaltningsmodell. I Nederländerna har ett departement, och därmed minister, huvudansvaret. Samma sak gäller för Estland där departementet med ansvar för ekonomi och kommunikation har det politiska ansvaret (SOU 2021:63).

Cybersäkerhetscenter

Många europeiska länder har ett cybersäkerhetscenter. Men mandat, resurser och utformning skiljer sig från Sverige.

Det svenska cybersäkerhetscentret är under uppbyggnad. Det är ingen egen juridisk person utan har formen av en samarbetsarena för de myndigheter som ingår, FRA, Försvarmakten, MSB och SÄPO. Någon utarbetad praxis för hur denna samverkan ska ske eller hur frågor där de deltagande myndigheterna har olika uppfattningar ska hanteras finns inte i dagsläget. Det operativa arbetet kring cybersäkerhetsfrågor utförs fortfarande inom ramen för varje myndighets verksamhet. I uppbyggnadsskedet är relativt få personer knutna till centret på heltid. Planerna är att antalet personer som arbetar inom ramen för centret ska vara uppemot 100 år 2023 (NCSC.se).

Förutsättningarna för cybersäkerhetscenterna i många andra länder är radikalt annorlunda. Bemanningen är jämfört med Sverige betydligt större och för många planeras utökningar av antalet medarbetare. I Storbritannien har National Cyber Security Center över 1000 anställda och franska ANSSI har 600 och ska öka till 750 (ANSSI 2021). Tyska BSI skall växa från 1350 till över 2100 anställda (BSI 2022) och nederländska NCSC-NL har 200 medarbetare, ett antal som ska öka. Finland har idag cirka 100 anställda.

Den politiska styrningen och centrets uppgifter skiljer sig från den svenska. I Frankrike rapporterar ANSSI direkt till premiärministern. I Storbritannien är National Cyber Security Center underställt regeringen. Nederländernas nationella cybersäkerhetscenter NCSC-NL är en separat myndighet under justitie- och säkerhetsministeriet.

Mandat och uppgifter är också betydligt större. Exempelvis NSCS-NL i Nederländerna är det centrala organet för information och expertkunskaper. Det har en nyckelroll på operativ nivå vid större IT-kriser där cyberhot är en del. Centret samlar även in och sprider information om identifierade cyberhot och attacker. Det är också den internationella kontaktpunkten i cybersäkerhetsfrågor (NCSC-NL, 2019). Storbritanniens NCSC har motsvarande mandat och uppgifter.

Näringslivets engagemang

Kritik har riktats mot att näringslivet inte involveras tillräckligt i Sveriges cybersäkerhetsarbete på nationell nivå (SOFF m.fl., 2020). I cybersäkerhetsstrategin har näringslivet en relativt liten plats, jämfört med exempelvis Försvarsmakten, Polisen och andra statliga myndigheter.

I många andra länder har näringslivet en mer central roll och är en integrerad del i cybersäkerhetsstrategierna. I Norges aktuella strategi är ett prioriterat område att stärka samarbetet mellan privat och offentlig sektor (SOU 2021:63).

Näringslivet är också, jämfört med Sverige, engagerade på en helt annan nivå och med mycket större intensitet i olika delar av cybersäkerhetsarbetet. I Frankrike deltar näringslivet aktivt i inrättandet av ett cybercampus och flera projekt bedrivs där samarbetet mellan stat och näringsliv är

CYBERSÄKERHET – REGLERINGAR OCH RAMVERK

Internationellt/EU
Standardisering, reglering och lagstiftning inom cybersäkerhetsområdet är internationell. Inom EU styr ramverk för cybersäkerhetscertifiering samt regleringen av samhällsviktiga och digitala tjänster i form av NIS-direktivet (EU 2016/1148) med tillhörande förslag till reviderat NIS2-direktivet. EU Cyber Security Act syftar till att uppnå en enhetlig säkerhetsnivå och standard i EU och reglerar certifieringar. Dataskyddsförordningen (GDPR) reglerar hanteringen av personuppgifter och den rättsliga grund individer har för att ta del av sina personuppgifter. eIDAS (electronic Identification, Authentication and trust Services) är en EU-förordning som reglerar elektronisk identifiering. Cyber Resilience Act, som EU-kommissionen föreslagit, ska reglera cybersäkerhetskrav på digitala produkter.

Sveriges medlemskap i NATO kommer att påverka arbetet med regelverken då EUs och USAs reglering skiljer sig åt inom vissa områden.

Sverige
Frågor som rör behovet av stärkt informations- och cybersäkerhet i olika samhällsverksamheter behandlas bland annat i 2020 års försvarsbeslut som gäller perioden 2021–2025, den nationella säkerhetsstrategin (Statsrådsberedningen 2017), den nationella strategin för samhällets informations- och cybersäkerhet (Skr 2016/17:213) samt den nationella digitaliseringsstrategin (Regeringskansliet 2017).

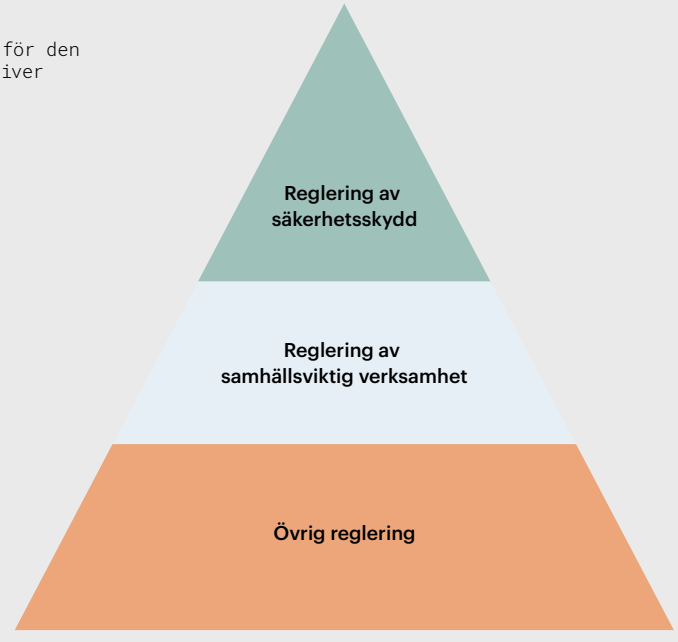
NIS-regleringen är samlingsnamn på den lag, (SFS 2018:1174), förordning (SFS 2018:1175) och föreskrifter som antagits i Sverige för att implementera NIS-direktivet (EU 2016/1148).

I säkerhetsskyddslagen (2018:585) kapitel 1, paragraf 1, finns bestämmelser om skydd i säkerhetskänslig verksamhet vilket är sådana som:

- är av betydelse för Sveriges säkerhet, eller
- omfattas av ett för Sverige förpliktigande internationellt åtagande om säkerhetsskydd.

Säkerhetsskyddslagens bestämmelser gäller för den verksamhetsutövare som till någon del bedriver säkerhetskänslig verksamhet.

Säkerhetsskyddsförordningen (2018:658) innehåller kompletterande bestämmelser till säkerhetsskyddslagen.



Figur 2: Reglering av olika skyddsnivåer i samhället.

centralt (Campus Cyber). I Storbritannien har ett stort antal företag gått igenom i100-programmet vid landets nationella cybersäkerhetscenter (NSCS UK). I Nederländerna ingår företag med anknytning till den digitala infrastrukturen i det nationella partnerskap som det nationella cybersäkerhetscentret ansvarar för (NCSC-NL 2019).

FoU och kompetensförsörjning

I Sverige, liksom i många andra länder, råder brist på IT-kompetens (Tech Sverige 2020, SOU 2021:63, MSB 2021, SOFF 2020, ISC2 2021). Inom cybersäkerhetsområdet har särskilda satsningar gjorts på KTH genom CDIS, *Centrum för cyberförsvar och informationssäkerhet*. Det startade 2020 och är ett nära samarbete mellan KTH, Försvarsmakten, Försvarshögskolan, FRA, MSB, och FOI. Även andra universitet bidrar (till exempel Karlstad, LiU, Chalmers, SU, LU) liksom forskningsinstitutet RISE och yrkeshögskolorna (CDIS).

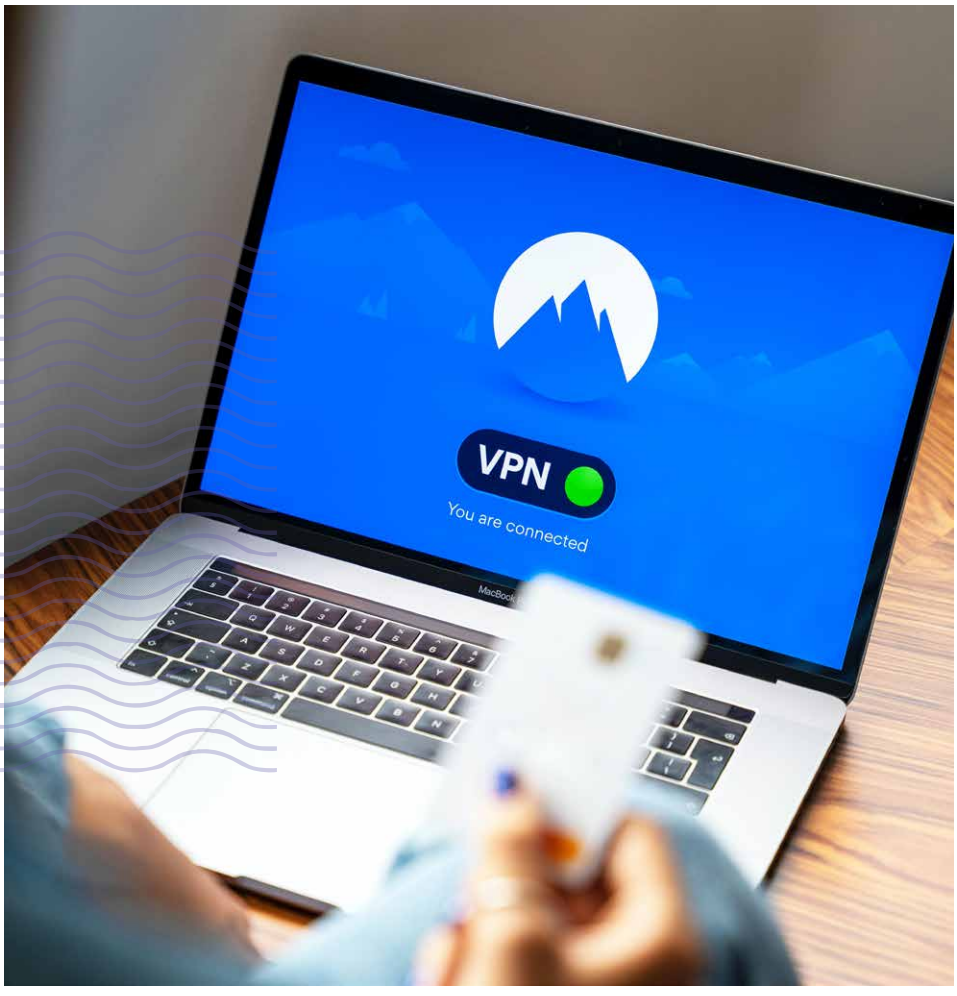
Arbetet med att skapa ett svenskt cybercampus pågår och är också en del av de förslag vi presenterar i denna rapport. Syftet med ett cybercampus är att kraftsamla kring forskning, innovation och utbildning.

Försvarsmakten kan spela en viktig roll för kompetensförsörjningen. I Sverige började man att utbilda cybersoldater 2020. Genom Försvarsmakten är Sverige idag aktiva i NATOs *Cooperativ Cyber Defence Center of Excellence* i Estland (CCDCOE).

Andra länder har kommit längre än Sverige kring FoU och kompetensförsörjning inom cybersäkerhetsområdet. Frankrike öppnade år 2022 sitt cybercampus (Campus Cyber). Även i Nederländerna och Norge finns väletablerade cybercampus. I Tyskland ryms motsvarande satsningar inom olika institut. Exempel finns också på utbildningssatsningar på lägre nivå (Cybercampus Sverige, 2022). I Storbritannien har mer än 50 000 ungdomar i skolåldern deltagit i olika aktiviteter för att öka sina kunskaper inom cybersäkerhet (NCSC-UK).

Många länder bygger upp relativt stora cybersäkerhetsstyrkor inom ramen för sin försvarsmakt. I Storbritannien finns sedan 2020 National Cyber Force (NCF).


AXIS
AXIS
HIKVISION



Nyckelområden och förslag

»Projektet lägger fram förslag inom fem nyckelområden som ska stärka Sveriges cybersäkerhet och konkurrenskraft.«

I projektets tre arbetsgrupper och i styrgruppen har fem nyckelområden identifierats. Inom dessa redovisar vi problembeskrivningar och lägger fram förslag till åtgärder för att stärka Sveriges cybersäkerhet och därmed konkurrenskraft:

- **Politisk styrning på nationell nivå** behöver bli effektivare.
- **Utbyte och användning av information** behöver effektiviseras.
- **Operativ förmåga inom organisationer** behöver stärkas.
- **Forskning, innovation och kompetensförsörjning** Sverige behöver kraftsamla för att klara kompetensförsörjningen, inte minst spetskompetens, inom cybersäkerhetsområdet. Kompetensen är en förutsättning för det FoU-arbete som krävs för att svenska företag ska behålla en stark internationell konkurrenskraft. Det finns också ett behov av breda utbildnings- och bildningssatsningar.
- **Mobilisering av resurser** – fler aktörer behöver mobilisera sina resurser för att hantera och förebygga incidenter.

Figur 3: Projektets fokusområden, förslag och förväntad effekt av förslagen.

PROJEKTETS FOKUSOMRÅDEN	FÖRSLAG	EFFEKT
Politisk styrning på nationell nivå – Sverige behöver en effektivare politisk styrning.	• **Cybersäkerhetsråd** inom regeringskansliet.	• Tydligare politiskt ansvar för styrning. • Tydligare uppdelning mellan strategiskt och operativt arbete.
Effektivare utbyte och användning av information – utbytet och andvändnigen av information behöver effektiviseras.	• **Informationsutbyte för kritisk infrastruktur mellan företag och myndigheter genom sektor ISACs.** • **Incidenthantering/"Haverikommission"** – från händelser till åtgärder, gemensamt lärande.	• Stimulera informationsdelning inom egna branschen. • Lära av andras misstag för bättre incidenthantering. • Större medvetande och insikt hos SME, mindre organisationer, regioner och kommuner.
Operativ förmåga inom organisationer – den operativa förmågan inom organisationer behöver stärkas.	• **Ägare, styrelser & ledning** – principer och verktyg för att stötta styrelse och ledning i deras långsiktiga arbete. • **Cybersäkerhetsnorm** – lätt att göra rätt, stegvis guide.	• Högre medvetande och bättre verktyg för att öka intresset och förmågan hos den högsta ledningen. • En norm kan höja lägstanivån och bli ett stöd för kontinuerlig förbättring av cyberförmågan genom att mäta och följa upp.
Forskning, innovation och kompetensförsörjning – Sverige behöver kraftsamla kring forskning, utbildning och innovation.	• **Cybercampus** – nationellt center för forskning, utbildning, innovation och långsiktig kompetensutveckling. Magisterprogram (60 högskolepoäng).	• Nationell kraftsamling på högskolenivå. • Blir en samlande aktör inom forskning och innovation som kompletterar andra satsningar.
Mobilisering av resurser – fler aktörer behöver mobilisera sina resurser för att hantera och förebygga incidenter.	• **Resurspool** för pågående incidenthantering • **Nationell övnings- och testverksamhet** • **Incitamentsdrivet program för upptäckt av sårbarheter.**	• Bättre utnyttjande av frivilliga resurser. • Ökad effekt av övning och test. • Effektivare upptäckt av sårbarheter.

Politisk styrning

I IVA-rapporten Digitalisering för ökad konkurrenskraft diskuterades styrning och samordningsfrågor kring digitalisering. I rapporten slogs fast att styrningen och samordningen av digitaliseringsfrågorna inom Regeringskansliet är svag och otillräcklig idag. Vi menar att beskrivningen är giltig för den delmängd av digitaliseringsfrågorna som cybersäkerhet utgör (IVA 2019).

Samtidigt arbetar olika statliga myndigheter med samordnings-och styrningsfrågor inom sina ansvarsområden. Arbetssättet har många styrkor. En rad initiativ och åtgärder initieras och genomförs av personer som arbetar direkt med aktuella frågor och problemställningar. Men för att arbetssättet ska vara effektivt krävs att initiativen och åtgärderna samordnas (IVA 2019).

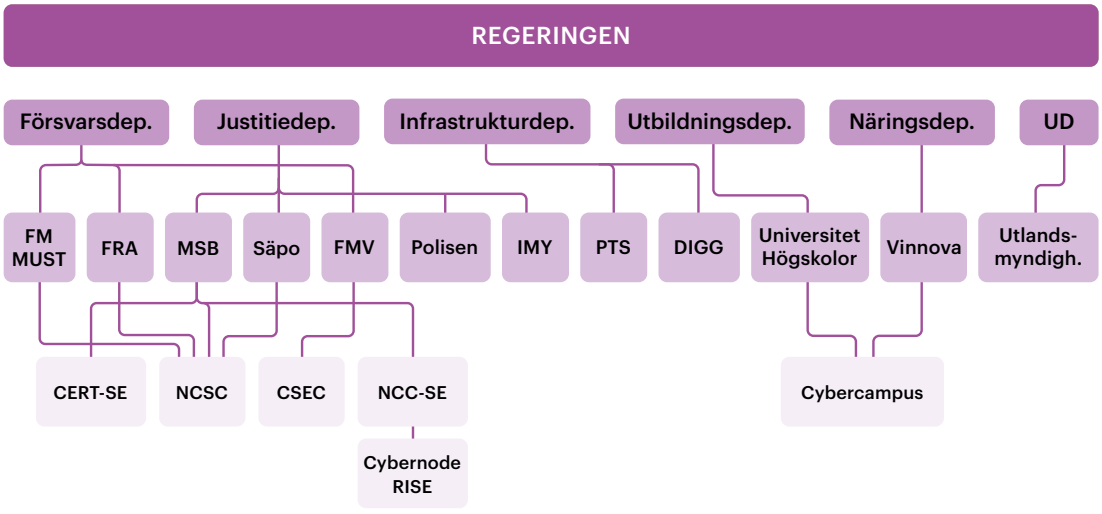
Ett antal myndigheter under i första hand försvars- respektive justitiedepartementen ansvarar för det statliga cybersäkerhetsarbetet (se figur 4 nedan). Dessutom har ytterligare ett antal myndigheter tillsynsansvar. Men det saknas ett sådant för viktiga områden som produktsäkerhet motsvarande det som finns för exempelvis fordonsbranschen. Även infrastruktur-, närings- och utrikesdepartementen är engagerade i arbetet.

Den svenska förvaltningsmodellen med departement och självständiga myndigheter ger förutsättningarna för den politiska styrningen. Regeringen förfogar över en rad verktyg som ger möjlighet till effektiv myndighetsstyrning genom möten, regleringsbrev, lagar och andra regelverk samt rätten att tillsätta och avskeda en myndighets generaldirektör. Påverkan kan också ske i de löpande kontakterna mellan departement och myndighet.

Den svaga styrningen och samordningen inom Regeringskansliet påverkar Sveriges arbete på EU-nivå. Detta är allvarligt eftersom en betydande del av svensk lagstiftning och reglering bestäms här. Exempel på viktiga områden är GDPR och arbetet med att balansera de amerikanska digitala jättarnas tekniska och marknadsmässiga dominans samt EU:s arbete med Digital Decade 2030 (EU-kommissionen 2019). Oklar ansvarsfördelning tillsammans med bristfälliga resurser leder till att EU-arbetet inte blir tillräckligt kraftfullt.

Vi menar att förändringar i styrning och samordning måste ske inom ramen för den befintliga statliga politiska och administrativa strukturen. Att inrätta en ny myndighet tar för lång tid. Utvecklingen av cyberhot och kraven på cybersäkerhet ger oss helt enkelt inte denna tid. Samtidigt visar olika initia-

Figur 4: Schematisk bild över det stora antalet ansvariga departement, myndigheter, enheter, grupperingar och funktioner inom cybersäkerhetsområdet. Myndigheterna har olika uppdrag där cybersäkerhet ingår i varierande grad och omfattning. Givet denna mångfald krävs tydligare styrning och samordning.



tiv att det är möjligt att göra viktiga förändringar inom den nuvarande strukturen. Ett exempel är att "Elektronisk kommunikation och post" blivit en egen beredskapssektor med samma dignitet som exempelvis energiförsörjning, transporter samt livsmedelsförsörjning och dricksvatten.

Vi föreslår därför att ett cybersäkerhetsråd inrättas inom Regeringskansliet. Ett sådant råd kan ge ämnet rätt dignitet samtidigt som det på ett effektivt sätt kan hantera nödvändiga avvägningar mellan områden som utrikesrelationer, handel, geopolitik, alliansfrågor, forskning och utveckling samt konkurrenskraft.

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:

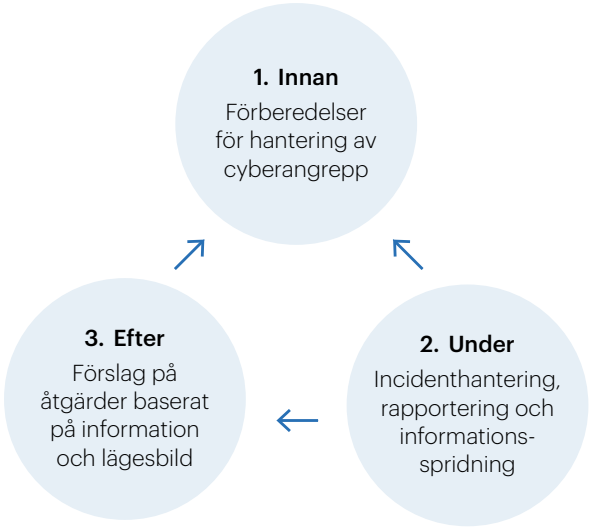
- Följa upp och styra implementeringen av regeringens strategi för informations- och cybersäkerhet samt bereda eventuella förändringar av strategin.

- 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.

Effektivare utbyte och användning av information

Grunden för dynamiken på operativ nivå i ett ekosystem för cybersäkerhet är:

Figur 5: Effektivt informationsutbyte och kontinuerligt säkerhetsarbete. Kontinuerligt säkerhetsarbete bygger på en fungerande cykel med arbete innan, under och efter en incident. Arbetet är viktigt på såväl nationell nivå som i varje enskild organisation.



- Implementering av förmågehöjande åtgärder
- Hantering av en incident, inklusive spridning av information
- Framtagande av förslag på åtgärder baserade på information och lägesbilder.

Ett meningsfullt informationsutbyte måste ske i en sådan form att det leder till åtgärder utifrån de lärdomar och kunskaper olika aktörer fått genom de tre tidigare stegen. Det ska också leda till arbetssätt som gör att olika aktörer kan hantera händelser utifrån nya kunskaper och insikter.

Företag har behov av regelbundna hotbildsanalyser. De efterfrågar även geopolitisk omvärldsbevakning, det vill säga underrättelser och information om de politiska motiven hos nationalstaters aktörer. Företagen har också behov av processer för delning av operativ information och analys av pågående och potentiella cyberhot.

Idag är det fullt möjligt för företag att skaffa sig en bild av cyberhoten från öppna källor. Exempel på kommersiella

sådana är incidenthanteringsföretag som Crowdstrike, ESET och Mandiant och stora techbolag som Google och Microsoft. Amerikanska Department of Justice är exempel på en offentlig aktör. Den information om specifika svenska förhållanden som kan läggas till materialet från dessa aktörer är relativt liten.

Det är alltså inte tillgången på information kring cybersäkerhetsfrågor som är problemet. I stället är frågan hur informationen ska utformas och spridas för att bli användbar för företag inom olika branscher och av olika storlek.

Inom den finansiella sektorn finns idag plattformar för informationsutbyte, ISAC (Information Sharing and Analysis Center). Plattformarna förbättrar säkerheten inom den aktuella branschen. Genom att bidra till att minimera risk skapar de möjligheter för Sverige att bli en arena för test av innovativa digitala lösningar. Därmed bidrar en välfungerande ISAC till att öka attraktionskraften för att locka kapital och företag att arbeta med Sverige som bas.

Det finns idag en rad olika forum för samverkan mellan företag i en bransch och de myndigheter som arbetar med cybersäkerhetsfrågor relaterade till denna. FIDI-Finans och FIDI-Telekom är två exempel. I arbetet med projektet har det framgått att vissa av dessa forum fungerar bra men att det finns brister hos andra. Representationen från myndigheterna vid vissa av forumens möten ger intrycket av att de i praktiken inte prioriterar samverkansformen.

En viktig del av informationsutbytet kring cybersäkerhet är att följa upp och dra lärdom av karaktären hos och hanteringen av IT-relaterade incidenter. Idag finns möjligheter, för vissa organisationer tvingande, att rapportera sådana till myndigheter som IMY, MSB, Polisen, PTS och SÄPO. Rapporteringen är dock bristfällig och regeringen gav nyligen MSB i uppdrag att förbättra arbetet. Även när rapporteringen är tvingande, enligt exempelvis NIS- och GDPR-direktiven, är det otydligt för uppgiftslämnaren vad mottagande myndigheter använder informationen till.

I länder med välfungerande CERT-funktioner finns en stöddjande funktion vilket gör att incitamenten för att rapportera ökar. Det finns ingenting i de svenska regelverken som förhindrar att svenska myndigheter kan agera på motsvarande sätt.

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.

Haverikommission för cyberincidenter

I Sverige finns varken system eller organisationer med huvuduppgiften att utreda cyberincidenter. Statens haverikommission kan göra det om händelsen uppfyller dess instruktioner. Nederländerna och Finland har utökat uppgiften för sina haverikommissioner att också omfatta IT.

Ett systematiskt arbete inom detta område kräver rotorsaksanalyser. Dessa innebär att man undersöker grundorsakerna till en större cyberincident för att få svar på vad som hände, varför och hur vi ska undvika att det händer igen. Analyserna är tidskrävande. Därför prioriteras de ofta bort. I stället litar många aktörer på tillfällig problemlösning med förhoppningen att den aktuella incidenten inte inträffar igen.

Vi menar att en haverikommission med fokus mot cybersäkerhet kan sprida information om sårbarheter och

konsekvenserna av dessa. Informationen ska dokumenteras väl, men inte i detalj göras tillgängliga för alla. Syftet är att skapa ett informationsflöde som bidrar till säkerhetsutvecklingen inom cyberområdet på motsvarande sätt som exempelvis incidentrapporteringen inom civil luftfart. Arbetet ska präglas av hög sekretess och höga säkerhetskrav. Därmed säkerställs att anonymiteten hos uppgiftslämnare garanteras och gör att den som råkat ut för ett cyberangrepp eller incident är villig att lämna information.

Kommissionens kompetens ska variera beroende på vilken typ av incident som inträffat. Bemanningen ska bestå av en kärna fast anställda och ett större nätverk av experter och andra nyckelaktörer inom informations-, IT- och cybersäkerhet samt infrastruktur för elektronisk kommunikation. Därmed kan haverikommissionen användas för ett brett spektrum av händelser.

Det är naturligt att arbetet med en haverikommission med fokus mot cybersäkerhet inspireras av Statens haverikommission. Men denna har mandat att fördela skuld och ansvar i samband med en olycka. Den kommission vi föreslår ska arbeta på ett annat sätt. Den ska inte peka ut brister i enskilda organisationer, fördela straff-, civil- eller förvaltningsmässig skuld. Den ska inte heller utfärda förbud mot användning av system och applikationer. Istället ska den presentera underlag och slutsatser som kan hjälpa olika aktörer att undvika att drabbas av cyberangrepp.

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.

Operativ förmåga inom organisationer

I regeringens cybersäkerhetsstrategi beskrivs en nationell modell för att hantera cybersäkerhet inom organisationers dagliga verksamhet. Den nationella modellen utgår från internationella regleringar (exempelvis NIS-direktivet och GDPR) och lagstiftning (EU-direktiv, den svenska implementeringen av dessa samt formuleringen i cybersäkerhetsstrategin). För att genomföra denna del av strategin behövs ett gemensamt förhållningssätt, en terminologi samt ett sätt att beskriva och följa upp det praktiska arbetet med att höja cyberförmågan inom organisationer. Här har en cybersäkerhetsnorm med principer och verktyg goda förutsättningar att vara ett effektivt stöd.

Riskhantering är en central del av arbetet i ett företags styrelse och ledning. Omvärldsförändringar gör att nya frågeställningar kommer upp på agendan. Finanskrisen i början på 90-talet satte fokus på den finansiella riskhanteringen. Ökade krav på Corporate Social Responsibility (CSR) under 1990-talet gjorde att företagen började ta upp CSR-frågor i sina årsredovisningar. Nya regelverk för finansiella verksamheter har gjort att kvaliteten i företagens compliance-arbete ökat. Att större företag har ett effektivt hållbarhetsarbete är idag en självklarhet. Resultat av arbetet inom dessa områden är viktiga underlag när investerare och kapitalmarknaden granskar och värderar företagen.

Cybersäkerhetsfrågor har ännu inte samma status som finansiella och hållbarhetsfrågor. Regelverken är ännu inte tillräckligt utvecklade. Hos många styrelser och företagsledningar är också kunskapen låg. Det gäller speciellt företag som påbörjat sin digitaliseringsresa relativt sent. Ledningen mäts dessutom sällan på beredskapen inom cyberområdet. Speciellt mindre och medelstora företag har inte heller tillräckliga resurser för att arbeta med frågorna. Revisionsfirmor har nu börjat sälja tjänster inom området. Men tjänsterna är ännu relativt sett mindre avancerade jämfört med exempelvis finansiell riskhantering.

I dagens situation menar vi därför att ägare och styrelse i företag och offentliga organisationer är hjälpta av en cybersäkerhetsnorm. En sådan ska vara konkret och innehålla handfasta råd. Den kan också vara ett verktyg för att relatera kostnader för investeringar till den nytta i form av minskade skador för cyberangrepp den kan ge. Därmed kommer

normen att spela en viktig roll i de delar av företagsstyrningen som berör cybersäkerhetsfrågor. Den kan också vara ett av verktygen för att formulera krav på ledningen.

En cybersäkerhetsnorm bör innehålla dels handfasta beskrivningar av åtgärder och råd, dels processer för utveckling och förvaltning av normen. Att ta fram normen kräver processer där offentliga och privata aktörer samverkar samtidigt med ett erfarenhetsutbyte som stärker kunskaperna hos de som deltar i arbetet.

Arbetet med normen börjar inte från noll. En slutsats från NISU 2014 var att en nationell styrmodell borde tas fram. De myndigheter som idag ingår i Nationellt cybersäkerhetscenter har tidigare arbetat med frågorna inom ramen för SAMFI (Samverkansgruppen för informationssäkerhet). MSB har ett uppdrag att ta fram en teminologidatabas som ska göras tillgänglig på en gemensam plattform. Det finns också standarder, som till exempel NIST 800, som kan anpassas till svenska förhållanden. En ytterligare möjlighet är att också använda ISO 27001.

FÖRSLAG

Vi föreslår att arbetet med en cybersäkerhetsnorm med det syfte, de grundkomponenter och egenskaper vi beskrivit ovan, 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.

Forskning, innovation och kompetensförsörjning

Cybersäkerhetsarbetet kräver många olika typer av kompetens. Idag råder det brist inom flertalet relevanta discipliner, inte minst inom IT-området. Därför behöver kompetensförsörjningen stärkas genom en rad åtgärder, allt från skolan, grund- och forskarutbildning på universitet och högskolor till fortbildning av yrkesverksamma.

Den ökade uppmärksamheten kring cybersäkerhetsfrågor gör det naturligt att diskutera vilken plats dessa ska ha i undervisningen i skolan. En möjlighet är att cybersäkerhet kommer in i läroplanen för grundskolan. Ett sådant förslag måste dock ta hänsyn till dagens stora stoffträngsel, det vill säga den totala mängd frågor som ska rymmas inom läroplanens begränsade utrymme.

Även breda folkbildningskampanjer kan spela en viktig roll. Redan idag finns många goda exempel på sådana initiativ från MSB, Internetstiftelsen och Stöldskyddsföreningen. Inspiration kan med fördel också hämtas från USA genom CISA (Cybersecurity and Infrastructure Security Agency) som arbetar för att höja medvetenheten kring cybersäkerhetsfrågor hos allmänheten. ENISAs cybersäkerhetsmånad är ett motsvarande initiativ på europeisk nivå.

Utbildningsinsatser måste även ske utanför skolan och universiteten. Företagen behöver utbilda sina medarbetare i cybersäkerhet. De behöver också engagera sig för att möta de snabbt växande behoven av kompetens. Ett sätt att möta dessa är att intensifiera samarbetet med yrkeshögskolorna.

Universitet och högskolor måste säkerställa bred kompetens på högskolenivå av relevans för cybersäkerhetsarbetet. Samtidigt behöver de säkerställa tillgången på spetskompetens i världsklass för att trygga svenska företags möjligheter till avancerad forskning och produktutveckling i en allt hårdare internationell konkurrens.

I Sverige finns idag en rad olika initiativ kring samordnings-, forsknings- och försvarsaspekter av cybersäkerhet. Exempel är NCSC, *Nationellt cybersäkertetscenter*, NCC-SE, *Nationellt samordningscenter för forskning och innovation inom cybersäkerhet*, som MSB ansvarar för, CDIS *Centrum för cyberförsvar och informationssäkerhet*. Men inget av dessa integrerar forskning, utbildning och innovation i tillräcklig grad. Sverige behöver därför ett cybercampus som gravitationscentrum i vårt nationella cybersäkerhetsarbete.

Många länder har kraftsamlat kring forskning, utbildning och innovation inom cybersäkerhetsområdet. I Norge, Schweiz och Frankrike finns cybercampus med omfattande utbildnings- och forskningsverksamhet. I Tyskland finns stora centrumbildningar. Israel har en mycket framgångsrik

innovationssektor runt cybersäkerhet där universitet, myndigheter och näringsliv samarbetar.

Cybercampus ska bidra till grundutbildningen på flera nivåer. Forskning, inte minst kring metoder för utveckling av säkra system i samverkan med näringslivet, är en central del av verksamheten. En viktig del i detta arbeta är att stimulera nya företag som arbetar med cybersäkerhet. Inom ramen för campuset ska flera universitet och högskolor samarbeta. Näringslivets engagemang är en förutsättning för campuset. Ett internationellt perspektiv är en självklarhet i alla delar av verksamheten.

En rimlig investeringsnivå för ett svenskt cybercampus är 100 miljoner kronor per år som bas med sikte på 500 miljoner kronor per år om fem år. Framgånsrika verksamheter som SciLifeLab, WASP och nystartade WISE kan här tjäna som förebilder.

En uppgift för de universitet som är engagerade i Cybercampus är att inrätta magisterprogram för yrkesverksamma. Dessa bör utformas så att personer utan teknisk grundutbildning kan öka sin kompetens för att kunna arbeta med verksamhetsnära säkerhetsfrågor relaterade till IT-system. I antagningen ska hänsyn tas till yrkeserfarenhet inom området. En ambition är att programmen ska bidra till att locka fler kvinnor till cybersäkerhetsområdet, vilka idag är kraftigt underrepresenterade inom sektorn.

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.

Mobilisering av resurser

Sverige saknar idag en sammanhållen övnings- och teststrategi för cyberdomänen. Sådana har växt fram i i USA, Storbritannien och EU under de senaste tio åren. Ett nationellt övnings- och testramverk kan bidra till strukturerade och mätbara resultat som ger värdefulla underlag och rekommendationer till beslutsfattare. Resultaten kan också användas för att identifiera förbättringsområden inom den nationella informations- och cybersäkerhetstrategin.

Det finns idag en rad aktiviteter inom området. RISE och FoI utvecklar övningsmiljöer. FoI:s övningsmiljö används av bland annat PTS (Cyber Defense Exercise – CDX) och Försvarsmakten (Safe Cyber). PTS gör dessutom övningar inom sin sektor, så kallade TELÖ. Försvarsmakten är ansvariga för Sveriges deltagande i övningen Locked Shields inom ramen för sin roll i CCDCOE i Tallinn. MSB genomför nationella informationssäkerhetsövningar, NISÖ.

Övningarna kan göras i en simulerad och kontrollerad miljö (Cyber Range) för att testa teknik och system. Men också frågor kring krishantering, beslutsprocesser och kommunikation kan övas i anslutning till de rent tekniska aspekterna.

Övningarna bör genomföras på organisations-, sektors- och nationell nivå samtidigt som erfarenheter delas i det nätverk som planerar och genomför dessa. Övningarna kan genomföras i den egna organisationen. Men de kan också göras tillsammans med andra för att utbyta erfarenheter, bygga ny kompetens och skapa ökat förtroende mellan de övande organisationerna. För mindre företag och kommuner kan inspiration hämtas från Storbritanniens NCSC Exercise-in-a-Box. Detta är ett verktyg som är tillgängligt gratis online och gör det möjligt för organisationer att öva på att hantera cyberangrepp.

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.

Resurser från det civila samhället kompletterar redan idag offentliga aktörer i olika sammanhang. Missing People hjälper polisen att leta efter försvunna personer. Frivilliga hjälper till vid stora skogsbränder. I Sverige finns många personer med IT-säkerhetskompetens som har sin dagliga gärning inom andra områden. Dessa kan utgöra en kompetenspool när tillgången till specialistkompetens är otillräcklig.

En möjlighet är att gruppen organiseras som en del av de frivilliga försvarsorganisationerna. Kompetenspoolen måste utformas och organiseras så att den inte snedvrider konkurrensen med privata aktörer. Poolen kan med fördel innehålla personer med kompetens inom exempelvis organisation, kommunikation och krishantering som också är viktiga i hanteringen av en cyberincident. För att ingå i gruppen måste en noggrann säkerhetsprövning göras.

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.

Tester och granskningar utförs idag på sektorsnivå eller i enskilda verksamheter. Eftersom nya tekniska hot ökar i snabb takt, är det svårt att genomföra tester och granskningar med tillräcklig omfattning och variation. Granskningarna begränsas också av verksamhetens budget och den tekniska kompetensen hos de som utför arbetet.

Sverige behöver ett incitamentsdrivet nationellt program för upptäckt av sårbarheter, ett Bug Bounty-program. Inspiration kan hämtas från USA där sådana program är etablerade inte bara hos företag utan även hos myndigheter och försvaret.

De företag eller myndigheter som vill få öppna delar av sina digitala system granskade annonserar detta på plattformar, till exempel Bugcrowd och HackerOne, som används av etiska hackare. Organisatören avgör vilka delar av det egna systemet som ska utsättas för angreppsförsök och de har en policy för detta. Det förekommer att hackare som man tror sig kunna lita på bjuds in. Men vissa organisationer lämnar det öppet för vem som helst att delta.

Hackarna försöker hitta svagheter och fel i de publika delarna av företagets eller myndighetens system. Upptäckta svagheter rapporteras till organisatören av Bug Bounty-programmet. Hur informationen förs vidare varierar. Exempelvis publicerar det amerikanska försvarsdepartementet resultatet av de etiska hackarnas arbete efter att ha tagit bort säkerhetskänsligt innehåll, men inte information om den upptäckta svagheten.

Incitamenten för att delta varierar. I vissa Bug Bounty-program lämnas ingen ersättning alls. Men i många fall får hackaren ekonomisk ersättning som kan variera i storlek. Den etiska hackaren har olika motiv att medverka – allt från att öka sin status i det egna nätverket till att tjäna pengar.

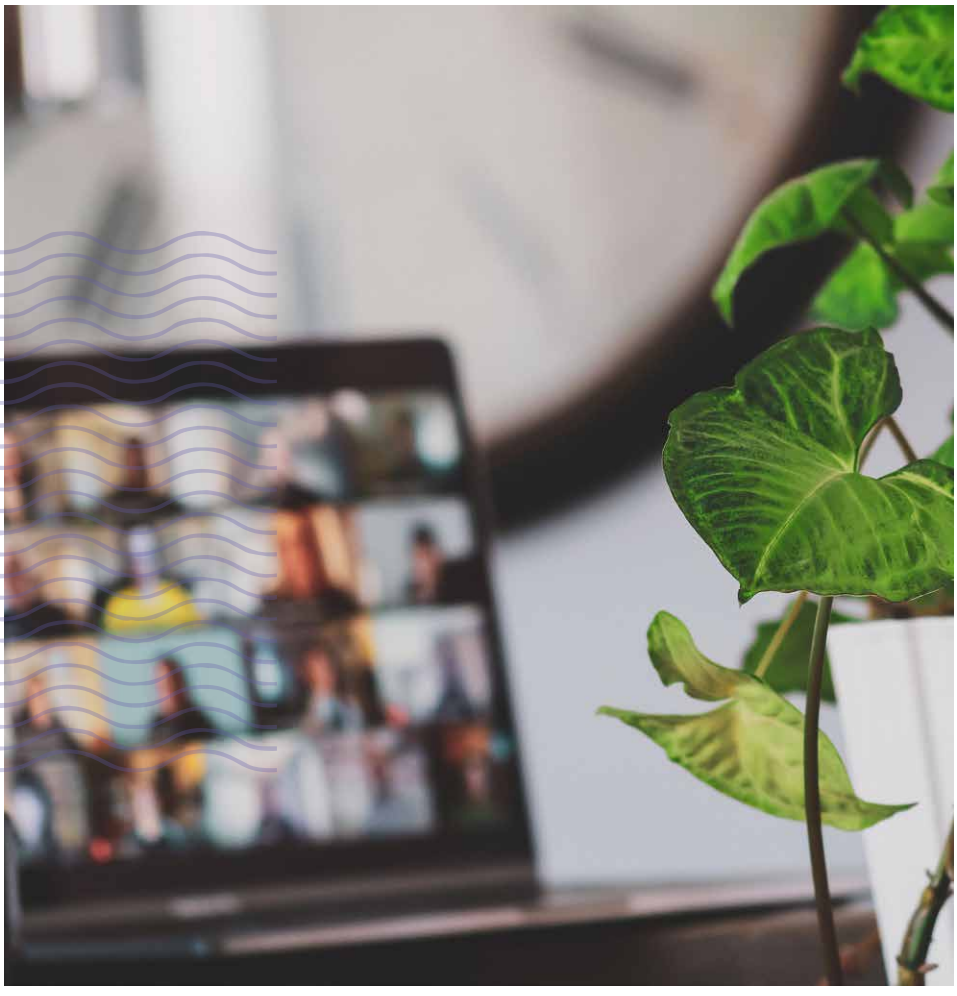
Erfarenheterna från dessa program är goda. Många svagheter upptäcks. De spelregler som sätts upp – att man enbart ska försöka hacka de öppna delarna av organisationens system och sedan rapportera dem – fungerar. För den som har andra avsikter än de som ryms inom Bug Bounty-programmen kommer de alldeles oavsett programmen att fortsätta sin brottsliga verksamhet.

Vi menar att initiativen och förslagen till utformning av svenska Bug Bounty-program inom samhällskritiska verksamheter lämpligen bör ske inom ramen för samarbetet inom Nationellt cybersäkerhetscenter.

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.


ACHIEVEMENT
47.29%
ACHIEVEMENT
73.43%



Appendix

Referenser

ANSSI, Agence nationale de la sécurité des systèmes d`information, https://www.ssi.gouv.fr/en/organisation/executive-office/

ANSSI Annual Review 2021, https://www.ssi.gouv.fr/en/mission/annual-review-2021/

BSI, https://www.bsi.bund.de/EN/Das-BSI/Organisation-und-Aufbau/organisation-und-aufbau_node.html

Bugcrowd, Secure the Government, https://bugcrowd.com/programs/organizations/cisa

Campus Cyber, Acteurs, https://campuscyber.fr/acteurs/

CCDCOE, The NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/

CDIS, Centrum för cyberförsvar och informationssäkerhet, https://www.kth.se/sv/cdis/centre-for-cyber-defence-and-information-security-1.946971

CISA, Cybersecurity & Infrastructure Security Agency, BINDING OPERATIONAL DIRECTIVE 20-01 - DEVELOP AND PUBLISH A VULNERABILITY DISCLOSURE POLICY, https://www.cisa.gov/binding-operational-directive-20-01

Cybercampus Sverige (2022), Forskning, innovation och utbildning för cyberförsvar och cybersäkerhet, KTH, RISE, Försvarsmakten

DESI (2022), The Digital Economy and Society Index, EU-kommissionen, https://digital-strategy.ec.europa.eu/en/policies/desi

EU-kommissionen (2019), Digital Decade 2030: EU-kommissionen, EU:s digitala decennium: digitala mål för 2030,

Fick, N., Miscik, J., (2022), Confronting Reality i Cyberspace, Foreign policy for a Fragmented Internet, Independent Task Force Report No 80, Council on Foreign Relations

FRA (2022), Medarbetare i demokratins tjänst, FRA årsrapport 2021, Försvarets Radioanstalt

ISC2 (2018), Cybersecurity Assessments in Mergers and Acquisitions december 2018

ISC2 (2021), A Resilient Cybersecurity Profession Charts the Path Forward

IVA (2019), Digitalisering för ökad konkurrenskraft

IVA (2015), Nycklar till ökad attraktivitet och konkurrenskraft

KKrVa (2022), Kungl Krigsvetenskapsakademien, Cyberförsvaret – en introduktion

Lundin, L-E., Magnusson G., red. (2022) På allvar. Svensk säkerhetspolitik i ofärdstider. Slutrapport från SES-projektet. Kungl. Krigsvetenskapsakademien

MSB (2021), Kompetens inom informations- och cybersäkerhet

MUST (2022), Musts årsöversikt 2021, Försvarsmakten

National Cyber Strategy (2022), Pioneering a cyber future with the whole of the UK

NSCS (2020), Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden, Nationella cybersäkerhetscentret

NCSC.se, Vårt uppdrag, https://www.ncsc.se/om-centret/vart-uppdrag/index.shtml, Nationella cybersäkerhetscentret

NCSC-NL (2019), Operatiional Framework NCSC-NL, Version March 21, 2019

NCSC-UK, About the NSCS, National Cyber Security Center, https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

Regeringskansliet (2017), För ett hållbart digitaliserat Sverige – en digialiseringsstrategi

RISE (2022), Cyberhot mot Sverige – en sammanfattning för ledare och beslutsfattare, RISE Centrum för cybersäkerhet

SIPRI (2022), World military expenditure passes $2 trillion for first time, https://www.sipri.org/media/press-release/2022/world-military-expenditure-passes-2-trillion-first-time

Skr (2016/17:213), Nationell strategi för samhällets informations- och cybersäkerhet

SOFF (2020),Så kan vi säkra kompetensförsörjningen inom cybersäkerhet

SOFF, Teknikföretagen (2020), Näringslivets syn på Sveriges kommande nationella cybersäkerhetscenter

SOU (2021:63), Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem. Betänkande av cybersäkerhetsutredningen

Statsrådsberedningen (2017), Nationell säkerhetsstrategi

Svenskt Näringsliv (2021), Företagen och IT-säkerheten – hotbilder, motåtgärder och behov

SÄPO (2022), Säkerhetspolisen 2021

Tech Sverige (2022), En techagenda för Sverige

Tech Sverige (2020), IT-kompetensbristen. En rapport från IT&Telekomföretagen (nuvarande Tech Sverige)

The Business Research Company (2022), Information Technology Global Market Report 2022

TRAFICOM, Havaro-tjänsten, https://www.kyberturvallisuuskeskus.fi/sv/havaro-tjansten

US. Dept. of Defence, hacerone, https://hackerone.com/deptofdefense?type=team

Om projektet

IVAs projekt Cybersäkerhet för ökad konkurrenskraft startade i juni 2021 och fortsätter fram till sommaren 2023. Projektets leds av en styrgrupp som inledningsvis beslutade om den plan som beskriver projektets mål, syfte och arbetsprocess.

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

Under projektet har en rad kunskapsseminarier, workshopar och möten hållits i en vidare krets. För att lära och få inspiration från omvärlden har seminarier och besök arrangerats med representanter från cybermyndigheterna i Frankrike, Storbritannien och Estland.

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), 2022
Box 5073, SE-102 42 Stockholm
Tfn: 08-791 29 00

Inom ramen för IVAs verksamhet publiceras rapporter av olika slag. Alla rapporter sakgranskas av sakkunniga och godkänns därefter för publicering av IVAs vd.

IVA-M 537
ISSN: 1100-5645
ISBN: 978-91-89181-32-8

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

Denna rapport finns att ladda ned via www.iva.se

Kungl. IngenjörsVetenskaps
Akademien