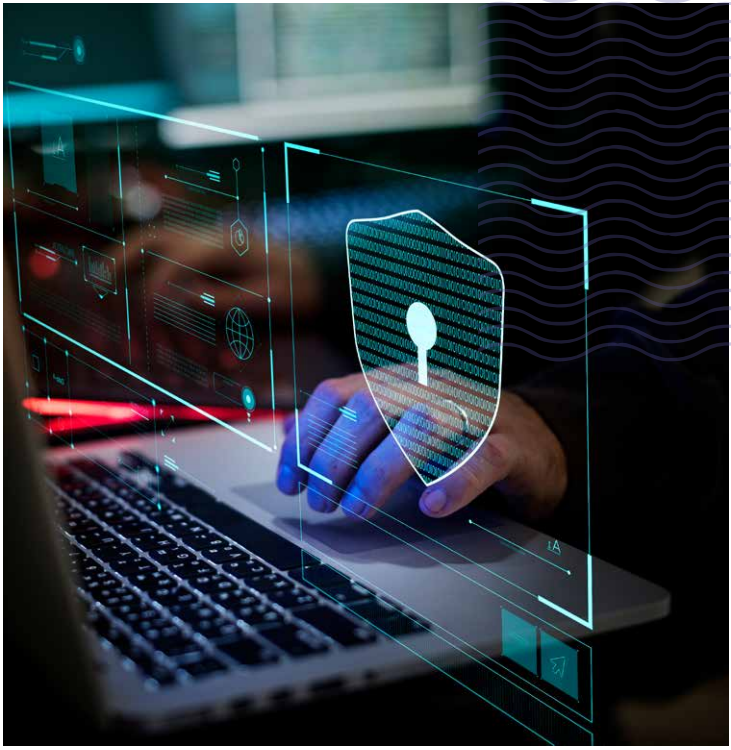
Cybersäkerhet för ökad konkurrenskraft



CYBERSÄKERHET FÖR
ÖKAD KONKURRENSKRAFT

DECEMBER 2021

IVA
Kungl. IngenjörsVetenskaps Akademien


Secured

Projektet

Antagonistiska cyberhot påverkar alla delar av det svenska samhället. Projektet ”Cybersäkerhet för ökad konkurrenskraft” fokuserar på hur privata och offentliga verksamheter kan stärka sin förmåga att möta cyberhot. Det ska också komma med förslag på åtgärder och beslut inom politik, privat och offentlig verksamhet som är nödvändiga för att stärka cybersäkerheten och därmed Sveriges konkurrenskraft.

Sverige ligger i internationell jämförelse långt fram när det gäller digitalisering. Men det finns ett glapp mellan denna tätposition och vår placering långt efter andra länder när det gäller förmågan att skydda sig mot antagonistiska cyberhot. Glappet måste slutas om Sverige ska kunna dra nytta av digitaliseringens alla möjligheter.

Medvetenheten och kunskapen om cybersäkerhetsfrågor hos politiker, beslutsfattare inom privata och offentliga verksamheter samt medarbetarna inom de båda sektorerna måste öka. Samordningen på politisk- och myndighetsnivå måste stärkas.

En utmaning för politiken är att hantera svåra avvägningar mellan olika åtgärder för att stärka cybersäkerheten ur ett samhällsperspektiv. Konkreta åtgärder för att förebygga och möta cyberattacker måste genomföras inom privata och offentliga verksamheter. Sverige behöver också mer forskning och utbildning om cybersäkerhetsfrågor.

Frågeställningar

Projektet arbetar med en rad frågeställningar:

- Vilka är de främsta orsakerna till dagens cybersäkerhetsproblematik? Vilken utveckling väntar i framtiden?
- Hur ändrar den tekniska utvecklingen cybersäkerhetsarbetet?
- Hur kan cybersäkerhetsarbetet i olika samhällssektorer förbättras?
- Hur kan styrning och samordning effektiviseras? Behövs mer resurser?
- Hur ökar vi tillgången till kompetens?
- Hur påverkar globaliseringen möjligheterna för en liten nation som Sverige att hantera cybersäkerheten?
- Hur kan vi bidra till och dra nytta av internationella initiativ och samarbeten, inte minst inom EU?
- Hur ska Sverige förhålla sig till olika geopolitiska blocks strävan att skapa regelverk som gynnar vissa och missgynnar andra nationer?

Projektet, pågår åren 2021–2023. Medverkar gör personer med expertis och erfaren-

het av olika cybersäkerhetsfrågor från privat och offentlig sektor. Tre arbetsgrupper fördjupar projektets frågeställningar:

- Styrning, samverkan och ansvarsfördelning
- System, teknik och beteenden
- Kunskap och kompetensförsörjning

Beskrivningar, analyser och förslag dokumenteras i rapporter och kommuniceras i rundabordssamtal, seminarier och andra publika sammanhang.

Styrgrupp

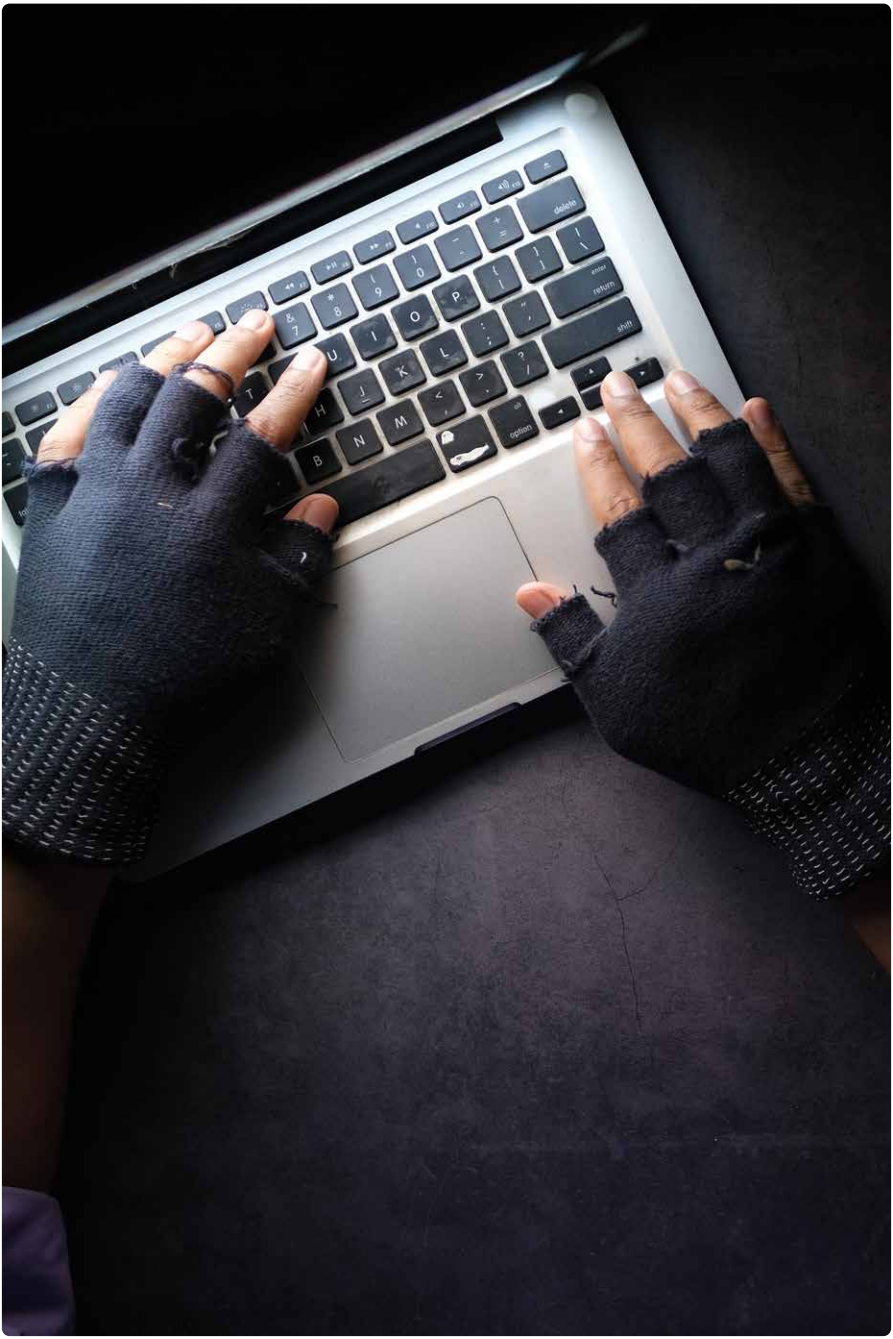
Håkan Buskhe, vd FAM AB (styrgruppens ordförande)
Anne-Marie Eklund-Löwinder, vd, Amelsec
Erik Ekudden, CTO Ericsson
Patrik Fältström, Technical Director Netnod (Ordförande System, teknik och beteenden)
Pontus Johnson, Professor KTH (Ordförande Kunskap och kompetensförsörjning)
Lena Klasén, Forskningsdirektör Polismyndigheten
Hans Lindberg, vd, Svenska Bankföreningen (Ordförande Styrning, samverkan och ansvarsfördelning)
Charlotte Lindgren, chef Cyberverksamheten, FRA
Jan Nygren, IVA-ledamot avdelning Utbildning och forskning
Staffan Truvé, Forskningsdirektör, Recorded Future

Projektledning

Per Hjertén, projektledare, per.hjerten@iva.se
Staffan Eriksson, delprojektledare, staffan.eriksson@iva.se
Eva Lagerblad, koordinator, eva.lagerblad@iva.se
Jan Westberg, kommunikationsansvarig, delprojektledare, jan.westberg@iva.se

Politisk referensgrupp

Åsa Eriksson (S), Näringsutskottet
Pål Jonson (M), Ordförande Försvarsutskottet
Caroline Nordengrip (SD), Försvarsutskottet
Hanna Gunnarsson (V), Försvarsutskottet (Vice gruppledare V)
Niels Paarup-Petersen (C), Utbildningsutskottet
Mikael Oscarsson (KD), Försvarsutskottet
Margareta Fransson (MP), Skatteutskottet
Allan Widman (L), Försvarsutskottet



Hotbilden

Hoten ökar

Hoten mot digitala system i Sverige är många och blir allt fler. En anledning är att verksamheter i olika samhällssektorer blir bättre på att dra nytta av digitaliseringens möjligheter. Genom användningen av information i de digitala systemen skapas betydande värden som lockar till sig aktörer med illegala syften.

För att skydda sig mot cyberhot är det nödvändigt att förstå angriparnas syfte och tillvägagångssätt, det vill säga hur de utnyttjar brister och svagheter i it-system och organisationer.

Det gäller också att ha kunskap om vilka skyddsvärden som är vitala för den egna verksamheten. Är det kunskap, information eller personer som är speciellt intressanta? Eller en kombination?

Olika beskrivningar av hotbilden

Expertmyndigheter och aktörer inom cybersäkerhetsområdet beskriver hotbilden på olika sätt. Detaljerade analyser görs utifrån myndighetens ansvarsområde och för att passa in i det specifika sammanhang den ska användas.

Underrättelsetjänsterna beskriver hotbilden utifrån sitt omfattande arbete. Av sekretesskäl delar de dock inte med sig av analyserna till offentliga eller privata aktörer.

Hotbilden är under ständig förändring. Det är viktigt att inte låsa sig vid en ögonblicksbild. I stället måste beskrivningarna utgå från den kontinuerliga förändringen av cyberhoten.

Tre kategorier aktörer

Hotaktörerna är mer eller mindre välorganiserade. Syftet med verksamheten skiftar liksom tidshorisonten för att nå sina mål. Resurser och förmåga varierar också kraftigt.

Det är svårt att skaffa sig en exakt bild av vilka aktörerna är, var de finns och hur de

agerar. De samverkar ofta med varandra, använder sofistikerade metoder för att inte upptäckas och gör komplexa gemensamma attacker.

Hotaktörerna kan delas in i statliga-, kriminella- respektive ideologiskt motiverade aktörer (Se faktaruta).

Oavsett typen av hotaktör är den gemensamma nämnaren i de flesta cyberattacker att angriparen tar sig in i ett utvalt it-system. Väl inne arbetar de för att identifiera fler sårbarheter och skaffa sig utökad behörighet. Därefter kan de stjäla data, modifiera eller lägga till skadlig kod som exekveras vid en bestämd tidpunkt.

Överbelastningsattacker är en annan typ av angrepp. Målet är att överbelasta systemet utan att ta sig in i det. Svenska banker har under de senaste tio åren drabbats av överbelastningsattacker.

STATLIGA HOTAKTÖRER

Statliga hotaktörer är ofta en del av en nations underrättelse- eller säkerhetstjänst. Syftet är att uppfylla nationella säkerhetspolitiska intressen, bland annat genom att påverka politiska processer i andra länder. De kan också bedriva industrispionage för att öka det egna landets konkurrenskraft.

De statliga hotaktörerna har stora resurser och förmåga till en hög aktivitetsnivå under en längre tid. Kategorin kallas ibland Advanced Persistent Threats (APT). Säkerhetslagstiftningen är inriktad mot att skydda Sverige mot statliga hotaktörer.

KRIMINELLA HOTAKTÖRER

Kriminella hotaktörer vill på enklaste sätt tjäna maximalt med pengar. Jämfört med de statliga hotaktörerna är de mindre sofistikerade och använder i regel existerande, och välbeprövade metoder. De utgör ofta allvarliga hot mot företagen genom att använda de 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 mot mål där risken för upptäckt är låg. Rena stölder av pengar, information, identiteter samt bedrägerier är vanliga. Låsning av system eller information följt av krav på lösensumma riktade mot globala tjänster och digitala leverantörskedjor har visat sig lönsamma och ökat i omfattning.

IDEOLOGISKT MOTIVERADE HOTAKTÖRER

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

Olika typer av sårbarheter i it-system utnyttjas

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

- Brister i behörighetshantering
- Undermålig it-arkitektur
- Avsaknad av rutiner för underhåll och uppdatering av programvara
- Brister i konfiguration
- Anslutning av icke godkänd utrustning.

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

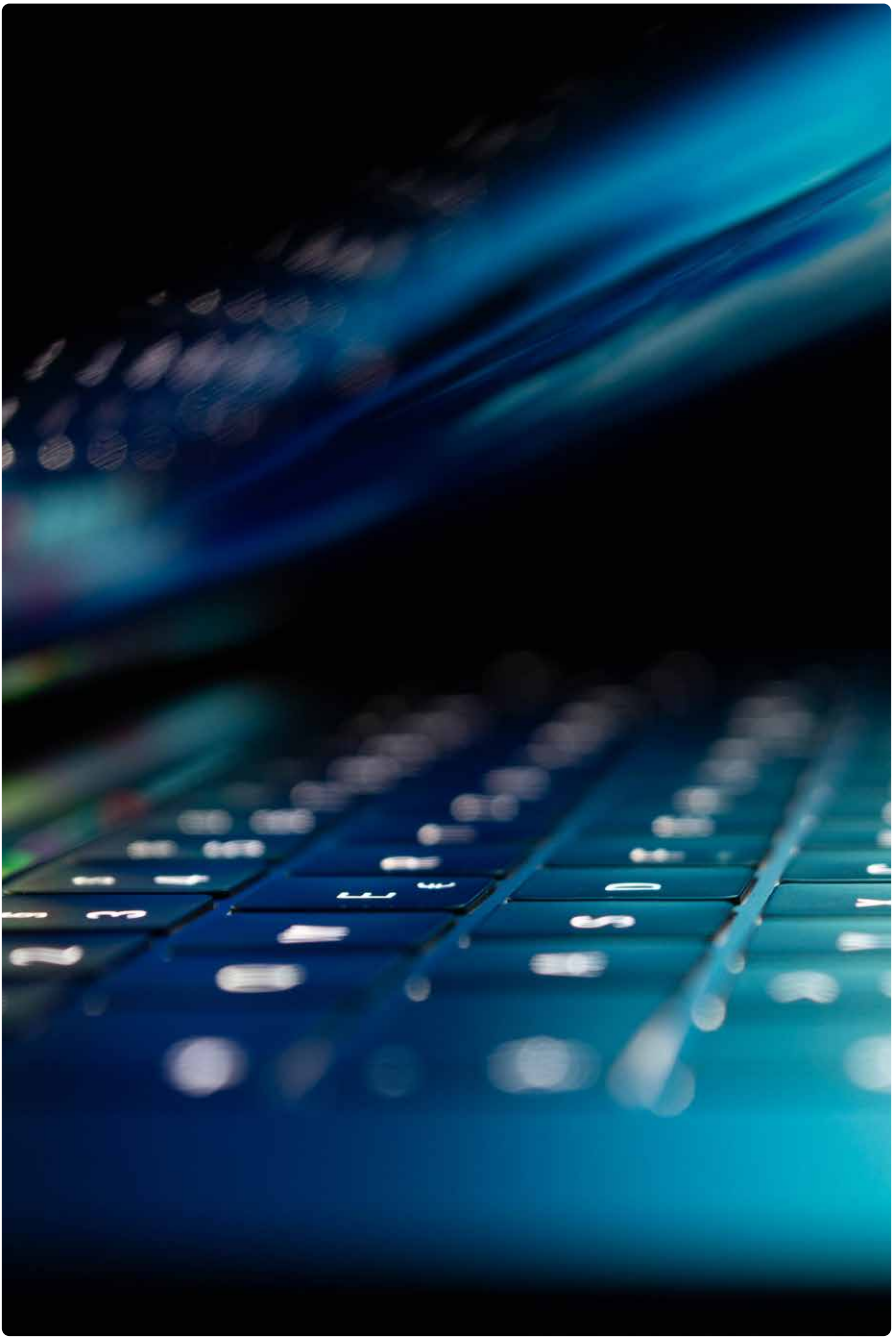
Okända sårbarheter kallas zero-day-sårbarheter. Dessa utgörs av nya sårbarheter i system som en hotaktör upptäcker och som kan utnyttjas ända till dess de åtgärdas. Hotaktörer handlar med zero-day-sårbarheter ofta med mäklare som mellanhand.

Olika metoder

Lösenordsbaserade cyberangrepp är en vanlig metod för angrepp. Hotaktören kan antingen utnyttja sårbarheterna som beskrivits ovan för att komma åt lösenord eller köpa tillgång till redan läckta. Ett annat sätt är att med datorkraft testa sig fram till rätt lösenord. Bredare sådana angrepp kallas phishing. Är de riktade till mindre grupper eller enstaka individer kallas de spear phishing.

En annan metod är att helt enkelt ringa till användare och utge sig för att vara supportpersonal. Man kan också få tillgång till it-system genom att sprida USB-minnen med skadlig kod eller rekrytera en person på insidan av organisationen.

För att angriparen ska kunna utnyttja tekniska sårbarheter utnyttjas det mänskliga beteendet. Ett vanligt tillvägagångssätt är att skicka epost, ofta med länk till en falsk webbsida, för att få en användare att installera programvara med skadlig kod eller lämna ut inloggningsuppgifter. Angriparen kan också använda sig av metoder som närmar sig spionerі för att lura till sig lösenord eller annan strategisk information.



Lägesbilden

I projektets inledande fas har styrgruppen och ett antal andra personer diskuterat lägesbilden av hanteringen av cybersäkerheten i Sverige. Vår sammanfattning av lägesbilden gör inga anspråk på att vara heltäckande. Men den pekar på ett antal viktiga områden för att förstå Sveriges relativt svaga förmåga inom cybersäkerhet, vilket lett till låga rankingar internationellt. Detta står i kontrast till vår stora förmåga att ta till vara på digitaliseringens möjligheter.

Fragmenterad diskussion och bristande samverkan

Ett antal departement och myndigheter arbetar med frågor relaterade till cybersäkerhet. Ofta präglas diskussioner och förslag av denna uppdelning genom att fokus ligger på de specifika frågor som behandlas inom respektive departementssfär. Därmed riskerar ett nödvändigt brett och integrerat angreppssätt att försvinna.

Exempelvis är samarbetet mellan Försvars- och Justitiedepartementen viktigt för att hantera cybersäkerhetsfrågorna. Det fungerar idag inte tillräckligt bra eftersom det saknas effektiva samverkansarenor.

Industrins behov kommer inte fram

Många stora industriföretag anser att deras problematik och behov inte uppmärksammas tillräckligt i nationella initiativ kring cybersäkerhet. Det gäller frågor som regleringar, ansvarsfördelning och inte minst kompetensförsörjning.

Målbilder finns för verksamheter på den offentliga sidan, exempelvis försvaret. Men frågor hur Sveriges arbete på nationell nivå kring cybersäkerhet kan stärka industrins konkurrenskraft uppmärksammas inte tillräckligt.

Nationella hot underskattas

Medvetenheten om cyberhot mot enskilda företag och offentliga verksamheter varierar mycket. Även då medvetenheten finns agerar många verksamheter inte tillräckligt kraftfullt och sätter inte av tillräckliga resurser för att stärka cybersäkerheten.

COOP-exemplet sågs av vissa som en nationell kris. Men matförsörjningen i Sverige hotades inte eftersom det fanns alternativ. Sådana finns inte om elnätet angrips och slutar att fungera vilket är ett reellt cyberhot. Storskaliga cyberattacker mot större banker kan utsätta det finansiella systemet för en allvarlig chock, vars spridningseffekter kan utlösa en finanskris.

Olika förväntansbild hos statliga och privata aktörer

Förväntningarna på vad olika privata och offentliga aktörer ska göra i cybersäkerhetsarbetet skiljer sig åt. Många företag förväntar sig att staten ska leverera och lösa frågor som rimligen ligger inom företagets eget ansvarsområde. Det finns en passivitet som gör att många företag inte agerar utifrån de möjligheter som finns. Istället gör de för lite i avvaktan på åtgärder från myndigheterna.

Förväntan på statliga initiativ är ofta stor både vad gäller regelverk och tillgängliga resurser. Givet hoten och riskerna är denna förväntan högst rimlig. Men de statliga satsningarnas omfattning och avsatta resurser är begränsade.

Ett exempel är förhoppningarna kring cybersäkerhetsscentret som fått relativt lite extraresurser till de sju myndigheter (FMV, FRA, Försvarsmakten, MSB, Polisen, PTS och Säpo) som är involverade. Inte heller har stora operativa resurser avsatts.

Sverige – ett litet exportberoende land

Viktiga spelare inom digitaliseringen, där cybersäkerheten är en del, är USA, Kina och EU. EU är mycket aktivt i cybersäkerhetsfrågor. Vår möjlighet att påverka internationellt måste ske genom stor aktivitet inom EU och i direkt samverkan med andra länder.

Idag är Sverige alltför reaktivt och utnyttjar inte de möjligheter till påverkan som tidigt agerande i EUs olika processer ger möjlighet till. Våra möjligheter till påverkan ökar ytterligare när Sverige blir ordförandeland 2023.

Kompetensbehov

Behov av ökad kunskap och kompetens inom cybersäkerhetsområdet är stort inom både privat och offentlig sektor. Kunskaperna och medvetenheten varierar mycket mellan olika branscher och verksamheter men också mellan verksamheter inom en sektor. På många håll råder okunskap kombinerad med vilsenhet om hur man bör agera och vilken kunskap och kompetens som behöver byggas upp. Detta är allvarligt eftersom ingen annan än verksamheten själv äger sina cybersäkerhetsfrågor.

Brister i systemutveckling och arkitektur

När brister i systemutveckling och arkitektur diskuteras måste det ske med utgångspunkten att säker systemutveckling och systemförvaltning är oerhört svårt. Men det går att komma runt svårigheterna genom att utveckla verktyg och metoder så att utvecklare och förvaltare kan bygga system med en acceptabel säkerhet. Det gäller också att se till att existerande verktyg används och att de verktyg man är van vid inte används på rutin.

Den digitala infrastrukturen är vital för vårt samhälle. Teknikutvecklingen har pågått länge och infrastrukturen möter höga funktionella krav. Strukturen bygger på att många olika aktörer samverkar och tar sitt ansvar för säkerhetsfrågorna. Här brister det idag. Relativt få aktörer behärskar säkerhetsfrågorna fullt ut . Därför kan de inte möta högt ställda säkerhetskrav kring hur exempelvis arkitektur, autentisering och säkra applikationer måste samverka.

Ett vardagsexempel är hem där hushållsapparater och annan utrustning kopplas till internet för att kunna styras och övervakas. Det finns ingen eller dålig kontroll och reglering av vilka säkerhetskrav sådana produkter och system måste uppfylla. Detta vill EUs Cybersecurity Act komma till rätta med. Det saknas också kunskap och kompetens hos konsumenterna om cyberhoten mot deras digitala hemmiljö.

Mänskliga faktorn underskattas

Kunskapen om sårbarheten i olika system till följd av samspelet mellan människa och system är för låg på alla nivåer i samhället. Rent tekniskt kan man uppnå ett mycket gott skydd av ett it-system. Men beteenden hos individer och organisationer som använder systemet är en svag punkt som ofta utnyttjas i cyberattacker. Åtgärder för att öka dessa mjuka delar är en viktig del av utveckling och implementering av olika system.

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), 2021
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-R 514
ISSN: 1100-5645
ISBN: 978-91-89181-21-2

Projektledning: Per Hjertén, IVA
Text och analys: Staffan Eriksson, Per Hjertén, Jan Westberg, IVA
Redaktör: Jan Westberg, IVA
Layout: Pelle Isaksson, IVA
Tryck: EO Grafiska

Texten finns att ladda ned via www.iva.se

Cybersäkerhet för ökad konkurrenskraft är ett projekt av **Kungl. Ingenjörs-vetenskapsakademien (IVA)** och finansieras av Vinnova, FRA, FMV, Trafikverket, Svenska Bankföreningen, Ericsson, Saab, Internetstiftelsen, Teknikföretagen och SNUS (Swedish Network Users Society).

För mer information och kontakt:

Cybersäkerhet för ökad konkurrenskraft
Kung. Ingenjörsvetenskapsakademien (IVA)
Box 5073, 102 42 Stockholm, Sweden
Tel: 08-791 29 00
E-mail: info@iva.se
www.iva.se

IVA
Kungl. IngenjörsVetenskaps Akademien