EUROPEISKA UNIONENS CYBERSÄKERHETSBYRÅ

ETT EUROPA SOM BYGGER PÅ TILLIT OCH CYBERSÄKERHET

Enisa-strategi

Juni 2020

ETT EUROPA SOM BYGGER PÅ TILLIT OCH CYBERSÄKERHET

EUROPEISKA UNIONENS CYBERSÄKERHETSBYRÅ

FÖRORD

I mer än 15 år har Enisa – Europeiska unionens cybersäkerhetsbyrå – spelat en viktig roll för EU:s ambition att tillsammans med medlemsstaterna och EU:s institutioner och byråer stärka den digitala tilliten och säkerheten inom Europa. Genom att sammanföra olika grupper har Enisa framgångsrikt bidragit till att stärka Europas beredskap och respons på cyberhändelser.

Samtidigt har digitaliseringen av ekonomin och samhället drastiskt ökat, vilket blev tydligt under covid-19-krisen då många gjorde gemensam sak och använde it-lösningar på distans för att hålla verksamheter i gång. Den här krisen har tydligt visat hur mycket cyberangripare drar fördel av att vi är så beroende av denna teknik. Den har också åskådliggjort hur cyberhotlandskapet har breddats från riktade angrepp till nya former av massiva hot mot miljontals företag och allmänheten, där ett stigande antal incidenter omfattar avancerade utpressningsprogram. Den snabba utvecklingen av digitala produkter och tjänster – från molntjänster och videokonferenser till 5G och artificiell intelligens – har också inneburit att nya utmaningar behöver identifieras och hanteras.

Med sitt permanenta mandat i kombination med mer omfattande arbetsuppgifter och kapacitet har Enisa bättre förutsättningar än någonsin att spela en ledande roll för att hjälpa EU och dess medlemsstater att hålla jämna steg med dessa utmaningar när vi nu går in i en ny epok i fråga om cybersäkerheten i Europa.

Enisa kommer att göra detta genom att arbeta för att förutse relevanta trender samt samla in och sprida senaste expertis och kunskap för alla. Byrån kommer att bistå Europeiska kommissionen och medlemsstaterna med att hjälpa offentliga och privata aktörer och allmänheten att förhindra och hantera risker i samband med cyberincidenter. Med genomförandet av ramen för cybersäkerhetscertifiering bidrar Enisa till ett paradigmskifte genom att höja säkerhetsnivån för de digitala lösningar som används i Europa. I och med detta skapar Enisa bättre förutsättningar för alla att välja och känna tillit. Byrån kommer även att aktivt stödja aktörer som arbetar med cybersäkerhet i Europa att ingå ett nära samarbete och förbereda en gemensam respons när nästa omfattande cyberincident slår mot Europa.

När Enisa börjar arbeta i sin nya roll kommer öppenhet, flexibilitet och tillförlitlighet att vara viktiga ledstjärnor för den dagliga verksamheten samtidigt som byrån inleder ett närmare samarbete med medlemsstaterna och Europeiska kommissionen för att samordna strategierna. Enisa kommer även att sträva efter att förbättra sin miljöpåverkan mot bakgrund av den pågående klimatkrisen samt att erbjuda en socialt ansvarstagande och inkluderande arbetsmiljö.

I detta strategidokument, som har utarbetats genom en inkluderande samarbetsprocess som har involverat Enisas samtliga medarbetare, styrelseledamöter och den rådgivande gruppen, fastställs tydliga mål som kommer att vara drivande för Enisas arbete under de kommande åren för att hantera de många utmaningar som ligger framför oss.

På uppdrag av styrelsen

Jean-Baptiste Demaison
Styrelseordförande

Krzysztof Silicki
Vice styrelseordförande

VISION

Ett Europa som bygger på tillit och cybersäkerhet

UPPDRAG

Europeiska unionens cybersäkerhetsbyrå (Enisa) har som uppdrag att uppnå en hög gemensam nivå av cybersäkerhet i hela unionen i samarbete med den större allmänheten. Detta gör byrån genom att fungera som ett expertcentrum inom området cybersäkerhet samt att samla in och tillhandahålla oberoende högkvalitativ teknisk rådgivning och stöd till medlemsstater och EU-organ i frågor som rör cybersäkerhet. Byrån bidrar till att utveckla och genomföra unionens cyberpolitik.

Vi arbetar för att stärka förtroendet för den uppkopplade ekonomin, förbättra motståndskraften och tilliten i fråga om unionens infrastruktur och tjänster samt att upprätthålla digital säkerhet för vårt samhälle och allmänheten. Vi strävar efter att vara en flexibel och människoorienterad organisation som tar ett miljömässigt och socialt ansvar.

VÄRDERINGAR

Grupporienterat tankesätt
Enisa arbetar med olika grupper genom att respektera deras kompetens och expertkunskap samt främjar synergier och förtroende för att fullgöra sitt uppdrag på bästa sätt.

Högsta kvalitet
Enisa eftersträvar expertkunskap på spetsnivå i sitt arbete, håller högsta kvalitet i sin verksamhet och utvärderar sina resultat för att fortlöpande bli bättre genom innovation och framåtblickande.

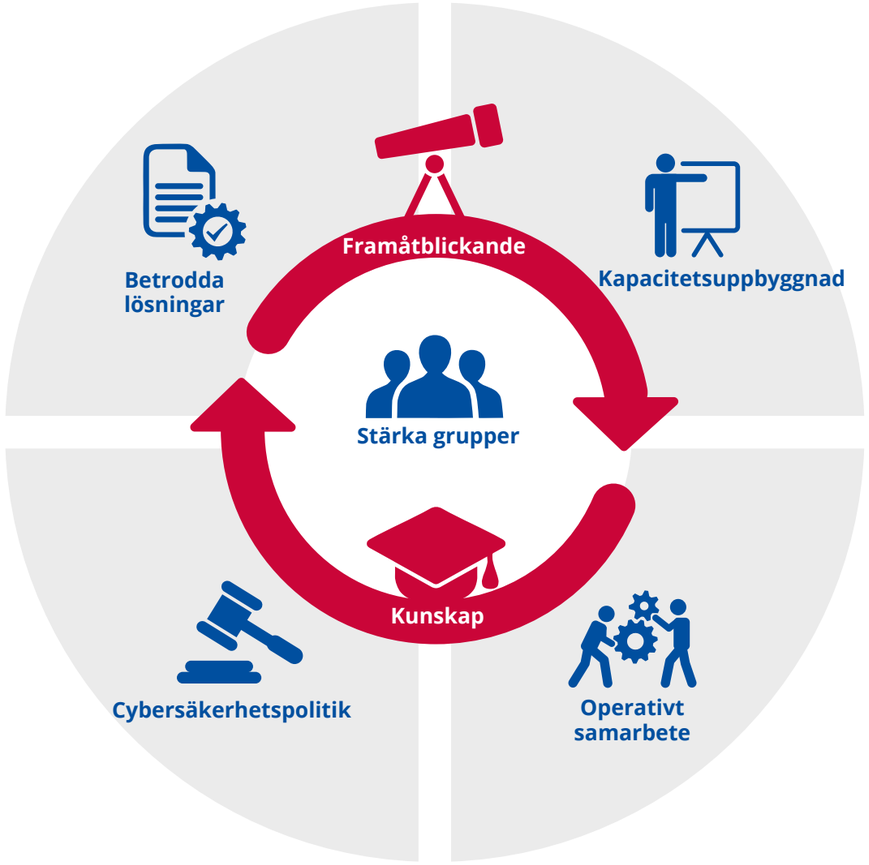
Integritet/etik
Enisa iakttar etiska principer och EU:s relevanta regler och åtaganden i sina tjänster och sin arbetsmiljö för att säkerställa rättvisa och inkludering.

Respekt
Enisa respekterar grundläggande europeiska rättigheter och värderingar i samtliga sina tjänster och sin arbetsmiljö samt sina intressenters förväntningar.

Ansvar
Enisa tar ansvar genom att säkerställa att sociala och miljömässiga aspekter integreras i praxis och förfaranden.

Öppenhet
Enisa inför förfaranden, strukturer och processer som är öppna, opartiska och oberoende för att på så sätt begränsa partiskhet, flertydighet, bedrägeri och oklarhet.

STRATEGISKA MÅL



STRATEGISKT MÅL 1

Strategiskt mål

STÄRKTA OCH ENGAGERADE GRUPPER I HELA EKOSYSTEMET FÖR CYBERSÄKERHET

Sammanhang

Cybersäkerhet är ett gemensamt ansvar. Europa eftersträvar en sektorsövergripande samarbetsram som inbegriper alla. Enisa spelar en viktig roll för att stimulera till aktivt samarbete mellan cybersäkerhetsintressenter i medlemsstaterna och EU:s institutioner och byråer. Byrån strävar efter att säkerställa att gemensamma insatser kompletterar varandra genom att tillföra ett mervärde till intressenter, utforska synergier samt utnyttja den begränsade tillgången till expertis och resurser inom cybersäkerhet på ett effektivt sätt. Grupper bör stärkas och ges utrymme att utöka modellen för cybersäkerhet.

Vad vi vill uppnå

- Ett EU-omfattande kunskapsorgan på spetsnivå för begrepp och metoder inom cybersäkerhet, som bygger upp ett samarbete mellan viktiga aktörer inom cybersäkerhet, sprider erfarenheter och EU:s expertis samt skapar nya synergier.
- Ett stärkt cyberekosystem som omfattar medlemsstaternas myndigheter, EU:s institutioner, byråer och organ, organisationer, forskningscentrum och universitet, branschen, privata aktörer och allmänheten, vilka alla har sin del i att göra Europa cybersäkert.

STRATEGISKT MÅL 2

Strategiskt mål

“

CYBERSÄKERHET SOM EN INTEGRERAD DEL AV EU:S POLITIK

Sammanhang

Cybersäkerhet utgör en väsentlig del av den digitala omvandlingen och behövs inom alla sektorer. Därför behöver denna fråga också övervägas inom ett brett spektrum av politiska områden och initiativ. Cybersäkerhet får inte begränsas till specialister i form av tekniska cyberexperter. Av dessa skäl ska cybersäkerhet integreras i alla områden inom EU-politiken. Det är viktigt att undvika fragmentering och det behöver säkerställas att strategin är konsekvent samtidigt som särdragen i varje sektor beaktas.

Vad vi vill uppnå

- Förebyggande rådgivning och stöd till alla berörda aktörer på EU-nivå där cybersäkerhet beaktas under hela processen för politisk utveckling genom genomförbara och riktade tekniska riktlinjer.
- Ramar för att hantera cybersäkerhetsrisker ska vara införda i samtliga sektorer och följas under hela processen för cybersäkerhetspolitiken.

STRATEGISKT MÅL 3

Strategiskt mål

> EFFEKTIVT SAMARBETE MELLAN OPERATIVA AKTÖRER INOM UNIONEN VID OMFATTANDE CYBERINCIDENTER

Sammanhang

Fördelarna med Europas digitala ekonomi och samhälle kan bara uppnås fullt ut om det råder cybersäkerhet. Cyberangrepp har inga gränser. Alla delar av samhället kan påverkas och unionen behöver vara redo att agera vid omfattande (storskaliga och gränsöverskridande) cyberangrepp och cyberkriser. Det ömsesidiga beroendet över gränserna har visat att det behövs ett effektivt samarbete mellan medlemsstater och EU-institutionerna för snabbare respons och samordning av insatserna på alla nivåer på ett lämpligt sätt (strategi, operativ drift, teknik och kommunikation).

Vad vi vill uppnå

- Ett fortlöpande gräns- och lageröverskridande stöd för samarbete mellan medlemsstater samt med EU-institutioner. Särskilt med tanke på potentiella storskaliga incidenter och kriser vill vi stödja utökningen av det teknisk-operativa, politiska och strategiska samarbetet mellan viktiga operativa aktörer för att möjliggöra läglig respons, informationsspridning, situationsmedvetenhet och kriskommunikation i hela unionen.
- Omfattande och snabb teknisk hantering på medlemsstaternas begäran för att tillgodose tekniska och operativa behov vid incident- och krishantering.

STRATEGISKT MÅL 4

Strategiskt mål

HÖG KOMPETENS OCH KAPACITET INOM OMRÅDET CYBERSÄKERHET I HELA UNIONEN

Sammanhang

Cyberangreppen sker allt oftare och blir alltmer avancerade samtidigt som användningen av IKT-infrastruktur och IKT-teknik ökar snabbt bland privatpersoner, organisationer och olika industrier. Det behövs mer kunskap och kompetens inom cybersäkerhet än vad det finns tillgång till. EU måste satsa på att bygga upp kompetens och utveckla personer med fallenhet inom cybersäkerhet på alla nivåer, från den vanliga användaren till den högkvalificerade specialisten. Investeringarna bör inte inriktas enbart på att höja kunskapsnivån om cybersäkerhet i medlemsstaterna, utan även på att se till så att olika operativa grupper har lämplig kapacitet för att hantera cyberhotlandskapet.

Vad vi vill uppnå

- Samordning av kompetens, yrkeserfarenhet och utbildningsstrukturer inom cybersäkerhet för att tillgodose EU:s ständigt stigande behov av kunskap och kompetens inom det här området.
- En högre grundnivå av medvetenhet och kompetens om cybersäkerhetsfrågor i hela EU samtidigt som cybersäkerhet integreras i nya ämnesområden.
- Väl förberedda och testade resurser med lämplig kapacitet att hantera de framväxande hoten i hela EU.

STRATEGISKT MÅL 5

Strategiskt mål

“

HÖG GRAD AV TILLIT TILL SÄKRA DIGITALA LÖSNINGAR

Sammanhang

Digitala produkter och tjänster innebär både fördelar och risker och dessa risker behöver identifieras och reduceras. När digitala lösningars säkerhet utvärderas för att säkerställa att de är tillförlitliga är det viktigt att tillämpa en gemensam strategi för att göra en avvägning mellan samhälleliga, marknadsmässiga, ekonomiska och cybersäkerhetsrelaterade behov. En neutral enhet som agerar transparent kommer att öka kundernas förtroende för digitala lösningar och den digitala miljön i stort.

Vad vi vill uppnå

- En cybersäker digital miljö i hela EU, där människor kan lita på produkter, tjänster och processer inom IKT genom att certifieringsprogram används inom viktiga tekniska områden.

STRATEGISKT MÅL 6

Strategiskt mål

FRAMÅTBLICKANDE I FRÅGA OM DE FRAMVÄXANDE OCH FRAMTIDA UTMANINGARNA PÅ CYBERSÄKERHETSOMRÅDET

Sammanhang

För en hel del ny teknik som fortfarande är i sin linda eller snart kommer att bli allmänt etablerad skulle det vara fördelaktigt med framåtblickande metoder. Genom en strukturerad process som möjliggör dialog mellan intressenter, beslutsfattare och politiskt ansvariga skulle det bli möjligt att fastställa tidiga reduceringsstrategier som förbättrar EU:s motståndskraft mot cybersäkerhetshot och hitta lösningar för att hantera framväxande utmaningar.

Vad vi vill uppnå

- En förståelse av framväxande trender och mönster med hjälp av framåtblickande och framtidsinriktade scenarier som bidrar till att reducera våra intressenters utmaningar inom cyberområdet.
- Tidig bedömning av utmaningar och risker med att framväxande framtida alternativ införs och anpassas i kombination med ett samarbete med intressenter om lämpliga reduceringsstrategier.

STRATEGISKT MÅL 7

Strategiskt mål

“

EFFEKTIV OCH ÄNDAMÅLSENLIG INFORMATIONS- OCH KUNSKAPSHANTERING OM CYBERSÄKERHET FÖR EUROPA

Sammanhang

Information och kunskap är en viktig faktor för att främja cybersäkerhet. Vi behöver fortlöpande samla in, organisera, sammanfatta, analysera, kommunicera och upprätthålla information och kunskap om cybersäkerhet för att de som arbetar professionellt med cybersäkerhet ska kunna uppnå våra mål, arbeta under förutsättningar som ständigt förändras – både sett till den digitala utvecklingen och aktörerna – och möta vår tids utmaningar. Alla faser är avgörande för att säkerställa att information och kunskap sprids och utökas inom EU:s ekosystem för cybersäkerhet.

Vad vi vill uppnå

- Gemensam informations- och kunskapshantering för EU:s ekosystem för cybersäkerhet i en tillgänglig, anpassad, lämplig och tillämpbar form, med lämpliga metoder, infrastrukturer och verktyg samt med kombinations- och kvalitetssäkringsmetoder för att se till att tjänsterna fortlöpande förbättras.

OM ENISA

Europeiska unionens cybersäkerhetsbyrå (Enisa) är en EU-byrå med uppgift att uppnå en hög gemensam nivå av cybersäkerhet i hela Europa. Europeiska unionens cybersäkerhetsbyrå, som grundades 2004 och stärktes genom EU:s cybersäkerhetsakt, bidrar till EU:s cyberpolitik, förbättrar tillförlitligheten för produkter, tjänster och processer inom IKT genom program för cybersäkerhetscertifiering, samarbetar med medlemsstater och EU-organ samt hjälper Europa att förbereda sig för morgondagens cyberutmaningar. Genom kunskapsspridning, kapacitetsuppbyggnad och åtgärder för att öka medvetenheten arbetar byrån tillsammans med sina huvudintressenter för att uppnå ökad tillit i den uppkopplade ekonomin, stärka motståndskraften i unionens infrastruktur och slutligen upprätthålla digital säkerhet för Europas samhälle och allmänhet. Mer information om Enisa och dess verksamhet finns på www.enisa.europa.eu

TP-02-20-759-SV-N

Enisa
Europeiska unionens cybersäkerhetsbyrå

Aten-kontoret
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Grekland

Heraklion-kontoret
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Grekland

enisa.europa.eu